Cleo Harmony®

User Guide

Version 5.8.1

September 2026

RESTRICTED RIGHTS
Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (C)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227 - 7013.

Cleo
4949 Harrison Avenue, Suite 200
Rockford, IL 61108 USA
Phone: +1.815.654.8110
Fax: +1.815.654.8294
Email: sales@cleo.com
www.cleo.com

Support: 1.815.282.7894, 1.866.444.2536 (US only), 02038653439 (UK), or support@cleo.com

Cleo reserves the right to, without notice, modify or revise all or part of this document and/or change product features or specifications and shall not be responsible for any loss, cost or damage, including consequential damage, caused by reliance on these materials.

This document may not be reproduced, stored in a retrieval system, or transmitted, in whole or in part, in any form or by any means (electronic, mechanical, photo-copied or otherwise) without the prior written permission of Cleo.

© 2003-2026 Cleo. All rights reserved. Cleo is a trademark of Cleo. Cleo Harmony, Cleo VLTrader, and Cleo LexiCom are registered trademarks of Cleo.

All other marks are the property of their respective owners.

Contents

Chapter 1: About Cleo Harmony, Cleo VLTrader, and Cleo LexiCom..... 11

Cleo Technical Support..... 11
Send Information to Technical Support..... 11

Chapter 2: Concepts..... 13

About Actions, Host Actions, and Hosts..... 13
Tree Structure..... 13
Screen layout..... 15
Tree Pane..... 15
Content Pane..... 15
Messages Pane..... 16
Status Bar..... 18
Log file..... 19
Directories/Maintenance..... 19
Dial-up Connections..... 30
Runtime Options..... 31

Chapter 3: Using your program..... 33

User Interface options..... 33
Requiring logins..... 33
Using the new Web Admin UI..... 33
Using the Classic Mode Web Admin UI..... 34
Controlling the program..... 38
Using the command line..... 38
Auto starting the VersaLex daemon in UNIX environments..... 51
Using a Custom Splash Screen..... 54
System Configuration..... 54
Monitoring source deletion..... 54
Configuring password policies..... 55
Setting up a GEGXS IBC dial-up connection (Windows users only)..... 56
Setting up a dial-up connection (Windows users only)..... 56
Setting up a LexiCom dial-up connection (Windows users only)..... 57
Configuring email or execute based on results..... 57
Generating files for an integration..... 58
Activating TradeLink communications agent service..... 59
Using macro variables..... 59
Using wildcards and regular expressions..... 69

Chapter 4: Hosts..... 75

Hosts – Web UI..... 75
Web UI Host Tree..... 75

Activating a host from a template in the Web UI....76
Advanced search options....76
Hosts and Mailboxes – Native and Classic Web UI....77
Activating a host from a template....77
Cloning and activating a pre-configured host....78
Configuring an active host....78
Creating a custom preconfigured host....79
Using the wizard to create a host or mailbox....79
Configuring mailbox packaging....79
Determining and providing your URL information....85
Acquiring your trading partner's signing and encryption certificates....86
Creating and providing your signing/encryption certificates....86
Emailing a profile to your trading partner....87
Sending a copy of a document to another host....88
Setting advanced host properties....89
Working with actions....89
Composing an action....89
Composing a host action....91
Using operating system commands in actions....93
Running and stopping an action....93
Host Technical Reference....93
FTP and FTP/s Hosts....94
HTTP and HTTP/s Hosts....120
AS2 Hosts....147
AS3 Hosts....177
AS4 Hosts....202
ebXML Hosts....231
SSH FTP Hosts....256
OFTP Hosts....285
MQ Hosts....321
SMTP and SMTP/s Hosts....343
MLLP Hosts....365
WS Hosts....385
RNIF Hosts....416
fasp Hosts....445
EBICS Hosts....464
HSP Hosts....498
Users Host....516
Connector Host....534
Standalone Actions....552

Chapter 5: Connectors....555

AMQP Connector....555
AzureBlob Connector....559
Clarify Connector....562
EEI Connector....563
File Connector....565
GCS Connector....569
HDFS Connector....570
IBMMQ Connector....571

ICAP Connector....574
Kafka Connector....575
LDAP Connector....584
Router Connector....587
S3 Connector....597
SFTP Connector....603
SharePoint Connector....606
SMB Connector....608

Chapter 6: Scheduler....611
Scheduling actions - Native and Classic Web UI....611
Scheduling actions to run at specific dates and times....612
Scheduling actions to run automatically by polling for files....613
Scheduling actions to run based on events....615
Scheduling actions - Web UI....616
Scheduling actions to run automatically by polling for files....617
Scheduling actions to run at specific dates and times....619
Scheduling actions to run based on events....620
Schedule formats....621
Date/time-based schedule format....622
Event-based schedule format....626

Chapter 7: Router....627
Setting up automated outgoing routes....628

Chapter 8: Partners....631
Managing Trading Partners....631
About the Trading Partners table....631

Chapter 9: Transfers....637
Viewing transfer status....637
Transfer Status Filter....637
Tool-tip snapshots....639
Right-click menu options....639
Viewing detailed information....640
Viewing a copy....640
Viewing Resend/Rereceive Chain....640
Resending and rereceiving....640
Emailing a Copy....642
Rerunning a Failed Action....643
Transfer Report Generation....643
Transfer EDI Table View....644
Transfer Entries for CHECK Commands....644
Viewing transfer status - Web UI....644
Resending and re-receiving - Web UI....645
Transfer Report generation - Web UI....645
View Information - Web UI....645

View File - Web UI....645
Download File - Web UI....645
Advanced filtering options for Transfers....646

Chapter 10: Logs....649

Viewing log files....649
Viewing the event log - Web UI....650
Advanced filtering options for Logs....651
Controlling Event Log Loading....652

Chapter 11: Administration....655

License and registration....655
About your license....655
Requesting a permanent license....657
Registering your serial number....658
Updating your software....658
Unregistering a license....660
Applications....660
Certificate management....661
Generating self-signed user certificates....662
Generating PEM-formatted certificate signing requests....664
Generating trusted CA certificates from OpenPGP or SSH FTP keys....665
Replacing a user certificate with a CA-signed certificate (server ID)....666
Importing certificates....666
Exporting certificates....668
Replacing trusted CA certificates....669
Moving certificates....670
Removing certificates....670
Configuring certificate management options including CRL and TSL....671
Viewing user and CA certificate usage....672
Exchanging certificates with your trading partner....672
About the Certificate Exchange dialog box....680
Scheduling certificates for future use....681
Reverting a certificate schedule....682
Allowing overlapping signing/encryption keys....685
Handling expired certificates....685
User management....686
Users....686
LDAP server....691
SAML configuration....696
File system....700
Specifying default host directories....700
CIFS directories....702
AS/400 Setup and installation....703
System....722
Databases....722
Exporting user files....726
Importing user files....727
Bootstrap configuration....728

Other system options....729
Advanced system options....743
Network....750
Local Listener....750
Clustering....880
Configuring for a proxy....881
Configuring IP filtering....886
Reviewing the IP filter list....887
Reviewing TCP/IP port usage....887
Synchronizing user configuration on multiple instances....888
Monitoring....892
Logs....892
Transfers....895
Polling....904
Thresholds....905
SNMP agent....907
Embedded database....909

Chapter 12: Cleo Portal....911
Configuring Cleo Portal....911
Customizing Cleo Portal....911
Setting Cleo Portal System Properties....913
Setting up single-login access to Admin UI and Cleo Portal....913
Two-factor authentication....914
Enabling mixed mode authentication for Cleo Portal....915
Copying items in Cleo Portal....915
Moving items in Cleo Portal....916
Renaming items in Cleo Portal....916

Chapter 13: Cleo VLNavigator....917
Configuring the Cleo VLNavigator application....918
Creating a VersaLex pool....918
VersaLex pools....920
User Groups, Transfer Monitors, and System Counters....921
Users....923
User Group Tab....929
Cleo VLNavigator User Tab....931
Applications....931
Dashboards....932
Operator Audit Trail....933
Cleo VLNavigator System Monitor....936
Configure Cleo Unify....937
Configure Cleo Trust....938

Appendix A: REST API....941

Appendix B: Extended Commands....943

CHECK command....943
CHECK command advanced properties....944
CHECK command dialog....944
CHECK command parameters....945
CHECK command search scope....949
CHECK command reference....950
SCRIPT command....951
SCRIPT command dialog....952
SCRIPT command reference....952

Appendix C: URI File System Interface....955
URI File System interface overview....955
JMS URI scheme....955
MSMQ URI scheme....960
VLPipe URI scheme....962
Custom URI scheme....962

Appendix D: Troubleshooting....965

Appendix E: XML file formats....969
Host files....969
System log file....972

Appendix F: Cryptographic Services....975
Cryptographic services overview....975
Signing and encryption: general overview....976
Content integrity through digital signatures (signing)....976
Encryption of zip files....977

Appendix G: AS2 Checklist....979
AS/400 Network Access Setup....980
AS/400 Network Access overview....980
Network Access process map....981
Configuring AS/400 Network Access....981
Selecting the AS/400 Inbound/Outbound Directory paths....982
Creating Inbound and Outbound native files....985
Creating links for the Inbound and Outbound files....985
Defining a default file member (AS2 only)....985
Defining an Authorization List....986
Configuring content-type inboxing for the Native File System (AS2 only)....986
Configuring AS/400 mapped drives for text conversion (Windows only)....989

Appendix H: Database Definitions....993
Driver and connection strings....994
Transfer database fields....996

Transfer log....996
External transfers....1000
EDI tracking fields....1000
XML tracking fields....1003
Text tracking fields....1004
Supplemental tracking fields....1004
SLA/KPI fields....1006
Static tables....1009
Database payload....1009
Sending database payload....1015
Receiving database payload....1016
Cleo VLNavigator Application/User access database fields....1017

Chapter

1

About Cleo Harmony, Cleo VLTrader, and Cleo LexiCom

VersaLex software is the platform that powers the Cleo family of Secure Data Integration (SDI) products—the Cleo LexiCom® application is a desktop-based client solution for communication with major trading networks. The Cleo VLTrader® application is a server-level solution designed to meet the needs of mid-enterprise organizations. The Cleo Harmony® application is tailored for large enterprise needs.

Cleo Technical Support

Standard Cleo Technical Support is available from 7am - 7pm CST, Monday through Friday. Support availability might differ depending on your support package.

Training and a support subscription are required to work with a Cleo technical support analyst for all products, except Cleo LexiCom.

When contacting the Cleo support team, have your contact information, the name of product you are calling about, and your serial number, if available. During the support process we may request additional information (for example, a support bundle) that will vary depending on the type of request or issue.

Requests are handled on a callback basis in the order they are received. The Cleo support answering service or web form will collect your information and your request will be placed in our callback queue.

To contact Cleo Technical Support:

- Use the request form at: https://support.cleo.com/hc/en-us.
- Call us:
  - 1-815-282-7894
  - US (toll free): 1-866-444-CLEO(2536)
  - UK: 02038653439

Send Information to Technical Support

In order to debug your specific problem, Cleo technical support might request that you send log files, host files or both for review.

1. In the web UI, go to **Administration** > **License & Registration** > **Support Bundle**. In the native UI, select **Help** > **Support** > **Bundle** from the menu bar.
2. Enter a description of the problem to be included in the bundle. If they are enabled, the system log file and debug file by default are included. The TCP/IP port usage report is always by default included. Host files can also be included; if selected, the user passwords encoded in a host file are cleared as the file is placed in the bundle. Click **Send**.
3. Enter your name, company name, phone number, and email address. The company name defaults to the license key owner. Modify the connection type, if necessary. Click **Send**.

Chapter

2

Concepts

This section provides basic conceptual information about Cleo Harmony you should be familiar with before you begin using the product.

About Actions, Host Actions, and Hosts

The basic building block of command execution within the product takes place within an action. From actions, sends (`PUT`) and receives (`GET`) are executed.

Actions are either mailbox-based, host-based, or not tied to any mailbox or host. Mailbox-based actions are the most common and are referred to as *actions* (or Action). Host-based actions are referred to as *host actions*. Both mailbox- and host-based actions are organized within the hierarchical structure of a host (see Tree Structure).

Actions not tied to any mailbox or host are referred to as *standalone actions*.

In this documentation, the term *action*, when used by itself, is considered a general reference to actions, host actions, or standalone actions, unless noted otherwise.

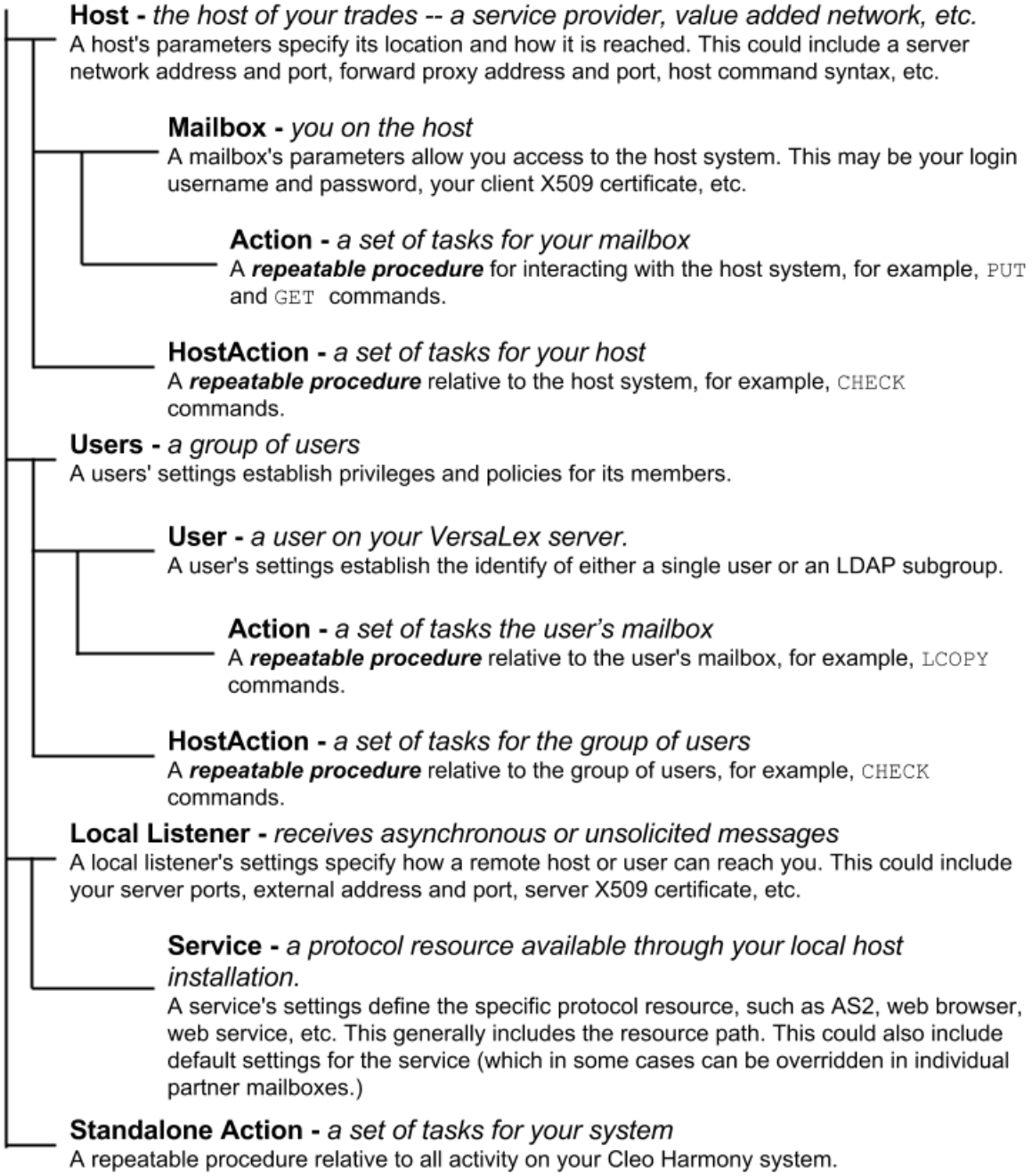
Note:

Host actions are only available in the Cleo Harmony and Cleo VLTrader applications.

Standalone actions are only available in the Cleo Harmony application.

Tree Structure

The Cleo Harmony application supports varying tree node types, including generic and customized FTP, HTTP, and AS2 connections, as well as user groups and services. But regardless of the host type, the Cleo Harmony application organizes the tree as shown in the following diagram.



Each branch is stored as an XML file. See XML file formats on page 969 for information about the layout of the XML file.

Screen layout

The main body of the Cleo Harmony window is divided into several sections:

- tree pane (upper-left),
- content pane (upper-right)
- messages pane (lower)
- status bar (bottom).

The Cleo Harmony application makes extensive use of right-click menus. When in doubt, especially in the tree pane, right-click.

Note: Any current or captured date and/or time shown within the Cleo Harmony application is formatted as `yyyy/mm/dd` and `hh:mm:ss` (24-hour clock).

Tree Pane

The tree pane actually contains two trees - the Active host tree and the Templates host tree. Only active hosts can be manipulated; template hosts are display-only until activated.

Within each folder in the tree, branches are sorted alphabetically.

Within the active tree, colors are used to represent status:

- Red indicates that the branch has been disabled and cannot be used.
- Orange indicates that configuration is incomplete for the branch and it is not yet ready for use.
- Green indicates that the branch or an action within the branch is currently running.

Content Pane

The tree pane selection controls what appears in the content pane.

- If you select a Hosts, Mailboxes, HostActions, TradingPartners, Actions, or Services folder in the tree pane, a folder table listing details specific to the folder contents is displayed in the content pane.
- If you select a specific host, mailbox, host action, trading partner, action, local host, or service in the tree pane, a configuration panel specific to the object selected is displayed in the content pane.

Folder table

When you select a folder containing Hosts, Mailboxes, HostActions, TradingPartners, Actions, or Services in the tree pane, the content of the folder is displayed in a table listing details specific to that folder.

Colors represent status:

- Red indicates that the branch has been disabled and cannot be used.
- Orange indicates that configuration is incomplete for the branch and it is not yet ready for use.
- Green indicates that the branch or an action within the branch is currently running.

You can sort the table using any column. The current sort column is marked accordingly.

Configuration panel

Even though configuration panels are specific to the host type and the branch selected, there are some similarities among them.

The upper section of the panel always contains the alias of the branch selected, the enabled selection, the ready indication, and the host type and transport description.

- If the enabled selection is set to `off`, it is displayed in red.
- Required fields are starred (*). If any required fields are missing or incorrect, the ready indication will be `off` and displayed as orange. If the mouse is moved over 'Ready', tool tip help will indicate which required field is missing.

The middle section of the panel always contains one or more tabbed sub-panels.

Some of the tabs are consistent across host types. For example, the **General** and **Notes** tabs above are used for ALL host types.

Password fields will mask the actual value entered (for example,).

The lower section of the panel always contains **Apply** and **Reset** buttons. These buttons are enabled only for **active** hosts when changes have been entered into the panel.

Messages Pane

The messages pane continually scrolls runtime messages as they occur. Messages can originate from two main sources:

A running *action, host action* or *local host* will generate status messages. Indentation and color are used to indicate message flow and status.

```
hh:mm:ss   <Action>Mailbox@Host         Run: type="type"
hh:mm:ss   <Action>Mailbox@Host         Detail: "message" level=#
hh:mm:ss   <Action>Mailbox@Host         Command: "put command"
 type="protocol" line=#
hh:mm:ss   <Action>Mailbox@Host         File: "local path" direction="Loca -
> Host" destination="remote path" number=# of #
hh:mm:ss   <Action>Mailbox@Host         PROTOCOL: "request"
hh:mm:ss   <Action>Mailbox@Host            Transfer: kB/sec=#.# kBytes=#.#
 seconds=#.#
hh:mm:ss   <Action>Mailbox@Host         Response: "good host response"
hh:mm:ss   <Action>Mailbox@Host         Result: "Success"
hh:mm:ss   <Action>Mailbox@Host         File: "local path" direction="Local-
>Host" destination="remote path" number=# of #
hh:mm:ss   <Action>Mailbox@Host         PROTOCOL: "request"
hh:mm:ss   <Action>Mailbox@Host            Transfer: kB/sec=#.# kBytes=#.#
 seconds=#.#
hh:mm:ss   <Action>Mailbox@Host         Response: "good host response"
hh:mm:ss   <Action>Mailbox@Host         Result: "Success"
--> hh:mm:ss   <Action>Mailbox@Host      Command:-->  "get command"
 type="protocol" line=#
hh:mm:ss   <Action>Mailbox@Host         File: "remote path" direction="Host-
>Local" destination="local path" number=# of #
hh:mm:ss   <Action>Mailbox@Host         PROTOCOL: "request"
hh:mm:ss   <Action>Mailbox@Host            Transfer: kB/sec=#.# kBytes=#.#
 seconds=#.#
hh:mm:ss   <Action>Mailbox@Host         Response: "bad host response"
hh:mm:ss   <Action>Mailbox@Host         Result: "unsuccesful" "reason"
hh:mm:ss   <Action>Mailbox@Host         Hint: "possible cause"
hh:mm:ss   <Action>Mailbox@Host   End
```

--> Message Type	Purpose	How many	Color
--> Run:	Mark start of action run, has run type	1	Black

--> Message Type	Purpose	How many	Color
--> Detail:	Provide extra detailed information; can appear anywhere in the flow	Unlimited	Black
--> Command:	Mark start of a command, has command text and line number	--> 0 or more per Run:	Green
--> File:	Mark start of a file transfer, has file paths and counts	--> 0 or more per Command	Blue
--> Transfer:	Mark completion of a file transfer, has transfer rate	1 per File	Blue
FTP: or HTTP:	Protocol-specific request made to host	0 or more per Command	Black
Response:	Protocol-specific response from host	1 per FTP or HTTP request	Black if good --> Red --> if bad
--> Result:	Mark end of a command or file transfer, has resultant status	--> 1 per Command or File	--> Green --> if successful --> Red --> if unsuccessful
Hint:	Provide insight into possible cause of error or exception	Unlimited	Magenta
End	Mark end of action run	1	Black

The outer Cleo Harmony application shell may detect a situation that requires a message. Color is used to indicate message severity.

hh:mm:ss Note: "*message*"

hh:mm:ss Warning: "*message*"

hh:mm:ss Error: "*message*"

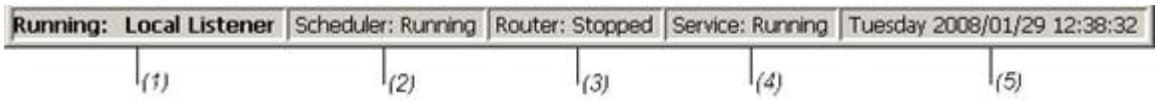
hh:mm:ss Exception: "*message*"

hh:mm:ss Detail "*message*" level=#

Type	Purpose	Color
Note:	Log a notable condition	Black
Warning:	Log a cautionary condition	--> Orange
Error:	Log an unrecoverable error	Red
Exception:	Log an unrecoverable program exception	Red
--> Detail:	Provide extra detailed information; can appear anywhere in the flow	Black

Status Bar

The status bar has five sections:



1. Lists any running *action*, *host actions*, and *local hosts*.
2. Indicates whether the Cleo Harmony scheduler is currently running.
3. VLTrader and Harmony only. Indicates whether the Cleo Harmonyrouter is currently running.
4. Shows the mode of the Cleo Harmony UI:
   - **Service/Daemon: Running** - The Cleo Harmony UI is a 2nd process attached to a Cleo Harmony Windows service or Unix daemon, which is running in the background. If the Cleo Harmony service/daemon should stop, the Cleo Harmony UI will indicate **Service/Daemon: Stopped** and then shutdown.
   - **UI Service/Daemon** - Cleo Harmony is not running in the background as a Windows service or Unix daemon, but the Cleo Harmony UI **is** enabled as a "service" (see Other system options on page 729). This means that the Cleo Harmony UI will act as a Cleo Harmony service/daemon would and service any Cleo Harmony command line processes.
   - **Standalone** - Cleo Harmony is not running in the background as a Windows service or Unix daemon, and the Cleo Harmony UI **is not** enabled as a "service" (see Other system options on page 729). This means that Cleo Harmony command line processes will queue up and only run after the Cleo Harmony UI is exited.
   - **Service/Daemon** - Cleo Harmony is running in the background as a Windows service or Unix daemon, but because the Cleo Harmony service/daemon is enabled as a UI (see Other system options on page 729), there is not a 2nd Cleo Harmony UI process attached (i.e. the Cleo Harmony service/daemon process itself is displaying the UI).

   Note: When Cleo Harmony is running on an AS/400, by default it is running in the background like a Windows service or Unix daemon. The Cleo Harmony UI can be displayed on a Windows PC connected to the AS/400, and in this case the Cleo Harmony UI mode will be **AS/400: Running**.
5. Continually reflects the current day, date, and time.

Log file

Each message shown in the messages pane is also written to an XML log file. The log file contents can be viewed via Cleo Harmony at any time. Additionally, since it is an XML file (and it is always well-formed), the log file can also be viewed through a browser at any time, potentially with an XSL style sheet applied. See XML file formats on page 969 for information about the layout of the log XML file.

If the size of the log file should reach five megabytes, by default Cleo Harmony will automatically archive and restart the log file.

A Cleo Harmony debug file (which contains very detailed protocol runtime information, mainly intended for technical support debugging purposes) is also potentially generated.

The level of detail shown in the messages pane can be configured differently than what is logged to the file. The default level of detail shown in the messages pane and logged to the file are both High – 3.

Directories/Maintenance

The directory structure for the installed product is as follows:

. \ (VersaLex home)

VersaLex executable file (‘ *VersaLex* .exe’), command line file (‘ *VersaLex* c.exe’), and other software executable files. If the java runtime environment (JRE) should terminate unexpectedly, it may dump trace or heap files.

Archive/copy files accumulate in this directory.

.license

Contains product license files.

Automatically created and updated when register product and acquire permanent license.

AS2

AS2 protocol directories

data

Message ID and filename history

Retention period can be changed in the AS2 service AS2 tab.

mdn

received

Message disposition notifications (receipts) received.

You can control the storage location. See *MDN Storage Folder* in Local Listener AS2 Service reference on page 768.

Received MDNs are always retained.

archived

Archived MDN zip files.

You can set Archive properties. See Specifying Local Listener advanced properties on page 759.

Archive/copy files accumulate in this directory.

sent

Message disposition notifications (receipts) sent.

You can control the storage location. See *MDN Storage Folder* in Local Listener AS2 Service reference on page 768.

For Cleo VLTrader and Cleo Harmony, sent receipts are always saved.

For Cleo LexiCom, you can configure your system to save sent receipts. See *Save Sent Receipt* in Specifying Local Listener advanced properties on page 759.

archived

Archived MDN zip files.

You can set Archive properties. See Specifying Local Listener advanced properties on page 759.

Archive/copy files accumulate in this directory.

received

Copies of raw incoming messages.

You control whether these messages are saved. See *Store Raw Received Message* in Specifying Local Listener advanced properties on page 759

Archive/copy files accumulate in this directory.

sent

Copies of raw outgoing messages.

You control whether these messages are saved per trading partner. See *Store Raw Sent Message* in AS2 Host: Advanced Tab on page 152.

Archive/copy files accumulate in this directory.

restart

Partial incoming message.

You can change this storage location. See *Restarts Temp Folder* in Local Listener AS2 Service reference on page 768.

unsent

Copies of outgoing messages waiting for asynchronous MDN.

AS3

AS3 protocol directories.

data

Message ID history.

You can control the retention period for this directory. See *Retain Message ID History* in Local Listener AS3 Service reference on page 770.

mdn

received

Message disposition notifications (receipts) received.

Received MDNs are always retained, but you can control the storage location. See *MDN Storage Folder* in Local Listener AS3 Service reference on page 770.

archived

Archived MDN zip files.

You can set Archive properties. See Specifying Local Listener advanced properties on page 759.

Archive/copy files accumulate in this directory.

sent

Message disposition notifications (receipts) sent.

You can control the storage location. See *MDN Storage Folder* in Local Listener AS3 Service reference on page 770.

For Cleo VLTrader and Cleo Harmony, sent receipts are always saved.

For Cleo LexiCom, you can configure your system to save sent receipts. See *Save Sent Receipt* in Specifying Local Listener advanced properties on page 759

archived

Archived MDN zip files.

You can set Archive properties. See Specifying Local Listener advanced properties on page 759.

Archive/copy files accumulate in this directory.

received

Copies of raw incoming messages.

You control whether these messages are saved. See *Store Raw Received Message* in Specifying Local Listener advanced properties on page 759

Archive/copy files accumulate in this directory.

sent

Copies of raw outgoing messages.

You control whether these messages are saved per trading partner. See *Store Raw Sent Message* in AS3 Host: Advanced Tab on page 180.

Archive/copy files accumulate in this directory.

unsent

Copies of outgoing messages waiting for asynchronous MDN.

AS4

AS4 protocol directories

data

Message ID history.

Retention period can be changed through the **PMode.ReceptionAwareness.DuplicateDetection.MaxWindow** setting.

ping

Payloads received as part of a Test Service PING operation.

receipt

received

Receipts received as part of a Test Service PING operation.

sent

Receipts sent as part of a Test Service PING operation.

receipt

received

Received receipts. Received receipts are always retained.

You can control the storage location. See Configuring AS4 Service on page 771.

archive

Archived received receipts.

These include the actual receipt files as well as the INF files that contain auxiliary information pertinent to a push of a User Message.

You can set Archive properties. See Specifying Local Listener advanced properties on page 759.

sent

Sent receipts. Sent receipts are always retained.

You can control the storage location. See Configuring AS4 Service on page 771.

archive

Archived sent receipts.

You can set Archive properties. See Specifying Local Listener advanced properties on page 759.

schemas

Schemas used by AS4 for XML schema validation.

sent+received

Copies of raw incoming and outgoing requests and responses. Stores information for both client-side and server-side operations.

You can configure whether raw messages are stored. See *Store Raw Sent Message* in AS4 Host: Advanced Tab on page 206 and *Store Raw Received Message* in Specifying Local Listener advanced properties on page 759.

Files in this folder are not archived, so generally this setting to should be 'off' to conserve disk space.

unsent

Transient copies of outgoing User Messages waiting for a response, either a synchronous response or an asynchronous response, depending upon the settings. Associated INF files are also stored while the transfer is in progress.

Transient copies of User Message will be deleted once the transfer is complete (successfully or otherwise). Associated INF files will be move to the receipt\received folder once the transfer is complete.

autoroute

Cleo VLTrader and Cleo Harmony systems only.

Default directory for outgoing payload files to be automatically processed based on routing rules

You can set up the Autoroute Directory. See Setting up automated outgoing routes on page 628.

autorun

Default directory for “command” files to be automatically processed

You can change the Autorun Directory. See Other system options on page 729.

backup

Versioned patch incremental backups. See Updating your software on page 658.

Archive/copy files accumulate in this directory.

BI

Cleo VLTrader and Cleo Harmony systems only.

Business intelligence resource folder for dashboards and system monitor.

certs

pending

Trusted and pending (untrusted) X509 certificate authority (CA) files for secure transfers.

You can add, modify, and delete trusted and pending certificate files directly in this directory, but the preferred method is to use the Certificate Manager. See Certificate management on page 661.

conf

Product configuration files.

Managed via various **Configure…** and **Tools…** items.

unsynced

Synchronized configuration changes not yet applied.

data

X509 user certificate and private key store files for secure transfers. Can include OpenPGP and SSH keys.

Managed using the Certificate Manager. See Certificate management on page 661.

EBICS

EBICS protocol directories

ack

sent

Acknowledgments (receipts) sent

“Save Sent Receipt” can be set in the Local Listener Advanced tab.

archive

Archived receipt zip files

“Archive ..." properties can be set in the Local Listener Advanced tab.

Archive/copy files accumulate in this directory.

schemas_2_4

EBICS Version 2.4 schema files

schemas_2_5

EBICS Version 2.5 schema files

sent+received

Copies of “raw” incoming requests and corresponding outgoing responses

“Store Raw Sent And Received” can be set in the EBICS host Advanced tab

Archive/copy files accumulate in this directory.

unsent

Transient copies of outgoing XML

ebXML

ebMS protocol directories

ack

received

Acknowledgments (receipts) received

You can control the storage location for received ACKs. See Configuring ebXML Message Service on page 772.

Received ACKs are always retained.

archive

Archived ACK zip files

sent

Acknowledgments (receipts) sent

You can control the storage location for sent ACKs. See Configuring ebXML Message Service on page 772.

For Cleo VLTrader and Cleo Harmony, sent receipts are always saved.

For Cleo LexiCom, you can configure your system to save sent receipts. See *Save Sent Receipt* in Specifying Local Listener advanced properties on page 759

archive

Archived ACK zip files

data

Message ID history

You can control how long this data is retained. See Configuring ebXML Message Service on page 772 and Local Listener ebXML Service reference on page 772.

schemas

ebMS schema files

sent+received

Copies of raw incoming and outgoing messages

You can control whether raw messages received are stored. See *Store Raw Received Message* in Specifying Local Listener advanced properties on page 759.

You can configure whether raw sent messages are stored per trading partner. See *Store Raw Sent* ebXML Host: ebXML Tab on page 233.

Archive/copy files accumulate in this directory.

unsent

Copies of outgoing messages waiting for asynchronous acknowledgment.

home

The default location for the file/directory chooser when there is no other appropriate default folder.

hosts

Active host XML files

Created when you activate a pre-configured host.

pre-configured

Pre-configured host XML files

archive

Pre-released, beta or “backup” hosts. Directory can be empty.

custom

Custom, preconfigured hosts

See Creating a custom preconfigured host on page 79.

support

Active support host XML files (for communicating with Cleo web site)

pre-configured

Pre-configured support host XML files

unsynced

Synchronized host changes not yet applied

HTTP

HTTP client protocol directories

sent

Copies of raw outgoing messages

You can configure whether raw sent messages are stored per trading partner. See *Store Raw Sent Message* in HTTP Host: Advanced Tab on page 125.

Archive/copy files accumulate in this directory.

inbox

Default (parent) directory for incoming payload files.

You can specify the default system inbox. See Specifying default host directories on page 700.

jre

Java runtime environment

lib

Main product library files

api

Embedded custom API libraries

You can specify custom classes. See *Custom ILexiComIncoming Class*, *Custom LexiComLogListener Class*, and *Custom LexiComOutgoingThread Class* in Other system options on page 729.

ext

Add-on third-party libraries, for example, database driver

help

Product help library

ws

Web service client runtime libraries

local\root

Default FTP, HTTP, and SSH FTP server root directory.

Note: Cleo VLTrader and Cleo Harmony systems only.

logs

System XML log file (`VersaLex.xml`), system debug file (`VersaLex.dbg`), and other log and debug files

You can set system log and debug options. See Logs on page 892.

You can set web UI debug options. See Configuring web browser service advanced properties on page 797.

Archive/copy files accumulate in this directory.

archive

Default directory for archived system XML log files

You can control storage location. See Logs on page 892.

Archive/copy files accumulate in this directory.

olddbg

Archived system debug files

Retention period of three days cannot be changed.

lostandfound

Incoming payload for unknown trading relationships

You can specify what, if any, action should be taken when a message is received form an unknown trading partner. See *Unknown Partner Message Action* in Specifying Local Listener advanced properties on page 759.

Archive/copy files accumulate in this directory.

OFTP

Odette FTP protocol directories

data

Message ID history.

You can control how long this data is retained.

See Configuring OFTP Service on page 777 and Local Listener OFTP Service reference on page 777.

eerp

received

End-to-end responses (receipts) received

Received EERPs/NERPs are always retained.

You can control where received responses are stored.

See Configuring OFTP Service on page 777 and Local Listener OFTP Service reference on page 777.

archive

Archived EERP zip files

You can specify Archive properties. See Specifying Local Listener advanced properties on page 759.

Archive/copy files accumulate in this directory.

sent

End-to-end responses (receipts) sent

You can control whether sent receipts are saved. See *Save Sent Receipt* in Specifying Local Listener advanced properties on page 759.

You can also control where sent receipts are stored. See Configuring OFTP Service on page 777 and Local Listener OFTP Service reference on page 777.

archive

Archived EERP zip files

You can specify Archive properties. See Specifying Local Listener advanced properties on page 759.

Archive/copy files accumulate in this directory.

received

Copies of raw incoming messages

You can control whether raw messages received are stored. See *Store Raw Received Message* in Specifying Local Listener advanced properties on page 759.

sent

Copies of “raw” outgoing messages

You can configure whether raw sent messages are stored per trading partner. See *Store Raw Sent Message* in OFTP Host: Advanced Tab on page 292.

restart

Partial incoming message

You can change this storage location. See *Restarts Temp Folder* in Local Listener OFTP Service reference on page 777.

unsent

Copies of outgoing messages waiting for EERP

outbox

Default (parent) directory for outgoing payload files

You can specify the default system outbox. See Specifying default host directories on page 700.

test

Files used for testing with the Cleo Test Server

receivedbox

System actually defaults to no receivedbox.

You can specify the default system receivedbox. See Specifying default host directories on page 700.

archive

Archived receivedbox copies zip files

You can set Sent/Received Box Archive properties. See *Sent/Received Box Archive*, *Sent/Received Box Archive After Files*, *Sent/Received Box Archive Size (mbytes)*, and *Sent/Received Box Archive Append To Zip* in Other system options on page 729.

sentbox

System actually defaults to no sentbox.

You can specify the default system sentbox. See Specifying default host directories on page 700.

archive

Archived sentbox copies zip files

You can set Sent/Received Box Archive properties. See *Sent/Received Box Archive*, *Sent/Received Box Archive After Files*, *Sent/Received Box Archive Size (mbytes)*, and *Sent/Received Box Archive Append To Zip* in Other system options on page 729.

rejectbox

Default directory for rejected outgoing files

You can specify the default system rejectbox. See Specifying default host directories on page 700 and Default host directory Reference on page 700.

resource

Installer resource files

RNIF

RosettaNet Implementation Framework protocol directories

ack

received

Acknowledgments (receipts) received.

Received ACKs are always retained.

You can control where received responses are stored.

See Configuring Local Listener RosettaNet Service on page 776 and Local Listener RosettaNet Service reference on page 776.

archive

Archived ACK zip files

You can specify Archive properties. See Specifying Local Listener advanced properties on page 759.

sent

Acknowledgments (receipts) sent

You can specify whether sent responses are stored. See *Save Sent Receipt* in Specifying Local Listener advanced properties on page 759

You can control where sent responses are stored.

See Configuring Local Listener RosettaNet Service on page 776 and Local Listener RosettaNet Service reference on page 776.

archive

Archived ACK zip files

You can specify Archive properties. See Specifying Local Listener advanced properties on page 759.

data

PIP Instance/Message ID history

You can control how long this data is retained.

See Configuring Local Listener RosettaNet Service on page 776 and Local Listener RosettaNet Service reference on page 776.

DTDs

PIP content validation DTD files shipped with product or imported

pips

Pre-defined PIPs shipped with product

schemas

PIP content validation schema files shipped with product or imported

sent+received

Copies of raw incoming and outgoing messages

You can control whether raw messages received are stored. See *Store Raw Received Message* in Specifying Local Listener advanced properties on page 759.

You can configure whether raw sent messages are stored per trading partner. See *Store Raw Sent Message* RNIF Host: Advanced Tab on page 423.

Archive/copy files accumulate in this directory.

unsent

Copies of outgoing messages waiting for asynchronous acknowledgment.

SMTP

SMTP protocol directories

data

Message ID history

Retention period can be changed in the SMTP Service SMTP tab.

You can control how long this data is retained.

See Local Listener SMTP Service on page 778 and Local Listener SMTP Service reference on page 779.

dsn

received

Delivery status notifications (receipts) received.

Received EERPs/NERPs are always retained.

You can control where received EERPs/NERPs are stored. See Local Listener SMTP Service on page 778 and Local Listener SMTP Service reference on page 779.

archive

Archived DSN zip files

You can specify Archive properties. See Specifying Local Listener advanced properties on page 759.

Archive/copy files accumulate in this directory.

sent

Delivery status notifications (receipts) sent.

You can specify whether sent receipts are stored. See *Save Sent Receipt* in Specifying Local Listener advanced properties on page 759

You can control where sent receipts are stored. See Local Listener SMTP Service on page 778 and Local Listener SMTP Service reference on page 779.

archive

Archived DSN zip files

You can specify Archive properties. See Specifying Local Listener advanced properties on page 759.

Archive/copy files accumulate in this directory.

received

Copies of raw incoming messages

You can control whether raw messages received are stored. See *Store Raw Received Message* in Specifying Local Listener advanced properties on page 759.

Archive/copy files accumulate in this directory.

sent

Copies of raw outgoing messages

You can configure whether raw sent messages are stored per trading partner. See *Store Raw Sent Message* SMTP Host: Advanced Tab on page 346.

Archive/copy files accumulate in this directory.

unsent

Copies of outgoing messages waiting for DSN

temp

VersaLex non-persistent work area

thirdparty

Information about included third-party software

translators

Sub-directories containing files for use with an EDI translator

See Generating files for an integration on page 58.

webserver

VLPortal

Cleo VLTrader and Cleo Harmony systems only.

Web portal documents, images, HTML pages, and language-specific property files.

Files can be imported through web page and web portal build functions that are described under the Web Browser Service VLPortal tab.

doc

img

html

internationalization

WS

Web service protocol directories

conf

Apache AXIS and WS security files

received

Copies of raw incoming messages

You can control whether raw received messages are stored. See *Store Raw Received Message* in Specifying Local Listener advanced properties on page 759.

sent

Copies of raw outgoing messages

You can configure whether raw sent messages are stored per trading partner. See *Store Raw Sent Message* WS Host: Advanced Tab on page 389.

"Store Raw Sent Message" can be set per trading partner in the WS host Advanced tab.

Files can accumulate in the directories marked with an **(X)** above. VersaLex will not automatically delete files in these directories. Be sure to turn off any debugging options that may cause files to accumulate once a problem has been solved. For example:

- Heap files in the home directory
- AS2 raw received files in the AS2/received directory
- HTML*.dbg files in the logs/ directory

VersaLex will also not remove any non-empty inbound or outbound directories associated with hosts or mailboxes if the host or mailbox is renamed or deleted since these directories could also be used by other trading relationships or by other applications. These directories may be manually removed, if desired, after verifying that they are no longer in-use.

Dial-up Connections

Windows users can install the Cleo LexiCom dialer and/or the GEGXS IBC dialer, which allow the use of dial-up networking for connectivity. The Cleo LexiCom dialer can be used to interface with Windows' Remote Access Service (RAS) phonebook entries to connect to the Internet or Virtual Private Networks (VPNs). The GEGXS IBC dialer is used specifically to connect to the GE hubs (GE Tradanet, GE EDI*Express, and GE ICS).

Runtime Options

There are five different Cleo Harmony runtime options.

Run action via Cleo Harmony UI

Use this option when:

- you run actions manually
- you schedule actions within the Cleo Harmony application to run either periodically or whenever there is a file to send.
- you use Cleo Harmony application as an "always live" server to receive files (for example, AS2)

Running the Cleo Harmony UI, installing as a Windows service or run as a Unix daemon, and running from the command line are not mutually exclusive.

Install the Cleo Harmony application as a Windows service or run Cleo Harmony as a Unix daemon

Use this option when:

- you schedule actions within the Cleo Harmony application to run either periodically or whenever there is a file to send.
- you use Cleo Harmony application as an "always live" server to receive files (for example, AS2)

See Auto starting the VersaLex daemon in UNIX environments on page 51.

Running the Cleo Harmony UI, installing as a Windows service or running as a Unix daemon, and running from the command line are not mutually exclusive.

Note: By default, Windows services run under a SYSTEM user and do not see mapped drives. If the Cleo Harmony application is installed as a service on Windows, use full network path names for the directories and ensure proper user authorization. If necessary, change the service to log on under a different account.

Run action via Cleo Harmony command line

Use this option when:

- you run actions manually
- a 3rd-party software application (for example, a translator) runs actions

Map/mount Cleo Harmony installed drive and run action remotely via Cleo Harmony command line

Use this option when:

- a remote computer needs to run an action

See Running from the command line on page 38.

To run an action remotely via command line, the Cleo Harmony application must be installed and/or running as a service/daemon on the target computer.

Note: By default, Windows services run under a SYSTEM user and do not see mapped drives. If the Cleo Harmony application is installed as a service on Windows, use full network path names for the directories and ensure proper user authorization. If necessary, change the service to log on under a different account.

Run action remotely via Cleo Harmony autorun

Use this option when:

- a remote computer needs to run an action

See Using Autorun on page 50.

To run an action remotely via autorun, the Cleo Harmony UI must be running or the Cleo Harmony application must be installed and/or running as a service/daemon on the target computer.

Chapter

3

Using your program

This section provides basic information about using your Cleo VersaLex program.

User Interface options

This section contains information about options related to the user interface for the Cleo Harmony application.

Requiring logins

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

See Cleo VLNavigator on page 917 for more information about privileges.

1. If the optional Cleo VLNavigator add-on application is installed, user groups and users can be created. As soon as at least one user group is assigned access to the Cleo VLTrader or Cleo Harmony application, a login is required with each invocation of the Cleo VLTrader or Cleo Harmony UI. (A login is always required with each invocation of the Cleo VLNavigator UI).
2. Enter your username and password (both case-sensitive). To change your password, click **Options**.
3. Click **OK** to proceed. The Cleo Harmony service/daemon will verify your credentials and apply your user group's granted privileges to the user session.

Using the new Web Admin UI

This section describes options specific to the new Web Admin UI.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

Accessing Classic mode in the Web UI

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

Data for the new Web Admin UI comes from the Cleo Harmony or Cleo VLTrader built-in NoSQL database. Prior to the 5.5 release, this database was disabled by default, and any historical data not present within is only available using Classic Mode or the native UI.

To access Classic Mode:

1. Click on the person icon in the top menu bar to expose its drop-down menu, and select **My Account**.
2. In the presented dialog, select the **Preferences** tab.
3. Check **Show classic mode** and click **Save**.

Settings persistence in the Web UI

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

In the new Web Admin UI, there are several auto-saved table settings. Each of them is stored in a per user, per browser fashion. Filter settings, column sizes, and column order, as well as specific table display preferences (for example, **Show milliseconds**) are saved to local storage. Local storage will persist until manually cleared. Column sorting is saved in the browser's session storage which is cleared whenever the browser tab or window is closed.

Please note that if the browser is being operated in "Incognito" or "Private" mode, the settings will not be saved or persist after the window is closed.

Controlling dialog boxes in the Web UI

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

Some dialog boxes in the web UI have interactive features. These dialog boxes can be minimized, maximized, resized, and repositioned to a different place on the screen. To identify these dialog boxes, look for the **Maximize Window** icon in the upper right corner of the box. Dialog boxes wtihout a **Maximize Window** icon do not have these capabilities.

- To expand the dialog box to the size of the page, click **Maximize Window**.
- To restore the dialog box to its original size, click the **Restore Window** icon in the upper right corner of the box.
- To resize the dialog box, hover over an edge until the cursor changes to an arrow, and then click and drag. Some dialog boxes have a minimum size requirement, so the box might not continue to shrink while dragging.
- To reposition the dialog box, click the title bar and drag to the desired location.
- Dialog box width and horizontal position will automatically adjust according to the browser window size. Once it has been resized or repositioned, it will no longer respond to browser window size changes.

Using the Classic Mode Web Admin UI

This section describes options specific to the Classic Mode Web Admin UI.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

Using the Web Browser UI

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

You can use a web browser UI to access Cleo Harmony, Cleo VLTrader, or Cleo VLNavigator software. To configure and set up the parameters of the web browser service, see Configuring Cleo VersaLex web browser service on page 781.

To run the Cleo Harmony or Cleo VLTrader application from a web browser while not running through a Cleo VLProxy connection, you must enter the proper URL in the browser:

```
http(s)://VersaLexComputerIP: http(s)Port/VersaLexResourcePath
```

To run VersaLex from a web browser while running through a VLProxy connection, the VersaLex serial number must be supplied as a parameter:

```
http(s)://VLProxyComputerIP: http(s)Port/VersaLexResourcePath?serial=LX7589-YU2693
```

or concatenated to the resource, preceded by a dash:

```
http(s)://VLProxyComputerIP: http(s)Port/VersaLexResourcePath-LX7589-YU2693
```

In addition, you can use a number of optional URL parameters to associate external IDs with new or existing VersaLex host/mailbox aliases, limit the contents of the UI, and provide user authentication:

Type	Parameter	Description	Values
a	`hostID=`	ID value for new or existing VLT host	Up to 255 characters, unique across all hosts
a	`mailboxID=`	ID value for new or existing VLT mailbox	Up to 255 characters, unique across all mailboxes
a	`type=`	If host or mailbox does not yet exist, comma-separated list of types of host to use	`ILexiCom.listHostTypes()[].getName()`
a	`alias=`	If host or mailbox does not yet exist, suggested value for new alias	Up to 50 characters, backslash character not allowed
b	`readonly=`	Comma-separated list of components that should be readonly	Host – host cannot be created or modified
b	`view=`	Comma-separated list of VLT UI components to show	Menubar Toolbar Tree Content Messages Statusbar
b	`toolbar=`	Comma-separated list of VLT toolbar buttons to show	Log Options Scheduler Router Certificates Transfers

Type	Parameter	Description	Values
b	`no=`	Comma-separated list of miscellaneous features/ components to hide	Scheduler – scheduler tool not shown Router – router tool not shown Boxes – inbox/outbox/sentbox/ receivedbox fields not shown Send+Receive – send+receive actions are not shown Collect – collect (and send+collect) actions not shown Release – release actions not shown

c	`auth=`	VLT web UI authentication. Edit/ view-only authentication request honored if hostID or mailboxID URL parameter also specified or if VLNavigator user groups have not been established for VersaLex.	`Edit;password="xxx"`
			or
			`View-only;password="xxx"`
			or
			`User;name="xxx";password="xxx"`

abc	`uiparms=`	Encrypted URL-encoded string containing any/all of the above parameters. Parameters can either appear directly in the URL or within the uiparms value.	URL-encoded string encrypted using `ILexiCom.encrypt()`.
			Pre-encrypted example:
			`hostID=p1&type=FTP%2FFTPs&`
			`alias=ACME&view=Content&`
			`no=Boxes%2CSend%2BReceive%2C`
			`Collect%2CRelease&`
			`auth=edit%3Bpassword%3D%22xxx%22`

abc	`reset=`	If this is not the first entry into VersaLex and a previous session already exists, indicates to reset the session using the parameters provided above. This parameter cannot be wrapped within the uiparms= parameter value.	True

All parameter names and values are case insensitive except for ID, alias, and password values.

Note: If a host or mailboxID is passed, Cleo Harmony is being integrated with another application's web UI and expects that application to display as a popup window. To distinguish hosts and mailboxes with ID associations, the tree node icon of a host or mailbox with an ID association will have a gray box around it. Host and mailbox IDs are stored in the host XML files and are retained on export/import of hosts.

To run Cleo VLNavigator from a web browser, you must enter the proper URL in the browser:

```
http(s)://VersaLexComputerIP:http(s)Port/VLNavigatorResourcePath
```

When Cleo VLNavigator logins are not in use (see **Require Logins** above), the web UI supports two password-protected modes:

view-only:	user can not modify any configuration data nor active hosts
edit:	fully-privileged user, like native UI user

The passwords are defined under the **Harmony** tab or **VLTrader** tab of the **Web Browser Service**.

While the web browser interface is active, you should not use the standard web browser refresh, back, and forward buttons. To force refresh, use the refresh button in the upper right-hand corner of the web UI. Instead of the back and forward buttons, navigate through the Cleo Harmony, , or windows as if you were using the native UI.

Do not attempt to have different tabs in the same browser session accessing multiple instances of the Cleo Harmony, , or application (or even the same instance in different tabs of the same browser session.) In this case, cached information can cause you to be directed to the incorrect session.

Creating active host subfolders

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

If a large number of hosts are going to be activated, it is advantageous to create host subfolders for groups of active hosts. Any structure of nested host subfolders – both depth and width – is allowed. This allows the tree pane as well as other dialogs (for example **Schedule**, **TCP/IP Port Usage**, **Transfer Report**) to show groupings of the active hosts rather than the entire, alphabetized list.

1. Click the **Active** tab in the tree pane.
2. Right-click the top Hosts folder or any host subfolder.
3. Click **New Folder** and rename the host subfolder to a meaningful name.
4. Click and drag any active hosts between host subfolders.

Searching for a host property value

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

1. Click the **Active** or **Templates** tab in the tree pane.
2. In the **Search** field, enter the property value you want to search for. Optionally, select **Match case**. Click **Search**.

   Note: Some right-click functions are not available while a Search is active.

3. Click **Clear** to remove the search results from the panel being viewed (**Active** or **Template**) and return to the original tree.

Watching messages

The **Messages** pane scrolls runtime messages for all actions and local hosts. For a description of the message types, see Messages Pane on page 16. The level of detailed messages shown in the messages pane can be configured. See Logs on page 892. If two or more actions are running concurrently, their messages will be intertwined.

1. Select a running *action* or *local host* in the tree pane.
2. Select the **Messages** tab in the content pane.

The Messages tab scrolls runtime messages for the selected *action* only. Other differences between the messages pane and the **Messages** tab include:

- During a file transfer, the **Messages** tab will continually reflect the current byte count and transfer rate.
- The **Messages** tab has no limit on the total number of messages it can contain.
- The contents of the **Messages** tab is retained until the next time the action is run, even if LexiCom is restarted.

Previous messages can also be viewed through the system log file. See Viewing log files on page 649.

Determining status

Status can be reviewed a number of different ways:

- The status bar will list which actions are running. Only one action within each activated host can be running at any given time.
- In the **Tree** pane, each *host\mailbox\ action* branch currently running is green.
- Select the **Hosts** folder in the **Tree** pane. The **Status** column in the **Content** pane table will indicate whether an action is running and the current command, and the file and byte count, when applicable.
- Select a running *action* in the **Tree** pane. The lower portion of the **Action** tab in the **Content** pane panel will indicate the current command, and the file and byte count, when applicable.

Controlling the program

This section provides information about various ways you can control your application.

Using the command line

You can use the command line to execute the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application and generate email, log reports, or transfer reports

Running from the command line

You can run the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application from the command line (absent a GUI) to do the following:

- Import and export hosts, certificates, and configurations
- Enable or disable one or more actions
- Run one or more actions
- Run as a service
- Modify properties
- Print current license and version information

Note:

- In Unix, the backward slash character (\) is a special escape character. To use the backward slash character in a host\mailbox\action path as shown below, use two backward slashes (\\) or more instead of one. An alternative is to just use the forward slash (/) instead of the backward slash (\). If, however, the actual host, mailbox, or action name has a forward slash in its name, use two forward slashes (//) in its place.
- Host actions are available only within the Cleo VLTrader and Cleo Harmony applications and, therefore, all references to *hostaction* should be ignored if you use the Cleo LexiCom application.
- Since the special characters, <, >, @, /, and \, can be used to construct a host, mailbox, action, or hostaction string, you should avoid using these characters in the actual name of any of these objects.

- Spaces are considered escape characters and can cause the program to be unable to read a path name with a space in it. If a path contains a space, enclose the string with two sets of double-quotes: `""C:\Cleo \work\New Folder""`
- Command line operations do cause extra system overhead. The system has to start up another JVM (Java Virtual Machine) as well as another copy of the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application. So, this startup process will use additional disk, memory, and CPU resources to run each command line. It might also use extra database resources depending on the command. The additional database connections are only active while the command line process is active. You should consider use of the API or web service to reduce the additional system overhead.

Using the command line

Run `Harmony`, `VLTrader`, or `LexiCom` from the command line.

```
Harmonyc [Import][Enable][Disable][Run][String]
```

```
VLTraderc [Import][Enable][Disable][Run][String]
```

```
LexiComc [Import][Enable][Disable][Run][String]
```

Note: Be sure to run `Harmonyc.exe`, `VLTraderc.exe`, or `LexiComc.exe` in the `Harmony`, `VLTrader`, or `LexiCom` home directory rather than `Harmony.exe`, `VLTrader.exe`, or `LexiCom.exe`.

Command options

General options

`-?`

Show command line options.

`-f "path"`

Process command line options specified in a file.

`-m`

Show all messages; default is `false`.

`-x`

Show error messages only; default is `false`.

`-l "path"`

Generate a log file; replaces existing log file.

`-b`

Export (back up) specified files and directories to a zip file.

Import options

Use the `-i` option to import a host from a file. You can use the `-e` and `-d` options with the `-i` option to enable and disable actions, respectively, after import.

`-i "path"`

Import host; replaces existing host. See Importing and activating a host on page 43.

-e "<*action*>*mailbox@host*"

-e "*host\mailbox\action*"

Enable action(s); * and ? are supported. See Enabling or disabling actions on page 43.

-d "*action*>*mailbox@host*"

-d "*host\mailbox\action*"

Disable action(s); * and ? are supported. See Enabling or disabling actions on page 43.

Export options

Use the -b command to export (back up) specified files and directories to a .zip file.

```
-b [-f "xmlFileFilter path"] -d "zip file path" -pp "passphrase"
```

-b

Export (back up) specified files and directories to a .zip file.

-f

Specifies the XML file filter on which to export. If unspecified, the entire configuration will be exported.

-d "zip file path"

Specifies the name of the .zip file that contains the backed-up files. If the file already exists, this action will replace the existing .zip file.

-pp

Passphrase used during export.

Run options

Use the -r option to run an action. You can use the -c and -t options with the -r option to replace existing commands and modify properties, respectively.

-r "<*action*>*mailbox@host*"

-r "*host\mailbox\action*"

Runs one or more actions; * and ? are supported. See Run actions on page 44.

-c "*command*"

Replaces existing commands. You can use the -c option mutliple times.

-t "<Host><*tag*>*value*"

-t "<Mailbox><*tag*>*value*"

-t "<Action><*tag*>*value*"

Modifies a property value. Specifies a host-, mailbox- or action-level property modification, the name of the property (*tag*) and the new value of the property. You can use the -t option mutliple times. See Supplying new property values while running actions on page 45

Modify options

Use the -p option to specify a host, mailbox, or action you want to modify without running an actions and use the -t option to specify the property within that host, mailbox or action you want to change and its new value. You can specify more than one -t option for each -p option.

For examples of how to use -p and -t together, see Supplying new property values without running actions on page 45.

-p "<*action*>*mailbox*@*host*"

-p "*hostmailbox**action*"**

-p "*host*/*mailbox*/*action*"

Specifies an action in a mailbox and host for which you want to modify properties.

-p "*hostservice*"**

Specifies a host and service for you which you want to modify properties.

-p "<*hostaction*>@*host*"

-p "*hosthostaction*"**

-p "*host*//*hostaction*"

Specifies a hostaction and host for which you want to modify properties.

-p "*standalone action*"

Specifies a standalone action for which you want to modify properties.

-t "<Host><*tag*>*value*"

-t "<Mailbox><*tag*>*value*"

-t "<Action><*tag*>*value*"

Specifies a host-, mailbox-, or action-level property modification, the name of the property (*tag*) and the new value of the property.

String options

-s "service"

Runs the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application as a service. See Running as a service on page 45.

-s "remote,target"

Runs the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application remotely. See Running as a service on page 45.

-s "license"

Displays license information. See Printing license information on page 46.

-s "version"

Displays version information. See Printing version information on page 47.

-s "service,stop"

Waits for ongoing transfers to complete and then stops the service.

-s "service,kill"

Stops the service immediately without waiting for ongoing transfers to complete.

-s "scheduler,start"

Starts the scheduler.

-s "scheduler,stop"

Stops the scheduler.

-s "router,start"

Starts the router.

-s "router,stop"

Stops the router.

`-s "transfers"`
Generates a transfer report. See Transfers on page 895.

Printing command line options

Print a list of command line options.

```
Harmonyc -?
```

```
VLTraderc -?
```

```
LexiComc -?
```

Printing messages

Print all messages (`-m`) while processing command line.

```
Harmonyc -m ...
```

```
VLTraderc -m ...
```

```
LexiComc -m ...
```

Print only error messages (`-x`) while processing command line

```
Harmonyc -x ...
```

```
VLTraderc -x ...
```

```
LexiComc -x ...
```

You can use either of these options with `-i`, `-e`, `-d`, `-r`, or `-s`.

You can increase your screen buffer width to ~160 characters to avoid message line wrapping.

Generating a log file

Generate a log file (`-l`) while processing a command line.

```
Harmonyc -l "path" ...
```

```
VLTraderc -l "path" ...
```

```
LexiComc -l "path" ...
```

You can use this option with `-i`, `-e`, `-d`, `-r`, or `-s`.

If the log file already exists, it is overwritten.

The system log file is not affected by this option.

Importing and activating a host

Import and activate a host (`-i`)

```
Harmonyc -i "path"
```

```
VLTraderc -i "path"
```

```
LexiComc -i "path"
```

path must point to a valid `.zip` file. The `.zip` should be structured to match the directory structure of Cleo Harmony, Cleo VLTrader, or Cleo LexiCom. If it is a just file in a `.zip`, it is placed in the appropriate home directory.

If the active host alias already exists, it is overwritten.

You can use the `-i` option to import patch files (usually in conjunction with `-m`):

```
Harmonyc -i "path_to_patch_file/0.1.zip"
```

The `-r` option can follow this option to run a newly imported host.

Enabling or disabling actions

Enable (`-e`) one or more actions.

```
Harmonyc -e "<action>mailbox@host"
```

```
Harmonyc -e "host\mailbox\action"
```

```
VLTraderc -e "<action>mailbox@host"
```

```
VLTraderc -e "host\mailbox\action"
```

```
LexiComc -e "<action>mailbox@host"
```

```
LexiComc -e "host\mailbox\action"
```

Disable (`-d`) one or more actions

```
Harmonyc -d "<action>mailbox@host"
```

```
Harmonyc -d "host\mailbox\action"
```

```
VLTraderc -d "<action>mailbox@host"
```

```
VLTraderc -d "host\mailbox\action"
```

```
LexiComc -d "<action>mailbox@host"
```

```
LexiComc -d "host\mailbox\action"
```

You can specify either action path format. You can use `*` and `?` to wildcard the path and possibly match more than one action. You can use `/` instead of a `\`.

You can specify a partial path (for example, "*host*" or "*host\mailbox*" or "*mailbox@host*") to enable or disable ALL actions within the path. `*` and `?` can also be used to wildcard the partial path.

Run actions

Run one or more actions (`-r`).

```
Harmonyc -r "<action> mailbox@host"
```

```
Harmonyc -r "host\mailbox\action"
```

```
VLTraderc -r "<action> mailbox@host"
```

```
VLTraderc -r "host\mailbox\action"
```

```
LexiComc -r "<action> mailbox@host"
```

```
LexiComc -r "host\mailbox\action"
```

You can specify either action path format. You can use `*` and `?` to wildcard the path and possibly match more than one action. You can use `/` instead of a `\`.

You can specify a partial path (for example, "*host*" or "*host\mailbox*" or "*mailbox@host*") to run ALL actions within the path. `*` and `?` can also be used to wildcard the partial path.

If more than one action is matched, the actions are run sequentially one-by-one.

See `sample.bat` in the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom home directory for an example.

Supplying new property values while running actions

Supply new property values while running one or more actions (`-r` with `-t`/ `-n`).

```
Harmonyc -r "<action>mailbox@host" -t "<Action><Commands>PUT ..." -n
"GET ..." ...
```

```
VLTraderc -r "<action>mailbox@host" -t "<Action><Commands>PUT ..." -n
"GET ..." ...
```

```
LexiComc -r "<action>mailbox@host" -t "<Action><Commands>PUT ..." -n
"GET ..." ...
```

The `-t` option specifies a host-, mailbox- or action-level property modification, the name of the property (*tag*) and the new value of the property. The property names correspond to the tagged values in the host XML file. See XML file formats on page 969 for information about the layout of a host XML file.

You can use the `-t` option mutliple times.

To specify a multi-line value, use `-t` to specify the first line, and then immediately following specify each remaining line with `-n` values.

More than one `-t` value (followed by `-n` values) can be specified to update multiple properties.

If more than one action is being run, the tagged values are applied to each action as it is run.

Supplying new property values without running actions

Supply new property values without running any actions (-p with -t/ -n).

```
Harmonyc -p "<action>mailbox@host" -t "<Action><Commands>PUT ..." -n
"GET ..." ...
```

```
VLTraderc -p "<action>mailbox@host" -t "<Action><Commands>PUT ..." -n
"GET ..." ...
```

```
LexiComc -p "<action>mailbox@host" -t "<Action><Commands>PUT ..." -n
"GET ..." ...
```

The `-t` option specifies a host-, mailbox- or action-level property modification, the name of the property (*tag*) and the new value of the property. The property names correspond to the tagged values in the host XML file. See XML file formats on page 969 for information about the layout of a host XML file.

You can use the `-t` option mutliple times.

To specify a multi-line value, use `-t` to specify the first line, and then immediately following specify each remaining line with `-n` values.

More than one `-t` value (followed by `-n` values) can be specified to update multiple properties.

Running as a service

Run the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application as a service (`-s`):

```
Harmonyc -s "service"
```

Running the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application as a service is identical to how they run when installed as a Windows service. Installing and running as a service has the following advantages:

- The service can run continuously. A user does not have to be logged into the computer to start the application. This is important for users wanting to schedule actions to run automatically. This is even more important for users who must have a local host always running listening for incoming messages.
- The GUI can still be started while the application is running as a service. When the GUI is exited, the service continues to run.
- Command line can also be used while the application is running as a service.

Running remotely

Run the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application remotely (`-s`):

```
Harmonyc –s “remote,target” ...
```

```
VLTraderc –s “remote,target” ...
```

```
LexiComc –s “remote,target” ...
```

This option can be used with `-e`, `-d`, or `-r`. The action paths specified with these options must exist within Cleo Harmony, Cleo VLTrader, or Cleo LexiCom on the target computer.

The target can be specified as a computer name or IP address. The Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application must be installed and/or running as a service (`-s “service”`) on the target server for the remote command to be accepted.

The `-l` option can be used to generate a local log file.

This option only requires a license on the target computer.

Printing license information

Print current license information (`-s`):

```
Harmonyc –s “license”
```

```
VLTraderc –s “license”
```

```
LexiComc –s “license”
```

This will generate output similar to the following:

```
 License Key                 = eb]|-y{8R-LyLo-GGjd-M{42-GkE4-QI7B-mqL^
License Owner               = Cleo Communications
Serial Number               = LX9012
Host ID                     = LO6354
Key Expires                 = 2003/01/08 (evaluation)
Max # of Hosts              = Unlimited
Max # of Mailboxes per Host = 5
Translator Integration      = Yes
AS2                         = Yes
FTP                         = Yes
FTP/S                       = Yes
```

```
HTTP                          = Yes
HTTP/S                        = Yes
API                           = Yes
```

Printing version information

Print current version information (`-s`).

```
Harmonyc -s "version"
```

```
VLTraderc -s "version"
```

```
LexiComc -s "version"
```

This will generate output similar to the following:

```
 Version = 2.0.03
 2002/05/08 07:48:28 CDT   as2bean.jar
 2002/04/29 16:31:22 CDT   dcebmxhttpsbean.jar
 2002/05/09 09:48:54 CDT   ftp.jar
 2002/05/09 09:48:58 CDT   ftps.jar
 2002/05/06 16:57:26 CDT   httpbean.jar
 2002/04/26 16:37:54 CDT   HTTPClient.jar
 2002/05/06 16:57:30 CDT   httpsbean.jar
 2002/05/06 16:57:20 CDT   lexbean.jar
 2002/05/08 09:53:38 CDT   LexiCom.jar
```

Processing command line options from a file

Process command line options specified in a file (`-f`) .

```
Harmonyc -f "path"
```

```
VLTraderc -f "path"
```

```
LexiComc -f "path"
```

And an example file:

```
 -m
-l log.xml
-i "hosts\preconfigured\ABC VAN.xml"
-r "ABC VAN\myMailbox\send+receive"
-t "<Host><Inbox>G:\edi\in\"
-t "<Host><Outbox>G:\edi\out\"
-c "CONNECT user=test,*pswd=test"
-c "PUT -DEL .\ receiver=EDI,type=X12"
-c "GET -DIR -CON -UNI .\[type]=X12"
```

The contents the file can contain any of the other command line options besides `-f`. Within the file, arguments can be separated by spaces and/or exist on separate lines.

Importing files

Import a file originally exported from the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application:

```
VersaLexc -i VersaLexConfig.zip -pp cleocleo -cp keypswd1 -cp keypswd2 -m
```

where:

`-i VersaLexConfig.zip`

Import the file, `VersaLexConfig.zip`.

`-pp cleocleo`

Specifies that `cleocleo` is the passphrase used when the data was exported.

`-cp cleo -cp keypswd1 -cp keypswd2`

Provides certificate private key passwords the system attempts to use in rotation until one matches.

Generating an operator audit trail report from the command line

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

You can use `VLTraderc` or `Harmonyc` from the command line to generate an Operator Audit Trail report that is either:

- Stored in an HTML file
- Stored in a CSV file
- E-mailed to a list of users

You can use operating system features to schedule a report to be automatically generated at a certain time.

```
Harmonyc -s OpAudit [-f xmlFilterFile] [-d destination] [-t title]
```

```
VLTraderc -s OpAudit [-f xmlFilterFile] [-d destination] [-t title]
```

`-s OpAudit`

Generates an Operator Audit Trail report.

`-f xmlFilterFile`

Uses the file, *xmlFilterFile*, to set the Operator Audit Trail Filter settings. You can save a filter using **Save As** in the Operator Audit Trail Filter dialog box. See Operator Audit Trail on page 933. If the `-f` option is not present on the command line, only the current days operator audit trail events will be in the report.

`-d destination`

Outputs the Operator Audit Trail report to the *destination* (HTML file, CVS file, or email addresses) you specify. Specifies an HTML file, CVS file, or email as the *destination* for the Operator Audit Trail report. If the filename has a `.csv` extension, the file is output as a comma-separated values (CSV) formatted file. If the *destination* contains an `@` symbol, it is assumed to be an email address. If you want to specify a list of email addresses, use commas to separate them. If the `-d` option is not present, the results will be displayed in CSV format to the console.

`-t title`

Appends *title* to the HTML report title and the email subject if applicable. If the *title* contains whitespace, enclose it within double-quotes, for example:

```
"title with whitespace"
```

Generating a log report from the command line

`LexLogc` or `VLLogc` can be used from the command line to generate a report that is either stored in an HTML file, or e-mailed to a list of users.

Use this feature to schedule a report to be automatically generated at a certain time.

```
LexLogc [-?] [-f xmlFilterFile] [-d destination] [-t title]
```

```
VLLogc [-?] [-f xmlFilterFile] [-d destination] [-t title]
```

-?

Displays the command line options

-f *xmlFilterFile*

Uses the file specified by *xmlFilterFile* to set the Log Report Filter settings. You can save a filter using **Save As…** in the **View the Log File** dialog box. If the `-f` option is not present on the command line, only the current day's log is included in the report.

-d *destination*

Outputs the log report (in an HTML format) to the *destination* (a file or list of email addresses) you specify. You can specify a list of comma-separated email addresses. If the *destination* value you specify contains an `@` symbol, the parameter is assumed to be an e-mail address. If the `-d` option is not present, the results are printed to the console.

-t *title*

Appends *title* to the HTML report title and the email subject if applicable. If the *title* contains whitespace, enclose it within double-quotes, for example:

```
"title with whitespace"
```

Generating email from the command line

Use the `LexMailc` or `VLMailc` command to generate email from the command line.

```
LexMailc [-?] -a addresses -r sender [-e emailserver]
         [-u username] [-p password] [-s subject]
         [-m txtmsg|-t textfile|-f attachments
```

```
VLMailc [-?] -a addresses -r sender [-e emailserver]
         [-u username] [-p password] [-s subject]
         [-m txtmsg|-t textfile|-f attachments
```

-?

Displays the command line options

-a *addresses*

Required. Comma-separated list of email recipients.

-r *sender*

Required. Email address of the sender.

-e *emailserver*

Optional. SMTP email server to use for sending the message.

-u *username*

Optional. SMTP email server authentication username.

-p *password*

Optional. SMTP email server authentication password.

-s *subject*

Optional. Subject of the message.

Although the following options are not required, you must specify at least one:

-m *textmsg*

Free-form text to include in the body of the message.

-t *textfile*

Path of the file containing text to include in the body of the message.

-f *attachments*

Comma-separated list of paths to files to be attached to the message.

Generating a transfer report from command line

Note: This section applies to Cleo Harmony and Cleo VLTrader only.

Use the `VLStatc` from the command line to generate a transfer report that is either stored in an HTML file or e-mailed to a list of users.

This feature allows a user to schedule a report to be automatically generated at a certain time.

```
VLStatc [-f xmlFilterFile] [-d destination] [-t title]
```

-?

Displays the command line options

-f *xmlFilterFile*

Uses the file specified by "xmlFilterFile" to set the Transfer Report Filter settings. You can save a filter using **Save As…** in the **Transfer Status Filter** dialog box. If the `-f` option is not present on the command line, only the current day's transfers will be in the report.

-d *destination*

Outputs the transfer report (in an HTML format) to the *destination* (a file or list of email addresses). If the *destination* contains an `@` symbol, it is assumed to be an e-mail address. If you specify multiple email addresses, use commas to separate them. If the `-d` option is not present, the results are displayed in the product UI.

-t *title*

Appends *title* to the HTML report title and the email subject, if applicable. If the *title* contains whitespace, enclose it within double-quotes, for example:

```
"title with whitespace"
```

Using Autorun

As an alternative to remotely running Cleo LexiCom commands using the command line `-s "remote,server"` option, the autorun feature can be used to automatically process **command** files when they appear in a specific directory. Autorun commands are identical to the options available when executing Cleo LexiCom from the command line except for `-m`, `-e`, and `-s`. See Running from the command line on page 38. In fact, the syntax of the **command** file matches the syntax of the `-f path` command line option. This feature is different from just executing

Cleo LexiCom with command line options because the Cleo LexiCom commands can be generated from a different computer than one on which the Cleo LexiCom software is actually running.

The autorun feature does not need to be specifically enabled. As long as the Cleo LexiCom software is running (either the GUI or `-s service`), the feature is on. You can modify the default `autorun\` directory. See Other system options on page 729. No special naming convention is required for the **command** files. A **command** file is deleted when Cleo LexiCom finishes processing the commands. Only one **command** file is processed at a time.

Auto starting the VersaLex daemon in UNIX environments

Warning: The following procedures have been tested with specific distributions of Solaris snd Linux; consult your system documentation to ensure that these steps are correct before starting. Review the run levels (rc#.d) and sequence numbers (S# and K#) given for appropriate values. Only the system administrator should perform these changes.

Note: This section applies to Cleo Harmony and Cleo VLTrader only.

Note: This section contains numerous command line examples referring to `VersaLex`, `VersaLexc`, and `VersaLexd`. Please substitute *VersaLex* with your specific product name (either `VLTrader`, or `Harmony`). For example, `VersaLexd` in practice becomes either `VLTraderd`, or `Harmonyd`.

Note: Prior to starting VersaLex as a UNIX daemon, you can verify that VersaLex is operational using the following command from the directory where VersaLex is installed:

```
./  VersaLex c -s "service" -m
```

Starting as a daemon on Solaris

1. Log in as root.
2. Change to the directory where Cleo Harmony is installed.
3. Verify that the *HRMHOME* or *VLTHOME* variable in the `VersaLexd` script points to the directory where Cleo Harmony is installed.
4. Copy the `VersaLexd` script to the startup/shutdown scripts directory:

   ```
   cp  VersaLex  d /etc/init.d/ .
   ```

5. Create a symbolic link to start the Cleo Harmony application:

   ```
   ln -s /etc/init.d/VersaLexd /etc/rc3.d/S98VersaLexd
   ```

6. Create a symbolic link to stop the Cleo Harmony application:

   ```
   ln -s /etc/init.d/VersaLexd /etc/rc2.d/K98VersaLexd
   ```

7. Log out and reboot your system.
8. After you reboot, display the Cleo Harmony GUI. Change to the directory where Cleo Harmony is installed and run:

   ```
   ./VersaLex
   ```

Running as a daemon on Linux

1. Log in as root.
2. Change to the Cleo Harmony installed directory.
3. Verify the *LEXHOME* or *VLTHOME* variable in the `VersaLexd` script points to the Cleo Harmony installed directory.
4. Copy the `VersaLexd` script to the startup/shutdown scripts directory:

```
cp VersaLexd /etc/rc.d/init.d/ .
```

5. Create a symbolic link to start the Cleo Harmony application.

```
ln -s /etc/rc.d/init.d/VersaLexd /etc/rc.d/rc5.d/S98VersaLexd
```

6. Create a symbolic link to stop the Cleo Harmony application:

```
ln -s /etc/rc.d/init.d/VersaLexd /etc/rc.d/rc4.d/K98VersaLexd
```

7. Log out and reboot your system.
8. After you reboot, display the Cleo Harmony GUI. Change to the directory where Cleo Harmony is installed:

```
./VersaLex
```

Starting as a daemon on systemd

1. Log in as root.
2. Change to the installed directory.
3. Create a unit file in /etc/systemd/system/VersaLexd.service. The values you use in your unit file will vary depending on whether the Log errors and warnings in System Event/Syslog File option is enabled. See Logs for information about this option.

   If the **Log errors and warnings in System Event/Syslog File** option is not enabled, use the following:

```
[Unit]
Description=Start VersaLex daemon

[Service]
Type=oneshot
ExecStart=/versalex/versalexd start
ExecStop=/versalex/versalexd stop
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

   If the Log errors and warnings in System Event/Syslog File option is enabled, use the following:

```
[Unit]
Description=Start VersaLex daemon

[Service]
Type=simple
ExecStart=/root/Harmony/Harmonyc -s service
ExecStop=/root/Harmony/Harmonyc -s service,stop

[Install]
```

```
WantedBy=multi-user.target
```

4. If stdout and stderr are not already being sent to journald, include the following in your unit file in the `[Service]` section:

```
StandardOutput=journal
StandardError=journal
```

5. Run `systemctl enable VersaLexd.service`
6. Verify the *HRMHOME* or *VLTHOME* variable in the `VersaLexd` script points to the installed directory.
7. Log out and reboot your system.
8. Verify is active.

Entropy and Linux systems

Java uses random numbers when encrypting data. In Linux, they are pulled from `/dev/random`, which is populated by interactions with the computer (mouse movement, keyboard presses, etc). With a Linux headless system (no interactive UI), these interactions rarely happen, which means it is more likely the Cleo Java processes will use up all the random numbers in `/dev/random`. In this case, calls to get a random number are blocked until there are more random numbers available and the overall effect is that the Linux machine will run slowly.

The `rngd` utility uses `/dev/urandom` to help seed `/dev/random` and keep it populated even when using many random numbers.

To check available entropy, use the following command:

```
cat /proc/sys/kernel/random/entropy_avail
```

RedHat 6/CentOS 6

Use rngd to create entropy for RedHat 6/CentOS 6 systems:

Install rngd if not already present

```
yum -y install rng-tools
```

Run the following command and edit the file as shown:

```
nano /etc/sysconfig/rngd

    #include the following statement to feed urandom from random every 5
 seconds
     EXTRAOPTIONS="-r /dev/urandom -o /dev/random -t 5"

service rngd
start chkconfig rngd on
```

RedHat 7/CentOS 7

Use `rngd` to create entropy for RedHat 7/CentOS 7 systems. Install `rngd` if not already present.

```
yum -y install rng-tools
```

Run the following command to create service file:

```
systemctl start rngd
```

Run the following command and edit the file as shown:

```
nano /usr/lib/systemd/system/rngd.service

    #add the following statement
     ExecStart=/sbin/rngd -f -r /dev/urandom

systemctl daemon-reload
systemctl start rngd
systemctl status rngd
```

Ubuntu Linux

Use `rngd` to create entropy for Ubuntu Linux systems. Install `rngd-tools` if not already present.

```
sudo apt-get install rng-tools
```

Run the following command and edit the file as shown:

```
sudo nano /etc/default/rng-tools
    #add the following statement
     HRNGDEVICE=/dev/urandom
sudo /etc/init.d/rng-tools restart
```

Using a Custom Splash Screen

Note: This applies to Cleo Harmony, Cleo VLTrader systems only.

- You can place a custom GUI splash screen in the `conf/images` directory in the Cleo Harmony home directory. The filename must start with `splash.` (the word *splash* followed by a period). Supported formats include JPEG, GIF, and PNG. The image can be no larger than 525X340 pixels and no smaller than 250X100 pixels.
- You can place a custom Cleo VLPortal splash screen in the `webserver/VAADIN/cleo/images/custom` directory. The filename must start with `splash.` (the word *splash* followed by a period). Supported formats include JPEG, GIF, and PNG. The image can be no larger than 525X340 pixels and no smaller than 250X100 pixels.

System Configuration

This section contains information about configuring your Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application.

Monitoring source deletion

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

When transfer logging is enabled (see Transfers on page 895), the source deletion monitoring feature is active. While this feature is active, any files that fail to be deleted as part of a `PUT -DEL` command in an action are

added to a monitoring list. Once monitored, they have a status of `Delete Error` in the transfer report. In addition, these files are skipped if an action attempts to resend them. Finally, an hourly cleanup task attempts to remove these files. Once a file is successfully removed, or if it is deleted manually, its status is set to `Delete Resolved` and it is removed from the monitoring list.

If a source deletion error occurs for an action being run by the scheduler and transfer logging is disabled, the action is disabled by the scheduler. To resolve this problem, manually delete the file and restart the schedule. To avoid disabling actions in the future, enable transfer logging and restart the schedule.

Configuring password policies

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

You can define a **Password Policy** that enforces password security requirements for any or all Local User mailboxes. To enforce a global password policy, go to **System Options** > **Other** tab in the native UI or **Administration** > **System** > **Other** in the web UI, and then select the **Enforce Password Policy** check box in the Property/Value list. This allows you to enable, disable, or override password policies for a particular local user host (FTP, HTTP, and SSH FTP) or Users host so that all underlying mailboxes operate with separate security restrictions.

To configure the password policy, after selecting the **Enforce Password Policy** check box, click **Configure** to display the **Password Policy** dialog box. Set values as required and click **OK**.

The default **Password Policy** settings are:

- **Minimum Password Length** enforces the minimum number of characters a password must contain. (The length can range from 1-24 characters)
- **Password Cannot Contain User Name** enforces that the user name (that is, the mailbox alias) cannot be part of the password specified in upper, lower, or mixed case.
- **Require Mixed Case** enforces the minimum number of upper and lowercase characters that a password must contain.
- **Require Numeric Characters** enforces the minimum number of numeric characters a password must contain (digits 0-9).
- **Require Special Characters** enforces the minimum number of special characters a password must contain (for example `@$%^&*!`).
- **Prevent Password Repetition** requires that a different password be used until the **Number of Passwords Before Repeats Allowed** value has been exceeded.
- When the **Enable Password Expiration** setting is selected, user passwords will expire after the specified number of days. The commonly used number of days is included in the drop-down list; however, a valid custom value can be entered instead.
- When the **Require password reset before first use** setting is selected, the user is required to update their password before being able to fully log in if a new mailbox is created under the host or the user's password is changed from the administrator console. There are provisions through FTP, interactive SFTP, and Portal to allow the password to be updated. This setting only applies to native users.
- If **Lock out user** is enabled, a user who fails to enter the correct password after **failed logon attempts** times within the specified number of **seconds** is locked out of the mailbox for the specified number of **minutes**. If the minutes are not specified (that is, the field is left blank), the user is locked out until the user's mailbox is unlocked manually by the Cleo VLTrader or Cleo Harmony user. Refer to the specific local user mailbox (FTP, HTTP, and SSH FTP) for further information.
- If **Allow User Groups to override policy** is enabled, a given User Group will be able to set different password security requirements for that particular group.

Note: All configured security settings except **Enable Password Expiration** and **Lock out user** are enforced at the time the user changes their password.

Setting up a GEGXS IBC dial-up connection (Windows users only)

In order to use GEGXS IBC dial-up connections, the GEGXS IBC dialer program must be installed.

The GEGXS IBC dialer provides a connection to the GEIO global dial-PPP network; therefore, the dialer can only be used to connect to GE hubs – GE Tradanet, GE EDI*Express, and GE ICS. In fact, the dialer must to be used to connect to these sites, as they cannot (as of yet) be accessed via the Internet.

After the IBC dialer is installed, you need to update its properties.

1. Select **Configure** > **GEGXS IBC Dial-Up** > **Properties** in the menu bar.
2. At a minimum, select one phone number and a modem, if necessary, and click **OK**.
3. Next, test to see if you can get a connection. Select **Configure** > **GEGXS IBC Dial-Up** > **Connect** in the menu bar.
4. Enter the username and password for one of your GEGXS IBC dialer accounts, click **Save password** if necessary, and click **Connect**. The connection status area echoes the connection steps, and on failure, indicates the reason for the error. If needed, try different phone numbers within your area code. On success, the dialog disappears and a GEGXS icon appears in the system tray.
5. Select **Configure** > **GEGXS IBC Dial-Up** > **Disconnect** in the menu bar.
6. If you will only be using one GEGXS IBC dialer account, configuration is complete because each GE host is pre-configured to automatically use GEGXS IBC dial-up. If you will be accessing more than one GE host using different GEGXS IBC dialer accounts, then one-by-one for each GE host:
   a) Select the GE *host* in the tree pane.
   b) b. Select the **General** tab in the content pane panel.
   c) c. The Connection Type should already be **GEGXS IBC Dial-Up Connection**.
   d) d. Enter the username and password for the GEGXS IBC account specific to this site.

   If once you get a connection, your commands “hang” or drop-off unrepentantly, try different phone numbers within your area code.

Setting up a dial-up connection (Windows users only)

Note: In order to use dial-up connections, the Cleo LexiCom dialer program must be installed.

1. If all of your active hosts will be dial-up, change the Default Connection Type to **Dial-Up Connection** - see Specifying default host directories on page 700.
2. If all of your dial-up hosts will be using the same phonebook entry, set the Default Phonebook Entry. See Specifying default host directories on page 700 .
3. If only a portion of your active hosts will be dial-up or different phonebook entries will be used for your different dial-up hosts, then one-by-one for each dial-up host:
   a) Select the dial-up *host* in the tree pane.
   b) Select the **General** tab in the content pane panel.
   c) Change the Connection Type to **Dial-Up Connection** if the System Default is **Direct Internet Access or VPN**.
   d) Enter the Phonebook Entry if the System Default is not the desired entry. Click **Select** to have the Cleo Harmony application display a selection list.
4. Select the desired phonebook entry and click **OK**.

5. If an appropriate phonebook entry does not exist, it must be added outside of the Cleo Harmony application using the dial-up networking options within Windows. For information on how to configure phonebooks and phonebook entries, etc., contact your ISP or see www.microsoft.com.
6. Click **Apply**.

Setting up a LexiCom dial-up connection (Windows users only)

In order to use Cleo LexiCom dial-up connections, the Cleo LexiCom dialer program must be installed.

If all of your active hosts will be dial-up, change the Default Connection Type to **LexiCom Dial-Up Connection** – see Specifying default host directories on page 700.

If all of your dial-up hosts will be using the same phonebook entry, set the Default Phonebook Entry – see Specifying default host directories on page 700.

If only a portion of your active hosts will be Cleo LexiCom dial-up or different phonebook entries will be used for your different Cleo LexiCom dial-up hosts, then one-by-one for each LexiCom dial-up host:

1. Select the dial-up *host* in the tree pane.
2. Select the **General** tab in the content pane panel.
3. Change the Connection Type to **LexiCom Dial-Up Connection** if the System Default is **Direct Internet Access or VPN**.
4. Enter the Phonebook Entry if the System Default is not the desired entry. Click **Select** to have Cleo LexiCom display a selection list.
5. Select the desired phonebook entry and click **OK**.

   If an appropriate phonebook entry does not exist, it must be added outside of Cleo LexiCom using the dial-up networking options within Windows. For information on how to configure phonebooks and phonebook entries, etc., contact your ISP or please see www.microsoft.com.
6. Click **Apply**.

Configuring email or execute based on results

You can configure the Cleo Harmony application to generate an email based on the results of an action or a host action:

- on any type of failure and/or
- on each successful send of a file and/or
- on each successful receive of a file and/or
- on each successful copy of a file using `LCOPY` or
- on overall conditions being met for a `CHECK` command (and Cleo Harmony applications only) or
- on overall conditions not being met for a `CHECK` command (VLTrader and Harmony only).

Similarly, you can also configure the Cleo Harmony application to execute a program, script, or operating system command based on the results of an action or a host action. The syntax and rules for execute-on commands are the same as those for the `SYSTEM` commands (see Using operating system commands in actions on page 93), with the following differences:

- The word `SYSTEM` is not used within the execute-on string.
- When using macro variables, the `Execute-On` context is used rather than the `SYSTEM` command context.

Below are some `Execute-on` command examples:

Operating System	Cleo Harmony Execute-On command
Windows	`command.com /c copy x y`
Windows	`cmd.exe /c copy x y`
Windows	`[SuccessCodes=0-1,255] cmd.exe /c copy x y`
Unix	`cp x y`

Additionally, selected action commands can also be used in **Execute-On** fields. `PUT` and `GET` action commands are not available for use in Execute-On. Directory listings (`LS` and `DIR` commands) are not available for use in Execute-On for FTP protocols. To specify an action command in an Execute-On setting, the command must be preceded with the '$' character. The additional character is to differentiate an action command script from an existing operating system command with the same name. The **Wait for Execute On** Advanced option is ignored when a `SCRIPT` command is executed. See SCRIPT Command. Execute-On will always wait for the JavaScript to complete. If needed, new threads may be created within JavaScript which would allow the executed script to return while further processing continues in the new thread. This logic also applies to any other action commands allowed in Execute-On. For instance, to use the local action command `LCOPY` (instead of the operating system copy command) use the following syntax in the **Execute-On** field:

```
$LCOPY x y
```

A list of multiple commands which may be either all operating system commands or the supported action commands may also be specified. The commands must be separated by either '&' or '&&' characters. When '&' is used all commands will execute sequentially regardless of the status of the previous command. For example, two `LCOPY` commands in the Execute-On field could be specified as:

```
$LCOPY x y & LCOPY a b
```

where the second `LCOPY` executes regardless of the status of the first `LCOPY`. When '&&' commands is used a command will execute if the previous command does not result in an error. For example in:

```
$LCOPY x y  && LCOPY a b
```

the second `LCOPY` will execute only if the first `LCOPY` does not result in an error. For operating system commands, the '&' and '&&' operator functionality is dependent on the operating system or shell being used.

To set the email and execute properties for all hosts at the system level, refer to Advanced system options on page 743.

To set the email and execute properties for a specific host, see Setting advanced host properties on page 89.

Note: A property value given at the host level overrides a system level value.

Generating files for an integration

The translator file generation assumes that the incoming file will be called **recvfile.edi** and the outgoing file will be called **sendfile.edi**. If the input/output file names differ from these, the user must manually update the files generated.

Hosts should already be activated and set up prior to running the translator file generation.

If host, mailbox, or action alias names are changed, the user will have to re-generate the translator files.

Generating integration files deletes the last set of files generated.

1. Translator Selection: Select **Configure** > **Integration** in the menu bar. (**Note**: If you are running with an AS/400 without translator integration, then the following panel will not be displayed. Proceed to **Host Selection** section below).
2. Select the translator from the Translator pull-down. If it is not listed, then enter the name of the translator. (**Note**: If a name is entered, then generic translator files will be generated).
3. If the Platform is not dimmed, select the platform for which you are generating script files.
4. Enter the directory path of the translator selected. You may also use the **...** button to browse to that directory.
5. Click **Generate Translator Files...** to begin the process of selecting hosts or actions for which you wish to generate translator files.
6. If GXS Application Integrator is the translator chosen, a Hosts selection panel, is displayed. Reference the GXS Application Integrator guide to proceed with this translator integration. For other translator integrations, continue using the following steps with the **Host Actions** dialog box.
7. Select the actions for which you want to generate script files. (**Note**: All files will be re-generated. Files previously generated and not selected will be deleted. For AS/400, another column will be shown where the user can name the CL-file)
8. Enter the **Script Location** where the scripts should be generated. (**Note**: For certain translators, additional files are generated into the **Translator Location** or one of its sub-directories).
9. Click **Generate** to begin generation of the translator files.

   Most translators require additional steps to be able to use these files.

Activating TradeLink communications agent service

Note: This section applies to TradeLink users only.

SoftCare TradeLink ebusiness community management software and manages electronic business document processes internally and among trading communities. TradeLink integrates with its various agent modules via the web service (SOAP/HTTP) protocol and uses the Cleo Harmony web service for trading partner communications.

1. Select the Web Service *service* under the Local Listener *local host* node in the active tree pane.
2. Click ☑ **Enabled**.
3. Enter the TradeLink database driver string, connection string (that is, URL), and username/password. If you are not sure of these values, contact the TradeLink system administrator.
4. Select **Allow web access to logs\ directory** if you require access to Cleo Harmony log files from within TradeLink.
5. Select **Apply**. The TradeLink communications agent service is now active.

The Cleo Harmony application supports the TradeLink compressed content option. For outgoing content, nothing needs to be configured. But for incoming content, the `TradeLink.compression.file.size.threshold` system property, if present, is used to determine whether the incoming content should be compressed (the property value is expressed in bytes). To set this property in the web UI, go to **Administration** > **System** > **Bootstrap** or in the native UI, go to **Configure** > **Launcher** (see Bootstrap configuration on page 728) and add `-DTradeLink.compression.file.size.threshold=...` to the Windows Service Other settings (or Command Line if Unix) and restarting the service (daemon).

Using macro variables

A macro variable is a string enclosed in a set of percent signs (e.g., %inbox%), used to indicate substitution of other data. You can use macros for many reasons, including, for example, defining a unique file destination,

indirectly referencing directory locations (for inboxes, outboxes, etc.), or passing information to an `Execute On Successful Send` command.

Types of macro variables

Macro variables are classified in one of three ways:

- **Reserved Macro Variables**: Variables that are predefined within the Cleo Harmony product. See the table below.
- **Custom Directory Macro Variables**: Directory variables that are defined by the Cleo Harmony user. You use directory macro variables to specify host directories. See Specifying default host directories on page 700.
- **Custom Macro Variables Defined as System Properties**: Variables that are defined as `name=value` pairs using the Java `-D` Command Line parameters (see Bootstrap configuration on page 728 for further information) or are specified in the `conf/system.properties` file. Note that Custom Macro Variables are resolved after Reserved Macro and Custom Directory Macro Variables and therefore cannot be used to override those variables.

The following table outlines the macro variables (both reserved and custom) and the various contexts in which they can be used.

Table 1: Macro Variables and their Contexts

Macro Variable	Context													
	Source File	Destination Files	SYSTEM Command	Default Host Directory	Default Local User Archive Directory	Default Root Directory	Windows/ Unix Folders	Custom Variable	Execute-On	Pre/Post Command	LCOPY Archive	Accessible through API	Directories Only	Banner/ Welcome Message
%system%				X	X									
%none%				X	X									
%inbox%	X	X	X					X	***X***		X	X	***X***	
%outbox%	X	X	X					X	***X***		X	X	***X***	
%file%									***X***			X		
%sourcefile%		***X***							***X***	X		X		
%srcfile%		***X***							***X***	X		X		
%sourcefilebase%		***X***							***X***	X		X		
%srcfilebase%		***X***							***X***	X		X		
%sourcefileext%		***X***							***X***	X		X		
%srcfileext%		***X***							***X***	X		X		
%destfile%									X	X		X		
%destfilebase%									X	X		X		
%destfileext%									X	X		X		
%date%	X	X	X	X	X				X	X		X		X
%time%	X	X	X						X	X		X		X
%index%	X	X	X						X	X		X		
%host%	X	X	X	X	X				X	X	X	X		
%mailbox%	X	X	X	X	X				X	X	X	X		
%status%									X			X		
%crc%									***X***			X		
%filesize%									***X***			X		
%transferid%		***X***							***X***			X		
%resttransferid%		***X***							***X***			X		

Macro Variable	Context													
	Source File	Destination Files	SYSTEM Command	Default Host Directory	Default Local User Archive Directory	Default Root Directory	Windows/ Unix Folders	Custom Variable	Execute-On	Pre/Post Command	LCOPY Archive	Accessible through API	Directories Only	Banner/ Welcome Message
%filesin%			X									X		
%filesout%			X									X		
%ebms.timestamp.date%		***X***												
%ebms.timestamp.time%		***X***												
%ebms.action%		***X***												
%ebms.service%		***X***												
%ebms.cpaid%		***X***												
%as2.to%		***X***												
%as2.from%		***X***												
%as2.subject%		***X***												
%oftp.sfiddsn%		***X***												
%oftp.sfidorig%		***X***												
%oftp.sfiddest%		***X***												
%oftp.sfiddesc%		***X***												
%as3.to%			X											
%as3.from%			X											
%ebics.ordertype%		X												
%command%									***X***			X		
custom directory variable	X	X	X	X	X	X	X		X		X	X	X	
system.properties variable	X	X	X	X	X	X	X		X		X	X	X	

Note: Cells with a bolded, italicized, underscored ***X*** indicate the value might not be known. If the value is not known, the macro name (for example, `%sourcefile%`) is simply passed through. Further, if a macro is used that is not supported within a particular context (for example, referencing `%crc%` within a Destination File context), it will simply be passed through as well.

Using `system.properties` Variables

It is possible to add general variables to the `conf/system.properties` file and use them within the contexts outlined in the table. To add a general variable to `conf/system.properties`, the syntax is: `varName=replacementText`. For example, if `conf/system.properties` has the following: `myvar=hello`, the usage would be `%myvar%` in the desired location.

Note:

1. Unlike other macro variables that are case-insensitive, `system.properties` macros are case-sensitive.
2. After adding a macro to `conf/system.properties`, the service must be cycled before the macro can be processed.

Context Definitions

Macro variables are valid in certain contexts. The following describes the various contexts in which macro variables are valid. Not all macro variables are valid in all contexts.

Source File

Applies to the "source" values of `LCOPY`, `LDELETE`, `LREPLACE`, `PUT`, and `CHECK` commands (Cleo Harmony and Cleo VLTrader applications only). Macros are also supported for the HTTP "filename" parameter and the "source" values of the `GET` commands for FTP, SFTP, and HTTP protocols only. Macros are not supported for the "source" values of `GET` commands for other protocols or the `DIR` command.

Destination File

Applies to the "destination" values of `LCOPY`, `PUT`, `GET`, and `CHECK` commands (Cleo Harmony and Cleo VLTrader applications only). It also applies to default file names, as specified under the host **AS2** tab (see AS2 Host: AS2 Tab on page 149), the host **AS4** tab (see AS4 Host: AS4 Tab on page 204), the host **ebXML** tab (see ebXML Host: ebXML Tab on page 233), the host EBICS tab (see EBICS Host: EBICS Tab on page 472), and the Local HTTP Users HTTP tab (see Configuring access for HTTP host users on page 835). It also applies to the file destination, as specified under the host **OFTP** tab (see OFTP Host: OFTP Tab on page 290). The Destination File context also applies to macros that can be included within HTTP parameter/header values, as defined under the HTTP tabs for HTTP-based protocols (for example, AS2, ebXML). Also, this context applies to the `FileFormat` parameter on EBICS `GET` command. See EBICS Command Reference on page 489. The Destination File context macro variables may also be used within the Subject header of the SMTP tab. Note that macros such as `%sourcefile%` and `%transferid%` really only make sense for the file name—not the file path. However, macros such as `%mailbox%` could make sense as part of the path.

SYSTEM Command

Applies to the `SYSTEM` command that can be run within the host actions (see Using operating system commands in actions on page 93).

Default Directories

Applies to the default inbox/outbox/sentbox/receivedbox, as specified under the host General tabs (for an example, see FTP Configuration on page 95). The `%host%` macro variable is supported, but not `%mailbox%`.

In addition, the `%date%` macro is supported, but the `%time%` macro is not. Be careful using the `%date%` macro in the default outbox because files in the date-stamped outbox subdirectory will not be sent if the send action occurs after midnight. Likewise, archiving entries in sentbox and receivedbox date-stamped directories will only occur for the current date.

Default Local User Archive Directories

Applies to the sentbox and receivedbox archive directories as specified under the local user host General tabs (for an example, refer to Configuring local FTP users on page 809). Both the `%host%` and `%mailbox%` macro variables are supported in this context.

In addition, the `%date%` macro is supported, but the `%time%` macro is not. Be advised that archiving entries in sentbox archive and receivedbox archive date-stamped directories will only occur for the current date.

Default Root Directory

Applies to the default root directory, as specified under the local user FTP tab, HTTP tab, and SSH FTP tab (for an example, refer to Configuring local FTP users on page 809). It also applies to the user home directory, as specified under the local user mailbox FTP tab, HTTP tab, and SSH FTP tab (for an example, see FTP Mailbox: FTP Tab on page 112).

Windows/Unix Folders

Applies to the UNC paths specified when you set up Windows/Unix folder access. See CIFS directories on page 702. Macros used in this context should always be UNC paths starting with two backslashes (\\). No other macros are supported within macros used in this context.

Custom Variables

Applies to the values that can be specified under custom directory variables on the **General** tab under **Configure System Options**. See Other system options on page 729 for more information.

Execute-On

Applies to the system commands that can be specified within the Execute On Successful Send/Receive/Copy/Check properties and the Execute On Fail property (system, host, or action level). See Advanced system options on page 743 for information about the **Advanced** tab under **Configure System Options** for definitions of these properties. With regard to `Execute On Fail` command, when a command is executed as a result of a failed transfer (either on the client or the server), then all applicable macros are supported. When a command is executed as a result of a general system failure, then only `%date%`, `%time%` and `%status%` are supported.

Post/Pre Command

Applies to the FTP properties Post Get Command, Post Put Command, Pre Get Command, and Pre Put Command, as specified under the FTP Host: Advanced Tab on page 97. This context also applies to the Post Put Command and Pre Put Command properties as defined in the SSH FTP Host: Advanced Tab on page 259.

LCOPY Archive

Applies to the archive directory that can be specified with the LCOPY Archive property (system, host, or action level). See Advanced system options on page 743 for more information.

Accessible through API

Applies to macros that are available through `IactionController` interface of the API (if the API is licensed). Refer to the API javadocs for a description of this interface and the method that can be used to obtain a given macro value.

Directories Only

Applies in several places where only the custom directories macros or %inbox%/%outbox% are appropriate.

Banner/Welcome Message

Applies to the banner and/or welcome messages for the HTTP, FTP, SMTP, and SSH FTP servers. See Configuring Local Listener Responses on page 757.

Rules Regarding Macro Variable Use

Below are some general rules for macro variable use.

1. Macros are identified by `%c%`, where `c` is one-to-many characters.
2. Macro variables are case insensitive. You can enter them in lowercase or uppercase.
3. You cannot place a `%` within a macro variable.
4. When a string contains macros to be resolved and a `%` that is not tied to a macro, you must escape the non-macro `%` with `%%`. After all macro substitution takes place, the software strips the extra `%`, yielding the intended character sequence. For example, `LCOPY test.edi %%%date%_%index%` is resolved to `%20090714_01`.
5. The `*` and `?` characters are not allowed within a macro name. Use other special characters with caution.
6. When using the `%date%` and `%time%` macros, it is your responsibility to ensure the formats for the date and time do not violate any file system naming conventions, for example, if the macros are being used to build a filename or directory.
7. Macros are not allowed within a source filename that contains a `*`, `?`, or regular expression. For example, in `LCOPY inbox/%mailbox%*`, `%mailbox%` is not resolved. However, in `LCOPY inbox/%mailbox%/*`, `%mailbox%` is resolved because it is referenced in the source directory path and not the source filename.
8. You can use macros multiple times within the same command. For `%date%`, `%time%` and `%index%`, the same substitution value is used in all references within the same command. However, when you use either of these macros within the destination path of an `LCOPY`, and multiple files are being copied in one command, the following special rules are enforced:
   a. If these macros are used anywhere within the directory path, they are only resolved once within command.
   b. If these macors are used within the file token, they are resolved for each filename.

9. Macros you use within a system command, either within the `SYSTEM` Command context or within the Execute-On context, can be used as part of the actual command or as parameters to a batch file.
10. If the absolute path of the any of the files referenced in the macros contain embedded spaces (for example., `%file%` resolves to `Program Files\LexiCom\inbox\testHost\test.edi`) it might be necessary to add double quotes to the macro specification(s) in the command in order for the command to be properly processed by the operating system. For example, `copy "%file%" "%file%.bad"`.
11. Special rules apply to using directory macro variables for example, `%inbox%`, `%outbox%`, and custom directory variables.
    - If you use these macros in a source file, destination file, custom directory variable definition, or an `LCOPY` Archive context, and the path is a non-URI path, they are replaced only at the beginning of the string. For all other contexts (for example, URI source/destination paths, `SYSTEM` commands), they are replaced anywhere in the string.
    - Although allowed, you should not use directory macros should within a remote destination file context, as they reference local directory paths and are therefore nonsensical in this context.
    - When preceding a path with a directory macro, you should place a file separator character (for example, '/'or '\' between the macro and the subsequent path (for example, `%inbox%/test.edi`).
    - When using directory macros, care should be used so as not to create circular references (for example, host outbox references `%CustomVar%` and `%CustomVar%` references `%outbox%`).
12. All directory macro variables reference their absolute paths.

Reserved Macro Variables

Below is the table of all reserved macro variables.

Macro	Description
Framework Macros	
`%system%`	References the system-level inbox/outbox/sentbox/receivedbox.
`%none%`	For sentbox/receivedbox fields where this option is available to select, this indicates that there should be no associated sent/ receivedbox (rather than defaulting to the system values in the absence of a selection)
`%inbox%`	References the absolute path of the configured host or local user inbox.
`%outbox%`	References the absolute path of the configured host or local user outbox.
`%file%`	References the local file (including the absolute path) involved in the current operation. For `PUT` and certain `CHECK` commands, `%file%` is the source file. For `GET`, `LCOPY`, and certain `CHECK` commands `%file%` is the destination file. See CHECK command on page 943. **Note:** The `CHECK` command is only available in Cleo Harmony and Cleo VLTrader applications.
`%sourcefile%` `%srcfile%`	References the source file name involved in the current operation. If the source file is local, and it is referenced in the Execute-On context, then the absolute path is included.
`%sourcefilebase%` `%srcfilebase%`	References the source file name base (everything up to, but not including, the last '.'.

Macro	Description
%sourcefileext% %srcfileext%	References the source file name extension (everything from, and including, the last '.'. If no extension is contained in the source file, blank is returned.
%destfile%	References the destination file name involved in the current operation. If the destination file is local, and it is referenced in the Execute-On context, then the absolute path is included.
%destfilebase%	References the destination file name base (everything up to, but not including, the last '.'.
%destfileext%	References the destination file name extension (everything from, and including, the last '.'. If no extension is contained in the destination file, blank is returned.
%date%	Specifies the current date in the format defined in the Macro Date Format setting (system, host, or action level). See Advanced system options on page 743 for more information about this property.
%date[+/-#y][+/-#m][+/-#d][,MacroDateFormat=...]%	Specifies a variant of the date as a value in either the past or the future. The '#' character specifies one or more digit values and the order of the +/- fields (y=year, m=month, d=day) dictates the order of the operation, however calendar rules still apply (for example, if the operation causes the day to wrap to the next month then the month value is automatically incremented). The MacroDateFormat parameter variable is case-insensitive. If it is specified with the +/- field(s), it must be specified as the last parameter. If it is not specified, the format defined in the Macro Date Format setting (system, host, or action level) is used. See Advanced system options on page 743 for more information about this property.
%time%	Specifies the current time in the format defined in the Macro Time Format setting (system, host, or action level). See Advanced system options on page 743 for more information about this property.
%time[+/-#h][+/-#m][+/-#s][,MacroTimeFormat=...]%	Specifies a variant of the time as a value in either the past or the future. The # character specifies one or more digit values and the order of the +/- fields (h=hour, m=minute, s=second) dictates the order of the operation, however calendar rules still apply (for example, if the operation causes the minute to wrap to the next hour then the hour value is automatically incremented). The MacroTimeFormat parameter variable is case-insensitive. If it is specified with the +/- field(s), it must be specified as the last parameter. If it is not specified, the format defined in the Macro Time Format setting (system, host, or action level) is used. See Advanced system options on page 743 for more information about this property.

Macro	Description
%index%	Specifies the usage of a daily host index value; often used to help guarantee file uniqueness. Each host's index is reset to 1 at the beginning of each day. It is incremented by one every time %index% is referenced. The minimum number of digits in the index string is determined by the Minimum Number Of Macro Index Digits system option. See Advanced system options on page 743 for more information.
%host%	The alias of the host involved in the current operation.
%mailbox%	The alias of the mailbox involved in the current operation.
%status%	The status of the current operation. Returned status values are either "Success" or "Warning" (both denote a successful transaction) and "Error" or "Exception" (both denote a failed transaction).
%crc%	The value of the computed CRC-32 associated with a transferred file. The CRC is computed only when Compute CRC on transfers is active. See Logs on page 892 for information. This feature is available only for Cleo Harmony and Cleo VLTrader applications.
%filesize%	The size of a transferred file in measured in bytes.
%transferid%	The value of the unique ID assigned to a transferred file. This feature is available only for Cleo Harmony and Cleo VLTrader applications.
%resttransferid%	The value of the unique ID assigned by the REST API to a file transferred (that is, this is the document DB transfer ID as opposed to the transmission transfer ID). This feature is available only for Cleo Harmony and Cleo VLTrader applications.
%filesin%	The number of files received through within an action.
%filesout%	The number of files sent through within an action.
%command%	The full command syntax (only available for the Execute-On context of CHECK commands).
ebMS Macros	
%ebms.timestamp.date%	The date portion of the SOAP header's <eb:Timestamp> value. The format of the date is determined by the Macro Date Format setting (system-, host-, or action-level). See Advanced system options on page 743 for information about Advanced tab under Configure System Options for a definition of this property. This macro will only be resolved when used in the default file name.
%ebms.timestamp.time%	The time portion of the SOAP header's <eb:Timestamp> value. The format of the time is determined by the 'Macro Time Format' setting (system, host, or action level). See Advanced system options on page 743 for information about Advanced tab under Configure System Options for a definition of this property. This macro will only be resolved when used in the default file name.

Macro	Description
%ebms.action%	%ebms.action% = the SOAP header's <eb:Action> value.
%ebms.service%	%ebms.service% = the SOAP header's <eb:Service> value.
%ebms.cpaid%	%ebms.cpaid% = the SOAP header's <eb:CPAId> value. These macros will only be resolved when used in the default file name.
AS2 Macros	
%as2.to%	The current AS2-To value provided in the received message header. This macro will only be resolved when used in the default file name.
%as2.from%	The current AS2-From value provided in the received message header. This macro will only be resolved when used in the default file name.
%as2.subject%	The current Subject value provided in the received message header. This macro will only be resolved when used in the default file name.
AS3 Macros	
%as3.to%	The AS3-To name of a client. This macro will only be resolved when used in the SITE command within an action to verify that the AS3 names are properly configured on the VersaLex AS3 server.
%as3.from%	The AS3-From name of a client. This macro will only be resolved when used in the SITE command within an action to verify that the AS3 names are properly configured on the VersaLex server.
EBICS Macros	
%ebics.ordertype%	For EBICS, this macro will resolve to the order type of the EBICS transaction.

Formatting %date% and %time% Macros

The default %date% setting is yyyyMMdd and the default %time% setting is HHmmssSSS.

To specify a different %date% or %time% format, use a pattern string in the 'Macro Date Format' and 'Macro Time Format' setting (system, host, or action level). See Advanced system options on page 743 for information about the Advanced tab under Configure System Options for definitions of these properties. Formats may also be specified as part of the macro definition, e.g., %date,MacroDateFormat=yyyyMMdd% and %time,MacroTimeFormat=HHmmssSSS%

In the pattern, all ASCII letters are reserved as pattern letters, which are defined as the following:

Symbol	Meaning	Example
G	era designator	AD
y	year	2004
M	month in year	September & 09
d	day in month	15

Symbol	Meaning	Example
h	hour in am/pm (1~12)	12
H	hour in day (0~23)	0
m	minute in hour	30
s	second in minute	24
S	millisecond	352
E	day in week	Wednesday
D	day in year	259
F	day of week in month	2 (2nd Wed in September)
w	week in year	35
W	week in month	2
a	am/pm marker	PM
k	hour in day (1~24)	24
K	hour in am/pm (0~11)	0
z	time zone	Central Standard Time
'	escape for text	delimiter
''	single quote	'

Any characters in the pattern that are not in the ranges of ['a'..'z'] and ['A'..'Z'] will be treated as quoted text. For instance, characters like '.', '#' and '@' will appear in the resulting date or time text even if they are not embraced within single quotes.

Note: A pattern containing any invalid pattern letter will result in a thrown exception during formatting or parsing.

Examples Using Pattern Strings:

%date% Format Pattern	Result
MM-dd-yyyy	09-15-2004
EEE_MMM_d_yy	Wed_September_15_04

%time% Format Pattern	Result
h_mm_a	12_08_PM
K_mma-z	0_00PM-CST

Macro Variable Usage Examples

Destination File Examples:

Action Command	Destination File Result
PUT test.edi %date%_%time%.edi	20090714_131524352.edi

Action Command	Destination File Result
PUT test.edi %date-1d,MacroDateFormat=MMdd%.edi	0713.edi
GET test.edi %srcfile%%date%-%time%-%index%	test.edi20090714-131524352-1
LCOPY test.edi %date%_%time%.%srcfileext%	20090714_131524352.edi
LCOPY test.edi %%%date%_%time%	%20090714_131524352

Source File Examples:

Action Command	Source File Result
PUT %inbox%\%date%\test.edi	inbox\20090714\test.edi
PUT %inbox%\%date,MacroDateFormat=yyyy%	inbox\2009\test.edi
PUT %outbox%\%mailbox%*	outbox\myMailbox*

Execute-On Examples:

After successful execution of 'LCOPY test.edi test2.edi':

Execute On Successful Copy System Command	System Command Result
cmd.exe /c copy "%destfile%" "c:\temp\%destfilebase%.copy"	cmd.exe /c copy "c:\LexiCom\inbox\test2.edi" "c:\temp\test2.copy"
cmd.exe /c ExecuteOnCopy.bat "%destfile%" "c:\temp\%destfilebase%.copy"	cmd.exe /c ExecuteOnCopy.bat "c:\LexiCom\inbox\test2.edi" "c:\temp\test2.copy"

Default Host Directory Examples:

Assume the system-level inbox is 'myInbox\' and the custom directory variable, '%custom1%', is set to '\\filsvr01\serverInbox\'.

Host Default Directory (Inbox) Setting	Resolved Location
%custom1%	\\filsvr01\serverInbox\
%custom1%\inbox1	\\filsvr01\serverInbox\inbox1
%system%	myInbox\
%system%\inbox1	myInbox\inbox1

Using wildcards and regular expressions

This section describes the usage of wildcards and regular expressions. Wildcards and regular expression are most often used in the paths of GET, PUT, LCOPY, LDELETE, LREPLACE, and CHECK commands. The CHECK is only available with the Cleo Harmony and Cleo VLTrader applications. Generally, wildcards and regular expressions are restricted to use only within the filename token of a path. Some cases, however, allow for placement within the directory tokens, as well. Refer to your specific command reference for locations where you can use wildcards and regular expressions. As an introduction, the table below provides some examples.

Command	Result
`PUT myOutbox\ab*.edi`	Searches `myOutbox` for all files that match the pattern `ab*.edi`
`PUT myOutbox\ab?.edi`	Searches `myOutbox` for all files that match the pattern `ab?edi`
`PUT myOutbox\[ab.*\.edi]`	Searches `myOutbox` for all files that match the regular expression `ab.*\.edi`
`CHECK *box\[ab.*\.edi]`	Searches first for directories that end in `box` (for example, `inbox` or `outbox`) and next for files that match the regular expression `ab.*\.edi`
`CHECK *box\[a.*]\[ab.*\.edi]`	Searches first for directories that end in `box` (for example, `inbox` or `outbox`), and next for the subdirectories that match the regular expression `a.*` , and finally for files that match the regular expression `ab.*\.edi`

Wildcards

Wildcards are represented by `*` or `?`, where `*` matches multiple characters and `?` matches only a single character. For example, assume the outbox has the following files.

`ab1.edi`

`ab2.edi`

`ab11.edi`

`ab12.edi`

The following commands produce the following results.

Command	Result
`PUT ab*.edi`	Sends all four files from the outbox
`PUT ab?.edi`	Sends only `ab1.edi` and `ab2.edi`

Note that, when using wildcards, it is possible to use multiple wildcards within the same token. For example, "**PUT ab*.***" and "**PUT ab?.***" are both acceptable.

Regular Expressions

When the basic wildcards do not provide the needed search criteria, regular expressions may be used instead. Regular expressions (abbreviated *regex*) are composed of a special syntax that enables a wider range of search patterns. All regular expression usage must follow these basic rules.

- The regex pattern must be enclosed in brackets (for example, `[test[ABC]\.edi]` or `[test\d\.edi]`). Note that, as seen in this example, it is possible for a regular expression to contain brackets as part of the pattern definition itself; however, it is still necessary to enclose the complete pattern in its own pair of brackets.
- Only one regex pattern is allowed per token, for example, a filename or a directory token. Furthermore, the pattern must consume the entire token. Below is a table containing some valid and invalid regular expression examples.

Command	Valid/Invalid
`PUT myOutbox\[ab.*\.edi]`	valid
`PUT myOutbox\ab.*\.edi`	invalid -- does not contain the brackets

Command	Valid/Invalid
`PUT myOutbox\ab[.*\.edi]`	invalid -- does not consume the entire filename token
`PUT myOutbox\[ab.*].[edi]`	invalid -- contains two regex patterns within one token (i.e., the filename token)

Regular Expression Constructs

This section provides descriptions of some commonly used constructs within regular expressions. For a more complete list of regular expression constructs and a more detailed discussion, visit http://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html#sum.

Table 2: Character Classes

Construct	Description
`[abc]`	`a`, `b` or `c`
`[^abc]`	Any character except `a`, `b` or `c`

Table 3: Predefined Character Classes

Construct	Description
`.`	Any character
`\d`	A digit: `[0-9]`
`\D`	A non-digit: `[^0-9]`

Table 4: POSIX Character Classes

Construct	Description
`\p{Lower}`	lowercase alphabetic character
`\p{Upper}`	An uppercase alphabetic character
`\p{ASCII}`	Any ASCII character: `[\x00-\x7F]`
`\p{Digit}`	A digit: `[0-9]`
`\p{Alnum}`	An alphanumeric character

Table 5: Quantifiers

Construct	Description
X?	*X*, zero or one time
*X**	*X*, zero or more times
X+	*X*, one or more times

Construct	Description
X{*n*}	*X*, exactly *n* times
X{*n*,}	*X*, at least *n* times
X{*n*,*m*}	*X*, at least *n* but not more than *m* times

Table 6: Boundary Markers

Construct	Description
^	Indicates the subsequent characters must appear at the beginning of the string
$	Indicates the preceding characters must appear at the end of the string

Table 7: Literal Expressions

Construct	Description
\	Escapes (quotes) the following character. Necessary if you want to match to a period ('.'), bracket ('[]'), brace ('{}') or other special character.
\Q	Starts an escaped (quoted) literal string. Literal string should be closed with \E.
\E	Ends an escaped (quoted) literal string that was started by \Q.

Table 8: Other

Construct	Description
(?i)	Turn on flag to ignore case.
(*X*)	Match string *X* .
(?i: *X*)	Match string *X* , ignoring case.
(?! *X*)	Do not match string *X* .

Regular Expression Examples

The table below contains some examples that might be used for file name searches.

Regex	Matches
[.*]	Matches any file
[test.*\.edi]	Matches test.edi through test (any character(s)) . edi (lower case only)
[(?i)test.*\.edi]	Matches test.edi through test (any character(s)) .edi (lower or upper case)

Regex	Matches
`[(?i)test[abc]{3}\d\.edi]`	Matches testaaa0.edi through testccc9.edi (lower or upper case)
`[test\p{Digit}{1,}\.edi]`	Matches test0.edi through test9.edi, test00 through test99.edi, etc. (lower case only)
`[(?!TestFile)(.*)]`	Matches every file *except* a file called "TestFile" (case sensitive).
`[(?i)(?!TestFile)(.*)]`	Matches every file *except* a file called "TestFile" (case insensitive).
`[(?!.*\.edi$)(.*)]`	Matches every file *except* a file that ends in ".edi" (case sensitive).
`[(?i:(?!.*\.edi$))(.*)]`	Matches every file *except* a file that ends in ".edi" (case insensitive).
`[(?!(\.)|(\.\.))(.*)]`	Matches every file *except* those named "." or "..".
`[(?i)(?!(.*\.tmp$))(.*)]`	Matches every file *except* those that end in ".tmp" (case insensitive).
`[(?i)(?!(^vltrader.*\.tmp$))(.*)]`	Matches every file *except* those that start with "VLTrader" and end in ".tmp" (case insensitive).
`[(?!(TestFile)|(Test\.File))(.*)]`	Matches every file *except* those named "TestFile" or "Test.File" (case insensitive).
`[(.*)(Primary)(.*)]`	Matches any file that contains the string "Primary" somewhere in it (case sensitive).
`[(.*)(?i:Primary)(.*)]`	Matches any file that contains the string "Primary" somewhere in it (case insensitive).
`[test.edi]`	Matches only "test.edi".
`[(?i)test.edi]`	Matches "test.edi" (case insensitive).
`[\+.*]`	Matches every file that starts with "+".
`[\+\+.*]`	Matches every file that starts with "++".
`[\Q+\E.*]`	Matches every file that starts with "+".
`[\Q++\E.*]`	Matches every file that starts with "++".
`[.*\Q+\E.*]`	Matches every file that contains "+" anywhere within the name.

Note:

1. If you need to download a specific file, but the absence of that file generates an unwanted error, enclose the filename in a regular expression to avoid the error. For example, `[test\.edi]` will match only a file called `test.edi`.
2. For `LCOPY -REC` commands, the final token cannot be a file. To get around this restriction, enclose the filename in brackets. For example, `outbox/test/[test.edi]`.

Chapter

4

Hosts

Use Hosts for initiating outbound connections.

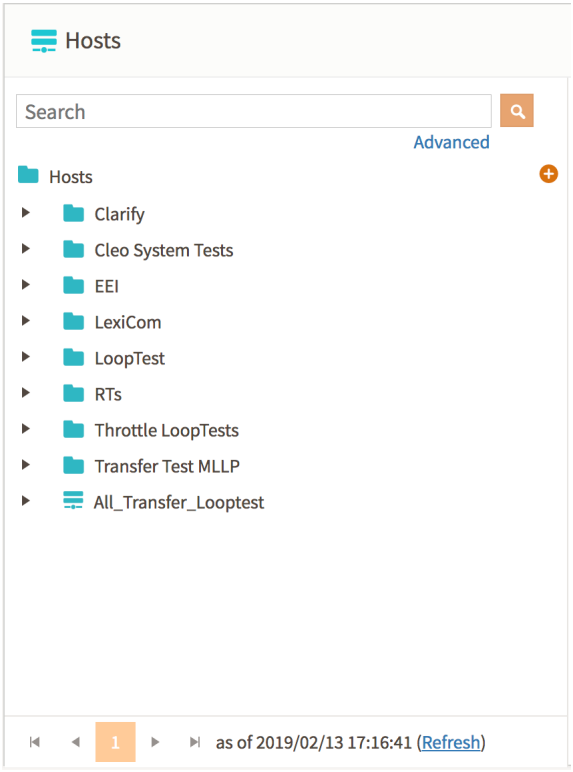
Hosts – Web UI

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

This section explains settings and details of the Hosts page that are specific to the Cleo Harmony and Cleo VLTrader Web UI.

Web UI Host Tree

The Host Tree in the Cleo Harmony and Cleo VLTrader Web UI displays available hosts. Access the Host Tree by clicking **Hosts** in the top menu bar.



You can activate hosts from the Host Tree by right-clicking, by using a template, or by searching for a specific host. See Activating a host from a template in the Web UI on page 76 and Advanced search options on page 76.

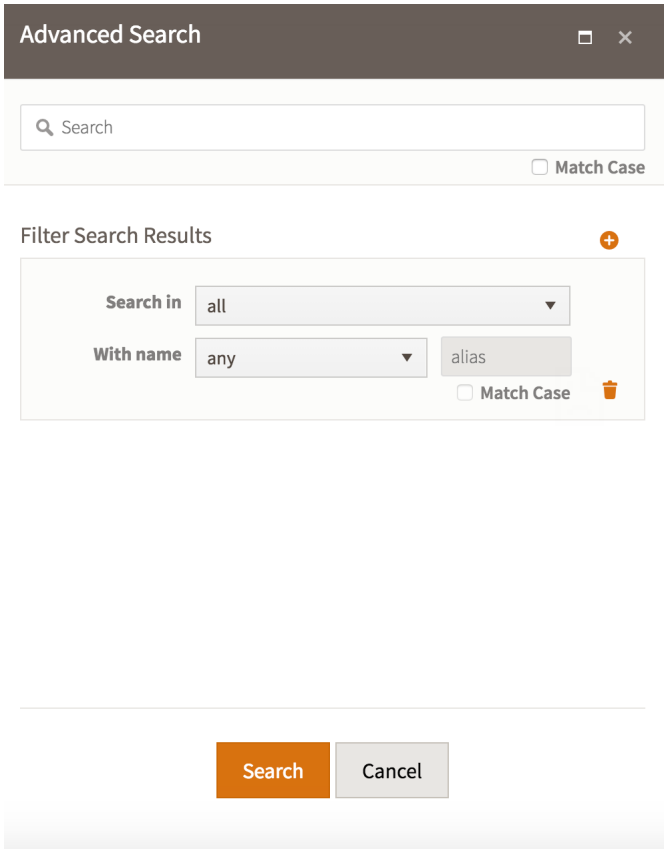
Activating a host from a template in the Web UI

Use the **Activate from Templates** button to activate a host from a template in the Web UI.

1. Click the + (**Activate from Templates**) button below the search bar in the **Hosts** page.
2. The **Templates** dialog box appears.
3. Use the **Hosts** tree in the **Templates** window to find the host you want to clone and activate. Right-click and select from the context menu to clone.

Advanced search options

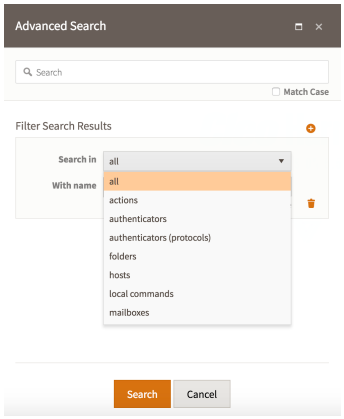
Use the advanced search to search through the active items in the host tree. You can access the advanced search by clicking the **Advanced** link under the search bar above the **Hosts** tree. The **Advanced Search** dialog box appears.



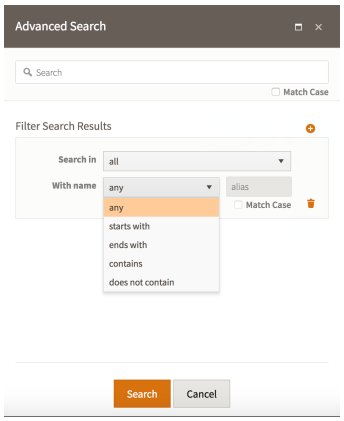
Type your search string directly into the **Search** field. If you want to search with case sensitivity, select **Match Case**. You can perform relevant right-click actions in the search results.

Filtering search results

To narrow your search, use the **Filter Search Results** menu below the **Search** field. By clicking the + icon, you can add more filters to your search. Click the **trash can** icon to remove filters from your search.



Use the **Search in** menu to restrict your search to certain types of items in the host tree.



Use the **Alias** menu and field to restrict your search to a certain naming convention.

Hosts and Mailboxes – Native and Classic Web UI

You use *hosts* to initiate outbound connections. Hosts allow you to create both client- and server-side connections that you can use to transfer data to and from your system. You use *mailboxes* to access the host system. This section explains how to activate, configure, and use hosts and mailboxes.

Activating a host from a template

1. Click the **Templates** tab in the tree pane.
2. If you are not sure which host you need to activate, do the following:
   a) Select the Hosts folder and the content pane table will list details about the all the available pre-configured hosts.
   b) Click through to open the tiered levels on any pre-configured host tree to review the provided *host*, *mailbox*, *trading partner*, and *action* configurations. Select the **Notes** tab in these panels to access any supplied documentation.
3. Right-click the desired *host* in the pre-configured host tree or right-click the detail entry in the content pane table for the desired *host.*

4. Select **Clone and Activate**. The entire pre-configured *host* branch will be copied and made active, the Active tab will be automatically selected in the tree pane, and the new active *host* will be automatically selected in the tree. The new active host alias may be appended with a number, if necessary to make it unique. The original pre-configured host will remain in the pre-configured tree.
5. If desired, type a new host alias in the content pane panel and click **Apply**.
6. A preconfigured host can also be activated from Cleo's web site. See Cloning and activating a pre-configured host on page 78.

Cloning and activating a pre-configured host

The Cleo Harmony application provides the capability for downloading preconfigured hosts directly from the Cleo web site, guaranteeing that the latest distributed host is always available for cloning and activation.

1. Click the **Templates** tab in the tree pane.
2. If necessary, click the **Connections** folder to open it and then click the **Pre-configured** folder.

   The product connects to the Cleo website to download pre-configured host data. After the download is complete, the preconfigured hosts are displayed in the **Pre-configured** folder and sorted into Industry folders.
3. If you are not sure which host you need to activate, do the following:
   a) Click on an Industry folder (that is, a child of the **Pre-Configured** folder) to display details about the available pre-configured hosts for that specific industry. If the host has not been downloaded yet, the number of Mailboxes, Actions, HostActions, and TradingPartners are initially set to 0. After the download has completed, you can view updated host details in the content pane table.
   b) Expand the Industry folder to display the host entries. If the host has not been downloaded yet, no tiered levels are displayed for the host. Once the host has been downloaded, review the provided *host*, *mailbox*, *host action*, *trading partner*, and *action* configurations. Select the **Notes** tab in these panels to access any supplied documentation.
4. To download a host from the website, click a *host* in the pre-configured host tree or click the detail entry in the content pane table for the *host*.
5. Right-click the *host* in the pre-configured host tree or right-click the detail entry in the content pane table for the *host.*
6. Select **Clone and Activate**. The entire pre-configured *host* branch will be copied and made active, the **Active** tab will automatically be selected in the tree pane, and the new active *host* will automatically be selected in the tree. The new active host alias may be appended with a number, if necessary, to make it unique. The original pre-configured host will remain in the pre-configured tree until the client session is closed.

Configuring an active host

1. Select the active *host* in the tree pane.
2. Depending on the level of detail preconfigured into the host, you may or may not need to create tree branches. At a minimum, you will need to have one action within one mailbox of your host in order to send and/or receive files.
3. Supply any required information for each tree branch. An incomplete branch is indicated by the color orange in the tree and by an unchecked £ Ready indication in the content pane panel. Required fields are starred (*) and possible values may be user choice or may need to come from the service provider. For the latter, check the **Notes** tab in the content pane for any known contact information.
4. You will likely need to supply your user name and password at the mailbox level. See the **Enter Your User Name and Password** section within the documents **Generic FTP and FTP/S** or **Generic HTTP and HTTP/S**, or the document specific to the desired target host type(s). Documentation specific to the host you are communicating with may be available from the LexiCom home directory: by default, `C:\Program Files\LexiCom \manuals\hosts`.

Note: For the Generic AS2 host, you will not need to supply a user name and password; however, you will need to follow the steps in the section **Generic AS2 Host and Local Listener**, to complete configuration.

Creating a custom preconfigured host

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

You can copy an active host to the **Templates** tree in order to retain custom settings you can use later.

1. Click the **Templates** tab in the tree pane.
2. Right-click the **Hosts** folder.
3. Select **newFolder** and rename the host subfolder to a meaningful name.
4. Click the **Active** tab in the tree pane.
5. Right-click the active host you want to copy and select **Copy to Preconfigured**.
6. Select the Folder where the active host will be copied from the drop-down list.
7. Use the suggested Target Alias (based on the current alias) or create a different unique alias.
8. Click **Continue** and the host is copied and displayed in the Templates tree.

Using the wizard to create a host or mailbox

Cleo Harmony, Cleo VLTrader, and Cleo LexiCom provides wizard that walk you step-by-step through the process of configuring the most common trading relationships.

Right-click the Local Listener in the active tree pane and select **Wizard** to do the following:

- Set the HTTP and HTTP/s listener port.
- Create and/or select SSL certificates (if applicable).
- Create and/or select signing and encryption certificates.
- Set the protocol (AS2/AS3 or ebMS).
- For AS2 and AS3 only:
  - Set the AS2/AS3 external address.
  - Set the AS2/AS3 administrator email address.

Right-click the AS2/AS3 mailbox in the active tree pane and select **Wizard** to:

- Set the AS2/AS3-From and AS2/AS3-To names.
- Select the trading partner's signing and encryption certificates.

Configuring mailbox packaging

Note: This section applies to all hosts, except the Local Commands host. For information about packaging for the Local Commands host, see Configuring Local Commands host on page 800.

Use the **Packaging** tab to configure encryption and decryption of payload files retrieved from the file system (or database payload repository) and stored to the file system (or database payload repository).

The **Packaging** tab consists of two sections: **Partner Packing** and **Local Packaging**. See Configuring partner mailbox packaging on page 80 and Configuring local mailbox packaging on page 83, respectively.

For each Partner and Local Packaging, there are two packaging schemes: **OpenPGP** and **XML Encryption**. Both schemes use a public/private key pair established through a shared certificate to perform encryption and

decryption. The OpenPGP option also supports digital signing. See Cryptographic Services on page 975 for general information regarding encryption and signing.

There are certain advanced properties that govern the details of the packaging selections. These properties are listed in the following table. See Setting advanced host properties on page 89 for more information.

OpenPGP Properties	XML Encryption Properties
PGP Compression Algorithm	XML Encryption Algorithm
PGP Encryption Algorithm	
PGP Hash Algorithm	
PGP Integrity Check	
PGP Signature Verification	
PGP V3 Signature	

Configuring partner mailbox packaging

You use the **Partner** section of the **Packaging** tab to configure outbound file packaging (files going to your trading partner) and inbound file un-packaging (files coming from your trading partner). This allows you to associate your trading partner's signing/encryption certificate with this mailbox for outbound packaging and associate your signing/decryption certificate with this mailbox for un-packaging inbound data.

Note: If you enable packaging through this panel, and packaging is also enabled through a protocol (for example, S/MIME encryption enabled through the mailbox AS2 tab), the payload will be doubly packaged. For example, if you select AS2 S/MIME encryption and XML Encryption, the XML-encrypted package will be encapsulated within the S/MIME-encrypted package.

Before you configure partner mailbox packaging, you must acquire your trading partner's signing/encryption certificate and provide to yours to your trading partner. See Acquiring your trading partner's signing and encryption certificates on page 86 and Creating and providing your signing/encryption certificates on page 86.

In the **Partner** section of the **Packaging** tab, select one of the following options from the **Packaging** menu and click **Configure**:

- **None** - partner packaging is not active.
- **OpenPGP** - OpenPGP partner packaging is active. See OpenPGP partner mailbox packaging reference on page 80 for information on setting up OpenPGP partner packaging.
- **XML Encryption** - XML Encryption partner packaging is active. See XML encryption partner mailbox packaging reference on page 82 for information on setting up XML Encryption partner packaging.

OpenPGP partner mailbox packaging reference

Note: Values you specify in the **Encrypt Outbound**, **Decrypt Inbound**, and certificate fields are shared between the OpenPGP and XML encryption configurations. You can specify these values once in either place to populate both configurations.

When using OpenPGP, if your trading partner has provided an OpenPGP public key, you can use the Certificate Manager to generate a Trusted CA Certificate from an OpenPGP key . See Certificate management on page 661 and Generating trusted CA certificates from OpenPGP or SSH FTP keys on page 665. Similarly, if your trading partner requires an OpenPGP public key, you can use the Certificate Manager to export an OpenPGP key . See Certificate management on page 661 and Exporting certificates on page 668.

Encrypt Outbound

Select this check box to enable fields related to encrypting outbound messages.

It is recommended that you enter both your trading partner's certificate and your user certificate as both might be necessary depending upon the options selected.

Values you specify in the **Encrypt Outbound**, **Decrypt Inbound**, and certificate fields are shared between the OpenPGP and XML encryption configurations. You can specify these values once in either place to populate both configurations.

Decrypt Inbound

Select this check box to enable fields related to decrypting inbound messages.

it is recommended that you enter both your trading partner's certificate and your user certificate as both might be necessary depending upon the options selected.

It is important to understand that the **Encrypt Outbound**, **Decrypt Inbound**, and certificate fields are shared between the two dialogs.

Encryption/Signature Verification

Certificate

Enabled when you select either the **Encrypt Outbound** or **Decrypt Inbound** check box.

Click **Browse** to navigate to and select the certificate you want to use. The **Certificate** field is populated with the path of the certificate you select.

If multiple recipients are required, you can use the `SET` command to specify multiple certificates using the '|' (pipe) character. For example:

```
SET mailbox.PartnerPGPEncryptionCert=certs\companyA.cer  | certs
\personB.cer | certs\trunk.cer | certs\companyC.p7b
```

Decryption/Signing

By default, the signing certificate you configured on the **Certificates** tab of the Local Listener panel is used to sign and decrypt your files. See Configuring certificates for Local Listener on page 758.

Override Local Listener Certificate

Enables fields where you specify a certificate to use instead of the one you configured for the Local Listener. See Configuring certificates for Local Listener on page 758.

If you override the default certificates, you must also exchange the certificates you specify here with your partner.

Exchange Certificates

Displays the Certificate Exchange dialog box, which allows you to send your certificates to your trading partner. See Exchanging certificates with your trading partner on page 672.

If you choose to schedule the PGP packaging certificate for future use, there is a field available, **Allow Overlapping Key Usage**, that lets you choose how certificates should be used when their schedules overlap. See Allowing overlapping signing/encryption keys on page 685.

Certificate Alias

Password

Click **Browse** to navigate to and select a certificate. Enter the **Password** for your certificate's private key.

Outbound Options

A file can be sent to the remote host with any combination of the following options available on the **Advanced** tab under **Configure System Options**. See Advanced system options on page 743 for more information.

Encrypted

Encrypt using the `PGP Encryption Algorithm` property.

Signed

Sign using the `PGP Hash Algorithm`.

Encrypt to My Certificate

Allow **My Certificate** as well as Trading Partner's Certificate to decrypt outbound encrypted files. The **Encrypted** box must be checked to enable and use this option.

Armored (Base 64)

Armor (Base64 encode) the data. Base64 encoding converts binary data to printable ASCII characters.

Compressed

Compress using the `PGP Compression Algorithm`.

Inbound Security

Force Encryption

Force Signature

When you select **Force Encryption** or **Force Signature**, all inbound messages are checked for the required security level. An error is logged and the message is rejected if the message is not received according to the corresponding message security settings. If either setting is not selected (default), the message is not checked for conformance with that security setting.

Allow non-OpenPGP

Allows non-OpenPGP formatted data to be processed without generating OpenPGP related errors.

XML encryption partner mailbox packaging reference

Note: Values you specify in the **Encrypt Outbound**, **Decrypt Inbound**, and certificate fields are shared between the OpenPGP and XML encryption configurations. You can specify these values once in either place to populate both configurations.

Encrypt Outbound

Select this check box to enable fields related to encrypting outbound messages.

Decrypt Inbound

Select this check box to enable fields related to decrypting inbound messages.

Encryption Certificate

Enabled when you select the **Encrypt Outbound** check box.

Click **Browse** to navigate to and select the certificate you want to use. The **Certificate** field is populated with the path of the certificate you select.

Decryption Certificate

Enabled when you select the **Decrypt Inbound** check box.

By default, the encryption certificate you configured on the **Certificates** tab of the Local Listener panel is used to decrypt your files. See Configuring certificates for Local Listener on page 758.

Override Local Listener Certificate

Enables fields where you specify a certificate to use instead of the one you configured for the Local Listener. See Configuring certificates for Local Listener on page 758.

If you override the default certificates, you must also exchange the certificates you specify here with your partner.

Exchange Certificates

Displays the **Certificate Exchange** dialog box, which allows you to send your certificates to your trading partner. See Exchanging certificates with your trading partner on page 672.

Certificate Alias

Password

Click **Browse** to navigate to and select a certificate. Enter the **Password** for your certificate's private key.

Configuring local mailbox packaging

You use the **Local** section to configure inbound encryption (files stored to the file system/database) and outbound decryption (files retrieved from the file system/database). This allows you to associate your signing/encryption certificate with this mailbox for inbound packaging and your signing/decryption certificate with this mailbox for outbound un-packaging. You can use the same certificate or two different certificates depending on your application. Before you configure **Local** packaging, you must create or acquire an encryption certificate to use for local storage encryption, decryption, and signing.

- In the **Local** section of the **Packaging** tab, select one of the following options from the **Packaging** menu and click **Configure**:
  - **None** - partner packaging is not active.
  - **OpenPGP** - OpenPGP partner packaging is active. See OpenPGP local mailbox packaging reference on page 83 for information on setting up OpenPGP partner packaging.
  - **XML Encryption** - XML Encryption partner packaging is active. See XML encryption local mailbox packaging reference on page 84 for information on setting up XML Encryption partner packaging.

OpenPGP local mailbox packaging reference

Note: Values you specify in the **Encrypt Certificate** and **Decrypt Certificate** sections are shared between the OpenPGP and XML encryption configurations. You can specify these values once in either place to populate both configurations.

Encrypt Inbound

Select this check box to enable fields related to encrypting inbound messages.

Values you specify in the **Encrypt/Signature Verification**, **Decryption/Signing**, and certificate fields are shared between the OpenPGP and XML encryption configurations. You can specify these values once in either place to populate both configurations.

Decrypt Outbound

Select this check box to enable fields related to decrypting outbound messages.

Values you specify in the **Encrypt/Signature Verification**, **Decryption/Signing**, and certificate fields are shared between the OpenPGP and XML encryption configurations. You can specify these values once in either place to populate both configurations.

Encryption/Signature Verification

Certificate

Enabled when you select either the **Encrypt Inbound** or **Decrypt Outbound** check box.

Click **Browse** to navigate to and select the certificate you want to use. The **Certificate** field is populated with the path of the certificate you select.

Decryption/Signing

By default, the signing certificate you configured on the **Certificates** tab of the Local Listener panel is used to sign and decrypt your files. See Configuring certificates for Local Listener on page 758.

Override Local Listener Certificate

Enables fields where you specify a certificate to use instead of the one you configured for the Local Listener. See Configuring certificates for Local Listener on page 758.

If you override the default certificates, you must also exchange the certificates you specify here with your partner.

Certificate Alias

Password

Click **Browse** to navigate to and select a certificate. Enter the **Password** for your certificate's private key.

Inbound Options

A file can be written to the file system/database with any combination of the following options available on the **Advanced** tab under **Configure System Options**. See Advanced system options on page 743 for more information.

Encrypted

Encrypt using the `PGP Encryption Algorithm` property.

Signed

Sign using the `PGP Hash Algorithm`.

Encrypt to My Certificate

Allow **My Certificate** as well as Trading Partner's Certificate to decrypt outbound encrypted files. The **Encrypted** box must be checked to enable and use this option.

Armored (Base 64)

Armor (Base64 encode) the data. Base64 encoding converts binary data to printable ASCII characters.

Compressed

Compress using the `PGP Compression Algorithm`.

Outbound Security

Force Encryption

Force Signature

When you select **Force Encryption** or **Force Signature**, all outbound files are checked for the required security level. An error is logged and the message is rejected if the message is not received according to the corresponding message security settings. If either setting is not selected (default), the message is not checked for conformance with that security setting.

Allow non-OpenPGP

Allows non-OpenPGP formatted data to be processed without generating OpenPGP related errors.

XML encryption local mailbox packaging reference

Note: Values you specify in the **Encrypt Certificate** and **Decrypt Certificate** sections are shared between the OpenPGP and XML encryption configurations. You can specify these values once in either place to populate both configurations.

Encrypt Inbound

Select this check box to enable fields related to encrypting inbound messages.

Decrypt Outbound

Select this check box to enable fields related to decrypting outbound messages.

Encryption Certificate

Enabled when you select the **Encrypt Inbound** check box.

Click **Browse** to navigate to and select the certificate you want to use. The **Certificate** field is populated with the path of the certificate you select.

Decryption Certificate

Enabled when you select the **Decrypt Outbound** check box.

By default, the encryption certificate you configured on the **Certificates** tab of the Local Listener panel is used to decrypt your files. See Configuring certificates for Local Listener on page 758.

Override Local Listener Certificate

Enables fields where you specify a certificate to use instead of the one you configured for the Local Listener. See Configuring certificates for Local Listener on page 758.

If you override the default certificates, you must also exchange the certificates you specify here with your partner.

Certificate Alias

Password

Click **Browse** to navigate to and select a certificate. Enter the **Password** for your certificate's private key.

Determining and providing your URL information

The AS2, AS3/FTP server (Cleo Harmony and Cleo VLTrader applications only), and ebMS protocols require you to forward your Cleo Harmony, Cleo VLTrader, or Cleo LexiCom URL to your trading partner.

Local Listener

If you have not already done so, configure your Local Listener. See Configuring the Local Listener on page 750.

Use the Local Listener Configuration Wizard configuration wizard (see Using the wizard to create a host or mailbox on page 79) and follow the steps to specify the address and ports.

Note: You can also use the Local Listener Configuration Wizard to create signing/encryption certificates.

URL exchange

The method of URL exchange must be agreed upon with the trading partner. The mailbox **Notes** tab may come preconfigured with specific information concerning URL exchange with a particular trading partner.

The Email Profile utility automatically builds the URL. If you are not using the utility, you must build the URL by hand.

Building an URL using the Email Profile Utility

If emailing, use the Email Profile utility. See Emailing a profile to your trading partner on page 87. Even if the utility is not used to forward your profile to your trading partner, you can use the utility to capture the information locally.

Note: This utility is also used to send your signing/encryption certificates.

Building an URL for AS2 and ebMS

AS2 and ebMS are HTTP protocols. An HTTP URL is of the form: `http(s)://your-host:httpport/your-resource-path` where:

- *http* or *https* is specified depending on whether you are using an HTTP or HTTP/s Port from the Configuring a Local Listener for HTTP on page 750.
- *your-host* is the fully qualified name (recommended) or static, external IP address of the VersaLex computer. For AS2, this is **My External Address** in the Configuring AS2 Service on page 767. Contact your systems administrator if you do not know your fully qualified name or external IP address. You may also obtain your external IP address by accessing http://www.cleo.com/whoami .

- *httpport* is the HTTP or HTTP/s Port in the **Local Listener: HTTP** tab. See Configuring a Local Listener for HTTP on page 750. Including *:httpport* in the URL is optional when the standard port is used. Port 80 is the standard port for HTTP and port 443 is the standard port for HTTP/s.
- If you are using Cleo VLProxy software (or a third party reverse proxy), *http* or *https*, *your-host*, and *httpport* depend on the proxy settings.
- *your-resource-path* is the Resource Path in either the **AS2 Service: AS2** tab or the **ebMS Service: ebXML** tab. See Configuring AS2 Service on page 767 and Configuring ebXML Message Service on page 772.

Building an URL for AS3 and FTP

For AS3 server or FTP server are FTP protocols. An FTP URL is of the form: `ftp(s)://your-host:ftpport` where:

- *ftp* is specified if using an FTP or FTP/s Explicit Port and *ftps* is specified if using an FTP/s Implicit Port from the Local Listener: FTP tab .
- *your-host* is the fully qualified name (recommended) or static, external IP address of the VersaLex computer. Contact your systems administrator if you do not know your fully qualified name or external IP address. You may also obtain your external IP address by accessing http://www.cleo.com/whoami .
- *ftpport* is the FTP or FTP/s Port in the **Local Listener: FTP** tab. See Configuring a Local Listener for FTP on page 752. (Inclusion of *:ftpport* in the URL is optional when the standard port is being used. Port 21 is the standard port for FTP and FTP/s Implicit and port 990 is the standard port for FTP/s Explicit.)
- If using Cleo VLProxy (or a third party reverse proxy), *ftp* or *ftps*, *your-host*, and *ftpport* depend on the proxy settings.

Acquiring your trading partner's signing and encryption certificates

AS2, AS3, AS4, ebMS, OFTPv2, RNIF, and other protocols require use of a digital certificate for encryption and signing purposes. Other security features within the Cleo Harmony, Cleo VLTrader, and Cleo LexiCom applications (for example, XML Encryption within the **Mailbox Packaging** tab) also require a digital certificate. See Mailbox Packaging Tab . As a prerequisite to setting up a trading relationship, you must aquire a digital certificate from your trading partner. See Certificate management on page 661 for information on digital certificates.

You and your trading partner must agree on the method of certificate exchange. You can exchange certificates through a web site, a courier service, regular mail, or as attachments through electronic mail.

Once you have received the trading partner's certificates, you can register the certificates with the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application by either saving the files directly in the `certs\` directory or by importing the certificates . See Importing certificates on page 666.

Finally, identify the signing/encryption certificates in the mailbox. For example, see AS2 Mailbox: Certificates Tab on page 168. Use the mailbox wizard and follow the steps to set the trading partner signing/encryption certificates. See Using the wizard to create a host or mailbox on page 79.

Creating and providing your signing/encryption certificates

AS2, AS3, ebMS, OFTPv2, RNIF, and other protocols require use of a digital certificate for encryption and signing purposes. Other security features within the Cleo Harmony, Cleo VLTrader, and Cleo LexiCom applications (for example, XML Encryption within the **Mailbox Packaging** tab) also require a digital certificate. See Mailbox Packaging Tab . As a prerequisite to setting up a trading relationship, you must aquire a digital certificate your trading partner. See Certificate Manager for information on digital certificates.

If you have not already done so, generate a user certificate to use for signing messages sent to your trading partner and decrypting message received from your trading partner.

Use the Local Listener configuration wizard (see Using the wizard to create a host or mailbox on page 79) and follow the steps to generate a new self-signed user certificate for signing and encryption. Normally, the same certificate is used for signing and encryption, but if required they can be different certificates. Be sure to remember or record the password of the certificate(s) created.

Note: The Local Listener wizard is also used to configure your external address and ports.

Your trading partner might not allow self-signed certificates, and instead require that your certificate be signed by a trusted Certificate Authority (CA). To acquire a CA-signed certificate, forward a Certificate Signing Request (CSR) to the CA. See Generating PEM-formatted certificate signing requests on page 664. Then, after receiving a signed certificate back from the CA, replace your self-signed certificate with the CA-signed certificate. See Replacing trusted CA certificates on page 669.

If you already have a certificate and private key currently stored outside of the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application to be used for signing/encryption, import the certificate and private key. See Importing certificates on page 666.

If you have **multiple** trading relationships, you might be able to use the same user certificate for all. The Local Listener wizard sets the default signing/encryption certificates in the **Local Listener: Certificates** tab. See Configuring certificates for Local Listener on page 758. If a different user certificate must be used for a specific trading relationship, you can override the Local Listener certificates at the mailbox level (for example, AS2 Mailbox: Certificates Tab on page 168).

You and your trading partner must agree on the method of certificate exchange. You can exchange certificates through a web site, a courier service, regular mail, as email attachments or through EDIINT Certificate Exchange Messaging (CEM) – see Exchanging Certificates with Your Trading Partner for further information.

If emailing, use the Email Profile utility. This utility is also used to send your URL information. Even if the utility will not be used to forward your profile to your trading partner, the utility can be used to capture the information locally.

The Email Profile utility automatically exports the appropriate user certificate(s) for attachment. If you are not using the utility, you need to export your user certificate by hand. See Exporting certificates on page 668

Emailing a profile to your trading partner

You can use the Cleo Harmony, Cleo VLTrader, and Cleo LexiCom applications to create an email containing all the required profile information for a specified mailbox and send it to your trading partner. You an automatically include any profile information configured for a specified mailbox in this email. This information includes any URLs (if applicable) and necessary certificates.

To send your profile information to your trading partner, select a mailbox in the active tree pane, right click and select **Email Profile**

Note: You might need to extract your service's profile information prior to actually defining a host/mailbox relationship. To do this, select a service under the Local Listener, right-click and select **Email Profile**.

Note: This example is for AS2 mailboxes. The Profile Information section will differ by protocol.

Complete the information on the screen:

1. In the **To:** field enter the email address of your trading partner. If the mailbox is associated with a Trading Partner (see Managing Trading Partners on page 631) and the Trading Partner has Technical contacts, then a **Get Partner Contacts** button will be displayed. Clicking this button will fill the **To:** field with all the associated Technical contacts.

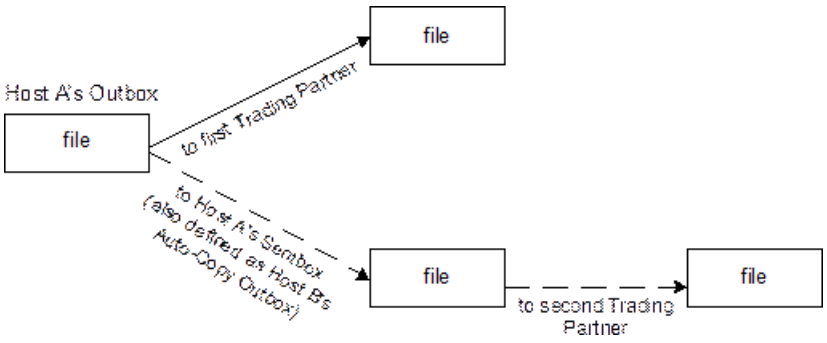
   a. You can also choose to send a copy of this email to your registered System Administrator Email address or to the email address that was specified in the primary contact information when you registered your product.
2. The **From:** field default value is taken from the System Administrator email address defined in the **Options > Other** panel. If this field contains multiple email addresses, only the first address is displayed.
3. Update the **Subject:** field as needed.
4. If multiple listening ports are specified (that is, HTTP and HTTP/s for AS2, ebMS, RosettaNet or WS; FTP, FTP/s Explicit and/or FTP/s Implicit for AS3 or FTP servers; or OFTP and OFTP/s or OFTP), multiple URLs are displayed. You can select and send any or all of the displayed URLs to your trading partner.
5. Choose the **Send all certificates in one zip file** option if your trading partner's email client has difficulty receiving files with a `.cer` extension for X509 certificates; `.asc` for PGP public keys; or `.pub` for SSH or OpenSSH public keys. (This is a common problem with MS Outlook.)
6. Optional - Type a message for your trading partner.
7. Click **Send**. A **Profile Confirmation** dialog box appears.
8. An additional Security Warning is displayed to indicate that this information will be sent in clear text via email over the internet. If you want to send anyway, click **Yes**. To suppress this Security Warning for future profiles that you email, select the **Do not show this message again** option at the bottom of this panel.

Sending a copy of a document to another host

If you have two trading partners (that is, hosts) configured, you can enhance your configuration to automatically send files to the second trading partner after the files have been successfully sent to the first trading partner using an *auto copy*. Given Host A (the original sender) and Host B (the additional sender), in most situations you would perform the following steps to configure auto copy:

- Add an auto copy action to Host B (steps 1-2 below).
- Configure Host A so that the files that have been sent are automatically deposited into the file source location (that is, the Outbox) for Host B's auto copy action (step 3 below).
- Configure the Host B auto copy action to automatically send the file when it is copied from Host A (step 4 below).

The following diagram illustrates the flow of the file that is sent using "Auto-Copy" (dotted lines signify dependence on successful completion of the file being sent to the first Trading Partner):



Auto-Copy Configuration

Follow the steps below to configure auto copy.

1. Create a new "uto copy action for Host B.
   a. In the Host B tree, right mouse-click the send action and select **Clone**.

      A new action called `newsend` is created.

   b. Rename the new action to `auto copy`. (The name is arbitrary; you can choose any name you want for your new action.)
2. In Host B's auto copy Action that you have just created, configure the `PUT` command with an `autocopy` subfolder in the path and a wildcard ("*") in the file name.
   a. **Wildcard Note:** Using a wildcard for the file name addresses the situation where Host A sends multiple files with the same file name before Host B can send the file. In that case, automatic versioning occurs (for example, `sendfile1.edi`, `sendfile2.edi`, etc.) in Host A's Sentbox, the file source location (that is, Outbox) for Host B's auto copy Action.
   b. **Subfolder Note:** Specifying the source path in the auto copy action differentiates Host B's auto copy Outbox location (...`\hosts\outbox\HostB\autocopy`) from the "normally used" Outbox location (...`\hosts\outbox\HostB`).
3. In the **General** tab for Host A, specify a Sentbox path that is the same as Host B's Outbox path.
4. In order for Host B to immediately send the file after Host A has successfully sent the file, configure the Host B auto copy action to run **whenever the action has a file to send**.
   a. Right-click Host B's auto copy Action (in the Tree pane) and select **Schedule...**
   b. A dialog box appears allowing you to schedule the action.
   c. Select **Whenever the action has files to send** and click **OK**.

Setting advanced host properties

1. Select the active host in the tree pane.
2. Select the **Advanced** tab in the content pane to display a list of advanced properties for that host.
3. Specify values for the properties as necessary. For information about host-specific properties, see the **Advanced** tab discussion for the host.

   You can condense the displayed list by selecting an item from the **Filter Group** drop-down list. To further filter the display, enter a case-insensitive string in the **Filter String** field. Note that for the Web UI you must press **Enter** after typing **Filter String** text.

You can also set properties using the `SET` command within an action; however, the `SET` value only affects the commands that follow the `SET` for that particular action.

Note that some host-level properties have associated system-level properties of the same name, for example, Email On Fail. See Advanced system options on page 743 for more information. For these properties, if a specific value is not set at the host-level, the associated system-level setting is displayed and used.

Working with actions

Actions are tasks for your host or mailbox. This section explains how to compose, run, and use actions.

Composing an action

An action is classified as a *Commands* action or a *JavaScript* action.

Note: JavaScript actions are supported only in the Cleo Harmony application.

For JavaScript actions, you can enter statements in a free-form manner. The Cleo Harmony application uses Rhino (http://www.mozilla.org/rhino), which is an open source, pure Java, JavaScript engine, to interpret and compile JavaScript source files into temporary Java classes for execution. Visit https://developer.mozilla.org/en/Rhino_JavaScript_Compiler.

See the API javadocs for examples and a description of the methods and functions available from within JavaScript (refer specifically to the ISessionScript class javadoc). The methods include the ability to run other action commands within JavaScript and writing to debug or the system log. These methods, when combined with JavaScript, make it possible to have complex sequences or decisions that would not be possible using Commands actions alone.

For Commands, an action consists of one or more commands that are to be run sequentially as a group. You can choose to have one action that does ALL sending and receiving, or you can choose to separate sending and receiving into two or more actions, potentially if sends and receives are not to be scheduled at the same intervals.

1. Select the action in the tree pane.
2. The potential set of commands depends on the client-to-host protocol.

   Note: HTTP derivatives like AS2, AS4, EBICS, ebXML, RNIF and WS generally only support a subset of the HTTP commands (typically only `PUT` and sometimes `GET`).

   The actual supported set of commands and their syntax is further dependent on the host type. For more information, see the section specific to the host type in question.

Table 9: Host Commands

	FTP	HTTP*	SSH FTP	OFTP	MQ	SMTP	HSP	MLLP	Purpose
`CONNECT`	X	X				X			Connect (login) to the host
`PUT`	X	X	X	X	X	X	X	X	Send one or more files to the host
`GET`	X	X	X	X	X			X	Receive one or more files from the host
`DIR`	X	X	X		X				Get a directory listing of available files from the host
`CD`	X		X						Changes the current directory on the host
`CONFIRM`		X							Confirm, on the host, receipt of one or more files
`DELETE`		X							Delete one or more files on the host
`REQUEUE`		X							Requeues one or more previously received files on the host
`QUOTE`	X		X			X			Send a raw command to the server
`SITE`	X								Send a site specific command to the server
`TYPE`	X								Sets file data type to ASCII or BINARY

Table 10: Local Commands

	FTP	HTTP*	SSH FTP	OFTP	MQ	SMTP	HSP	MLLP	Purpose
`SET`	X	X	X	X	X	X			Change an action property value

	FTP	HTTP*	SSH FTP	OFTP	MQ	SMTP	HSP	MLLP	Purpose
CLEAR	X	X	X	X	X	X			Clear an action string property
SYSTEM	X	X	X	X	X	X			Execute a local system command
WAIT	X	X	X	X	X	X			Pause
LCOPY	X	X	X	X	X	X			Copy local files
LDELETE	X	X	X	X	X	X			Delete local files
LREPLACE	X	X	X	X	X	X			Replace bytes in local files

Table 11: Extended Commands

	FTP	HTTP*	SSH FTP	OFTP	MQ	SMTP	HSP	MLLP	Purpose
CHECK	X	X	X	X	X	X			Check for certain events or non-events. (Cleo VLTrader and Cleo Harmony only)
SCRIPT	X	X	X	X	X	X			Run an external JavaScript command. (Cleo VLTrader and Cleo Harmony only)

3. Right-click in the empty space or on a command in the **Action** tab to display a menu. (Note that JavaScript actions will not contain the **Edit** or **Comment** options.)
   a. Select **Edit** to edit the current line using the dialog editor (refer to step 4).
   b. Select **Insert** (or the button) to insert a new line before the current line using the dialog editor (refer to step 4).
   c. Select **Move Down** or **Move Up** (or the and buttons) to move the current line down or up.
   d. Select **Comment** (or the button) to change the current command line to a comment line.
   e. Select **Delete** (or the button) to clear the current line.
4. The **Action** tab is a freeform editor. For JavaScript actions, type in your JavaScript. For Commands actions, if you are familiar with the supported commands and syntax, you can type commands in directly. Otherwise, you can use a dialog editor that will format commands for you. To open the dialog editor, click the wizard button. The wizard button is not available for JavaScript actions.
   a. Select the desired command from the list on the left.
   b. The dialog box prompts for source and destination paths (and allows for browsing), when applicable to the command and possible for the host type.
   c. Available options for the command are listed.
   d. For HTTP, the dialog prompts for any needed or optional parameter and/or header values for the command.
   e. For LCOPY zipping operations, the dialog prompts for any needed password information if AES encryption is being used.
   f. The resultant command text is displayed on the bottom line (native UI only).
   g. Edit as necessary and click **OK**.

Composing a host action

Note: Host actions are only available in the Cleo VLTrader and Cleo Harmony applications.

A *host action* consists of one or more commands that are to be run sequentially as a group (similar to a script). You may choose to have one host action that does all commands, or you may choose to have separate host actions, each performing different commands.

1. Right-click a host in the tree pane and select **New HostAction**.
2. Enter a unique hostaction alias and click **OK**.
3. Select the host action in the tree pane.

   The potential set of commands for host actions is given below:

Type	Command	Purpose
Local commands	`SET`	Change an action property value. See your host's command reference or to Local command reference on page 876 for a description of SET.
	`CLEAR`	Clear an action string property. See your host's command reference or to Local command reference on page 876 CLEAR Command for a description of CLEAR.
Extended commands	`CHECK`	Check for certain events or non-events (Cleo VLTrader and Cleo Harmony applications only). See CHECK command on page 943 for a description of CHECK.
	`SCRIPT`	Run an external JavaScript file. (Cleo VLTrader and Cleo Harmony applications only). See SCRIPT command on page 951 for a description of SCRIPT.

4. Right-click in the empty space or on a command in the **Actions** tab to display a menu.

   - Select **Edit** to edit the current line using the dialog editor (refer to step 4).
   - Select **Insert** (or the button) to insert a new line before the current line using the dialog editor (refer to step 4).
   - Select **Move Down** or **Move Up** (or the and buttons) to move the current line down or up.
   - Select **Comment** (or the button) to change the current command line to a comment line.
   - Select **Delete** (or the button) to clear the current line.

5. The **Actions** tab is a freeform editor. For JavaScript actions, type in your JavaScript. For Commands actions, if you are familiar with the supported commands and syntax, you can type commands in directly. Otherwise, a dialog editor is available to format commands for you. To open the dialog editor, click the wizard button.

   Note: The wizard button is not available for JavaScript actions.

   a) Select the desired command from the list on the left.

   The dialog prompts for source and destination paths and allows browsing.

   Available options for the command are listed. The resultant command text is displayed on the bottom line (native GUI only).

b) Edit as necessary and click **OK**.

Using operating system commands in actions

On Windows, a DOS command can be executed by using the /c option of the command program. A Unix command can be specified directly. For example, if file ‘x’ needed to be copied to file ‘y':

Operating System	LexiCom SYSTEM command
Windows 95/98	SYSTEM command.com /c copy x y
Windows NT/2000/XP	SYSTEM cmd.exe /c copy x y
Unix	SYSTEM cp x y

Note: If the command program can not be found, its location is probably not in the Path environment variable and you may need to specify its full path. The ComSpec environment variable should indicate its full path.

If the program that is being executed prints messages, it may fill up the standard out or standard error buffer and hang execution. To avoid this, pipe all the output to a file:

```
SYSTEM myprogram.exe > myprogram.log 2 > &1
```

```
2 > &1 pipes standard error to standard out.  If you don’t care to capture
 the output, pipe all the output to keyword ‘nul’:
```

```
SYSTEM myprogram.exe  >  nul 2 > &1
```

Also, when executing LexiCom from the command line, some Unix shells will expand file matching characters - * ? [ ] - ~ { and } - even when enclosed in double quotes - “” (e.g. –c “GET *” expands to –c GET as2bean.jar ftp.jar ftplog.txt …). To avoid this, try enclosing the wildcard character in double quotes “” and the entire argument in single quotes ‘’ (e.g. –c ‘GET “*”’).

Running and stopping an action

1. Once the required information for a *host* \ *mailbox* \ *action* branch has been supplied through the configuration panels, the action can be run.
2. Select the *action* in the tree pane.
3. To start the action, right-click the *action* and select **Run** or click in the **Action** tab. An action can also be run via command-line parameters. See Running from the command line on page 38.
4. To monitor progress, use the **Determine Status** and **Watch Messages** windows.
5. To interrupt the action, right-click the *action* and select **Stop** or click in the **Action** tab.

Host Technical Reference

The following sections explain each of the available types of hosts.

FTP and FTP/s Hosts

The generic FTP and FTP/s hosts enable a user to fully specify a client file transfer interface to an FTP server. If at all possible, use a pre-configured host specific to the target server; this will save the effort of having to research, specify, and then debug the interface.

The generic FTP host provides an interface over non-secure FTP. If you or your trading partner requires Secure Socket Layer (SSL) FTP, use the generic FTP/s host.

Not all FTP servers will support or require the full set of host commands allowed by VersaLex. At a minimum, the server must support PUT and/or GET. The following action commands are available on VersaLex:

	Command	**Purpose**	**Underlying FTP method**
Host commands	PUT	Send one or more files to the host	STOR
	GET	Receive one or more files from the host	RETR
	DIR	Get a directory listing of available files from the host	LIST
	CD	Changes the current directory on the host.	CHDIR
	QUOTE *command*	Sends a raw command to the server	command
	SITE	Sends a site specific command to the server	SITE
	TYPE	Sets file data type to ASCII or BINARY	TYPE
Local commands	SYSTEM	Execute a local system command	-
	WAIT	Pause	-
	SET	Sets a property	
	CLEAR	Clears a string property	
	LCOPY	Copy one or more local files	-
	LDELETE	Delete one or more local files	-
	LREPLACE	Replace bytes in one or more local files	-
	CHECK	Check for a transfer, file, or directory (VLTrader and Harmony only)	-

	Command	Purpose	Underlying FTP method
	SCRIPT	Execute a JavaScript File (VLTrader and Harmony only)	-

FTP Configuration

Activate either a trading partner-specific host or the generic FTP or FTP/s pre-configured host and then configure host, mailbox and actions.

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.

4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See FTP Host Configuration on page 95.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See FTP Mailbox Configuration on page 112.
   c) Click **Apply** to save your work.
6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See FTP Action Configuration on page 113.
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the native UI to prompt to you click **Apply** when changes are made. See Other system options on page 729. However, in the web UI, this is not valid. In the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

FTP Host Configuration

The FTP Host parameters indicate a host's location and how to reach it.

FTP Host: General Tab

Server Address

Either a fully qualified name (recommended) or an IP address.

Port

The FTP command port. You can specify either a specific port number or `-1` to indicate the default port for FTP (21) or FTP/s (990).

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` - Use either a direct connection to the internet or a VPN.

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For Cleo VLTrader and Cleo Harmony, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and/or Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

FTP Host: FTP Tab

Security Modes

For FTPs servers only.

Possible values:

- `None` - For servers that require Secure Socket Layer (SSL). Indicates non-secure transfers; commands and data are clear-text.
- `SSL Implicit` - For servers that support only SSL connections.
- `SSL Explicit` - For servers that support SSL through the use of either the `AUTH SSL` or `AUTH TLS` command.

Default value: `SSL Explicit`

Default Data Type

The data type used when transferring files to and from the FTP server.

Possible values: `ASCII` or `Binary`

Default value: `ASCII`

Data Channel Mode

The sets the default behavior for opening data port connections between the FTP client and FTP server.

Active mode

causes the client to listen for an inbound connection from the server during data transfers. The **Low Port** / **High Port**, if left at 0/0, will be a random number between 1024-65535; otherwise specify a specific range. Because this is active mode, this port range must be open inbound on your firewall.

Passive mode

causes the server to listen for an outbound connection from the client during data transfers. The server indicates the IP address and port number. The FTP server will cycle through port numbers, usually a subset of 1024-65535. **Substitute Passive IP Address** indicates that VersaLex should ignore the IP address specified by the server and reuse the command port address instead. (This may be necessary if the server is advertising an internal rather than an external IP address.)

FTP Host: Advanced Tab

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for FTP include:

Abort In Process Transfers

Indicates that the FTP server supports the `ABORT` command when a data transfer is interrupted.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Inbox

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Avoid List Command When Space In Path

When using the retrieving nested subdirectories (`GET -REC` option) and any of the nested subdirectories have spaces, indicates that the FTP server does not properly handle spaces in the `LIST` command path and that CDs should be used to avoid the issue.

Possible values: `On` or `Off`

Default value: `Off`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0` - `n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Data Socket Accept Timeout

The amount of time allowed for each read operation on the data port.

Possible values: `0` - `600` seconds, where `0` indicates no timeout.

Default value: `150` seconds

Delete Zero Length Files

Indicates whether files received that are zero-length (<= 5 bytes) should be deleted rather than processed.

Possible values: `On` or `Off`

Default value: `Off`

Disable Address Resolution

Indicates to connect directly to an IP address if the IP address is known and a DNS lookup is not desired.

Possible values: `On` or `Off`

Default value: `Off`

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by

including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Explicit SSL Command

Indicates the AUTH command to be used when the Security Mode specified on the Host/FTP tab is "SSL Explicit".

Possible values:

- `AUTH SSL`
- `AUTH TLS`
- `AUTH TLS-C`
- `AUTH TLS-P`

Default value: Depends on the requirements of the trading partner's FTP server.

Explicit SSL Post Command

A command or set of commands to be issued after the Explicit SSL Command and login sequence. The `PBSZ` and `PROT` commands ("PBSZ 0;PROT P") are required by some servers regardless of the AUTH type used and are necessary for data channel protection (AUTH TLS or AUTH TLS-C).

If multiple FTP commands are needed after the AUTH command, set this property to **all** of the commands separated by semicolons (;).

Note: For legacy reasons, this property applies to all connections whether secure or not, with the configured commands executing right after login.

File List Parse Method

The NLST commands on some FTP servers do not return a standard file list.

Possible values: `Tradanet` or `GXS NBT`

Default value: None

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0` - `n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Get Number of Files Limit

Limits the number of files retrieved from a server directory listing by one `GET` command.

Possible values: `0` - `n`

`0` indicates no limit.

Default value: `0`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

`Incoming`
`Outgoing`
`Both`

Ignore Exception After Quit

Indicates to ignore any I/O errors that occur when attempting to read the SMTP server response after issuing a `QUIT` command.

Possible values: `On` or `Off`

Default value: `Off`

Ignore Retrieve Error Code

Indicates an FTP server response code (after an FTP `RETR` request) that should not be treated as an error condition. This property is useful when the absence of a file on the server is not considered an error.

CAUTION: If the server uses the same error code for multiple reasons, this property can potentially mask unknown error conditions.

Possible values: Three-digit error code value.

You can specify multiple error codes separated by commas (,) or semicolons (;). Alternatively, you can use a regular expression (denoted by enclosing it in square brackets '[]') instead of a three-digit error code. For example, `[550.*No such file.*]` would ignore `550` errors containing 'No Such File'. If it is necessary to include a ',' or ';' in the regular expression, the character would need to be escaped (`\x2C` or `\x3B`) instead of using a comma or semicolon. See Using wildcards and regular expressions on page 69 for additional information.

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

Include Filename In Store Unique Command

Indicates whether the FTP server expects a starting filename to be included when using the store unique option (`PUT -UNI`).

Possible values: `On` or `Off`

Default value: `Off`

Interim Retrieve

Indicates to set result of any successfully retrieved file to `Interim Success` rather than `Success`. This would normally be used when transfer logging is being monitored by a backend system to allow coordination of any post processing of the received file that needs to occur prior to setting the transfer status to `Success`.

Possible values: `On` or `Off`

Default value: `Off`

Issue Command After Opening Data Connection

Indicates to issue the retrieve, store, or list command until after the data port connection has been established rather than before.

Possible values: `On` or `Off`

Default value: `Off`

Keepalive Noop Command (seconds)

Indicates the amount of time in-between issuing `NOOP` commands on the command port while a transfer is active on the data port. 0 indicates to not issue `NOOP`s.

Possible values: `0 - n`

Default value: 0

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more

restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Next File On Fail

When a download fails, indicates whether a wildcarded `GET` should proceed to the next available file rather than terminate if the server is still connected.

Possible values: `On` or `Off`

Default value: `Off`

Only Retrieve First Available File

Indicates a `GET *` should only retrieve the first available file from the server.

Possible values: `On` or `Off`

Default value: `Off`

Only Retrieve Last Available File

Indicates a `GET *` should only retrieve the last available file from the server.

Possible values: `On` or `Off`

Default value: `Off`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

Password Automatic Update (days)

If greater than zero and `Password Update Format` has been set, the number of days after which the software will generate and apply a new FTP password.

Possible values:`0-n days`

Default value: `0 days`

Password Update Format

If supported by the server, the format of the `PASS` command value when changing a user's password. The server dictates the format.

Use `%old%` and `%new%` keywords to specify the format, for example, `%old%/%new%`.

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512
```

Default value: `System Default`

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: `On` or `Off`

Default value: `On`

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: `On` or `Off`

Default value: `On`

PGP V3 Signature

Post Get Command

Post Put Command

In an action, specify commands to be executed only after a successful `GET` or `PUT` as post-get or post-put commands, respectively. When using this property, use a `SET` command within the action **before the `GET` or `PUT` command** rather than the **Advanced** tab.

The Post Put Command can be set to `QUIT`, which allows a disconnect and reconnect between file uploads when necessary.

If multiple FTP commands are needed after the `GET` or `PUT`, set this property to **all** of the commands separated by semicolons (;). If a specific FTP command needs to contain a semicolon, enclose that specific FTP command in quotes ("). Use of macro variables is supported. Refer to Using macro variables on page 59 (Post/Pre Command context) for a list of the applicable macros.

Pre Get Command

Pre Put Command

In an action, specify commands to be executed before a `GET` or `PUT` as pre-get or pre-put commands, respectively. This has the benefit of keeping the log results relative to just `GET`s and `PUT`s (especially important for Cleo VLTrader and Cleo Harmony `GET` transfer logging). In addition, for the `PUT`, it avoids connecting and

logging into the server when there are no files to send. When using this property, use a `SET` command within the action **before the `GET` or `PUT` command** rather than the **Advanced** tab.

If multiple FTP commands are needed prior to the GET or PUT, set this property to **all** of the commands separated by semicolons (;). If a specific FTP command needs to contain a semicolon, enclose that specific FTP command in quotes ("). Use of macro variables is supported. See Using macro variables on page 59 (Post/Pre Command context) for a list of the applicable macros.

Pre Put Change Directory

For `PUT` commands whose destination contains a directory path, forces an explicit `CWD` request to the destination directory path prior to issuing the `STORE` request.

Some FTP servers treat directories as logical rather than physical directories, and require directories be set only through a `CWD` request.

Possible values: `On` or `Off`

Default value: `Off`

Pre Put Command For First File Only

If a Pre Put Command is specified, indicates whether to execute them before each file being transferred by the `PUT` or only before the first file transfer.

Possible values: `On` or `Off`

Default value: `On`

REST Enabled

Allows the host to be accessible through the REST API. This feature is only supported on **AS2**, **AS4**, **FTP** and **SSH FTP** and *only when the host has exactly one mailbox*.

When this setting is enabled, new mailboxes cannot be created and the existing mailbox cannot be cloned, disabled, or removed.

Possible values: `On` or `Off`

Default value: `On` for **AS2**. **AS4**, **FTP** and **SSH FTP** when the host has exactly one mailbox. `Off` in all other cases.

Resume Failed Transfers

When selected and a transfer fails (and Command Retries > 0), attempt to resume the transfer on a retry. If OpenPGP is enabled on the packaging tab (see Configuring mailbox packaging on page 79), the entire file is transferred instead of resuming with a partial file. The server must support the `FEAT`, `SIZE`, and `REST STREAM` extensions to FTP. For more information, visit http://tools.ietf.org/html/rfc3659.

Possible values: `On` or `Off`

Default value: `Off`

Retrieve Directory Sort

Used to control the order in which files are downloaded from the FTP server. Using this property does cause the LIST command rather than the NLST command to be used when VersaLex is determining the available file list – which might be a problem if the server responds with different lists (e.g. NLST only lists files not previously downloaded while LIST lists all files regardless). Windows and Unix/Linux FTP servers are supported.

Possible values:

```
Alphabetical (ascending)
Alphabetical (descending)
Date/Time Modified (ascending)
Date/Time Modified (descending)
Size (ascending)
```

`Size (descending)`

Retrieve Last Failed File First

If a file download previously failed and you are attempting to `GET` a list of files again, this property indicates whether the previously failed file should be attempted first.

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

Reuse SSL Session

Indicates the command port SSL session should be reused when possible for any subsequent data port SSL connections. This setting does not affect the reuse of command port SSL sessions.

Possible values: `On` or `Off`

Default value: `Off`

Reuse SSL Sessions Across Actions

If selected, and if no forward proxy is being used for this host, SSL sessions from previous connections to the same destination (address and port number) may be resumed to avoid costly negotiation. If unselected, only SSL sessions used in the current action to the same destination may be resumed. When unselected, a new SSL session is created for the initial command port connection.

Possible values: `On` or `Off`

Default value: `On`

SSL Allow Legacy Renegotiation

When selected, legacy renegotiation is allowed. If this property is not selected, the extension described in RFC5746 is used for renegotiation and the server must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Possible values: `On` or `Off`

Default value: `On`

SSL Cipher

Indicates a specific cipher, or an ordered list of ciphers, to be used with the server for SSL key exchange, encryption, and hashing.

If not set (that is, left blank), the list of default ciphers (all standard ciphers, excluding anonymous and non-encrypting) is presented to the server and the server picks one. If a regular expression (enclosed in brackets) or a wildcard expression is specified, a list of implemented ciphers (all standard ciphers, including anonymous and non-encrypting) is presented to the server, based on the conditions of the pattern. For example, if a regular expression of `[.*ECDH.*]` is specified, then the list is a subset of all implemented ciphers that belong to the Elliptical-curve Diffie-Hellman group (for example, `ECDH` is in included in their string). In all cases, whenever a list is presented, it is always ordered by cryptographic strength, with the strongest listed first.

Based on the expression you type, the **List** button shows the resulting set of ciphers in the **SSL Cipher List** dialog box. Within this dialog box, you can view the list or select a specific cipher. If you select a cipher, then its value is displayed in this field.

Possible values:

Blank

a specific cipher picked from the SSL Cipher List dialog box

a regular/wildcard expression

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed. By default, this field is blank, designating that Cleo Harmony, Cleo VLTrader, or Cleo LexiCom will select the most recent version (currently TLS 1.3).

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed when selecting an SSL cipher. To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128`, or `256` (depending on the requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed. SSL 3.0 is the default value for compatibility with servers that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

Default value: `SSL 3.0`

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding CHECK commands: Terminate On Fail is only honored if the ConditionsMet parameter is set and the result of the CHECK is classified as Error. The CHECK command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: On or Off

Default value: On

Unzip Use Path

Indicates whether or not zip entry paths should be used for LCOPY -UNZIP operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: On or Off

Default value: On

Use EPRT and EPSV

Indicates to use Extended Port (EPRT) and Extended Passive (EPSV) commands for IPv6-style network addressing. EPRT/EPSV is used regardless of this setting if the host address is or resolves to an IPv6-style address.

Possible values: On or Off

Default value: Off

Use External IP Address in PORT request

Indicates for active (aka port) mode that the external rather than the local IP address should be included in data port requests to the FTP server.

Possible values: On or Off

Default value: Off

Use NLST

During a GET * command, indicates that VersaLex should use an NLST command rather than LIST when getting the list of files available for download.

Possible values: On or Off

Default value: On

Wait For Execute On

Indicates whether execution should wait for processing to complete within an Execute On Fail, Execute On Successful Copy, Execute On Successful Receive, or Execute On Successful Send command. Note that this option does not apply to native AS400 execution.

Possible values: On or Off

Default value: On

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If System Default is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

System Default
TripleDES
AES-128
AES-192
AES-256

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

FTP Mailbox Configuration

The FTP Mailbox parameters allow you access to the host system.

Note: This feature is being deprecated. For protocols other than AS3, use a Users host. See Users Host on page 516 for more information. For AS3, you can continue to use the FTP Users host and mailbox until further notice.

FTP Mailbox: FTP Tab

Note: By default, FTP hosts have the **REST Enabled** advanced property set to `On`, which prevents the host from having more than one mailbox. If you want more than one mailbox for this host, set the **REST Enabled** advanced property to `Off`. See FTP Host: Advanced Tab on page 97.

User Name

Password

FTP Account

Credentials for authentication to the FTP server. Select **No Password Required** if there is no password required for authentication.

FTP Account is optional.

FTP Mailbox: Security Tab

Note: This tab applies only to FTPs hosts.

Security Mode

Possible values:

- `None` - For non-secure transfers, and commands and data are clear-text.
- `SSL Implicit` - For servers that support only SSL connections.
- `SSL Explicit` - For servers that support SSL by using either the `AUTH SSL` or `AUTH TLS` command.

Client Certificate

If `SSL Explicit` or `SSL Implicit` is specified in the **Host FTP** tab, the target server can issue client certificates. In this case, import the client certificate using Certificate management on page 661 and then use the Certificate Alias and Password fields to specify (or browse for) the imported certificate.

FTP Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information regarding payload file packaging.

FTP Action Configuration

An action's parameters capture a repeatable transaction for your mailbox on the host system. Create a new action under the mailbox.

FTP Action: Action Tab

See Composing an action on page 89 and FTP Command Reference on page 113.

FTP Command Reference

Descriptions of commands and their options, arguments, and parameters.

CHECK

See CHECK Command for information about this command.

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

Comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

DIR

Get a directory listing of available files from the host

```
DIR "source"
```

source

Remote source directory path

GET

Receive one or more files from the host

```
GET [-ASC|-BIN] [-REC] [-DEL] [-UNI|-APE] "source" "destination"
```

ASC

Transfer file in ASCII format.

BIN

Transfer file in Binary format.

REC

Recursively retrieve nested subdirectories.

When you use the REC option, nested server directory structure is maintained locally.

When you use the REC option in conjunction with the DEL option, the retrieved files are deleted from the server, but the subdirectories remain.

DEL

If `GET` is successful, delete remote file.

UNI

Ensure local filename is unique.

APE

Append to existing destination file.

source

Remote source path

destination

Local destination path. Use of macro variables is supported. See Using Macro Variables (Destination File context) for a list of the applicable macros.

- Path can be to a filename or to a directory.
- If relative path, then uses user's home directory.
- Use of macro variables is supported. See Using Macro Variables (Destination File context) for a list of the applicable macros.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.

- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"input bytes"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"output bytes"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

PUT

Send one or more files to the host.

```
PUT [-ASC|-BIN] [-DEL] [-UNI|-APE] "source" "destination"
```

ASC

Transfer file in ASCII format

BIN

Transfer file in Binary format

DEL

If `PUT` is successful, delete local file.

UNI

Ensure remote filename unique

APE

Append to existing destination file

source

Source path

- path can be to a filename or to a directory
- * and ?, or a regular expression, are supported in filename. See Using wildcards and regular expressions on page 69 for additional information.
- if relative path, then uses user's home directory
- usage of macro variables is supported. See Using Macro Variables (Source File context) for a list of the applicable macros.

destination

Remote destination path. Use of macro variables is supported. See Using Macro Variables (Destination File context) for a list of the applicable macros.

QUOTE

Send a raw command to the FTP server

```
QUOTE "command"
```

source

Command to be sent to the server. (Example: PWD, CWD, DELE) See the FTP RFC 959 for more details on specific FTP commands.

SCRIPT

See SCRIPT command on page 951 for information about this command.

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

SITE

Sends a site-specific command to the server.

```
SITE "command"
```

command

Site specific command with any arguments

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"path"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

TYPE

Set the default data type for file transfers.

```
TYPE "data type"
```

data type

ASCII or Binary

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

HTTP and HTTP/s Hosts

Not all HTTP servers will support or require the full set of host commands allowed by Cleo Harmony. At a minimum, the server must support PUT and/or GET. The underlying HTTP method that the command uses is dependent on the specific HTTP server. The following action commands are available in Cleo Harmony:

	Command	Purpose	Underlying HTTP method
Host commands	CONNECT	Connect (log in) to the host	Always POST
	PUT	Send one or more files to the host	Either POST or PUT
	GET	Receive one or more files from the host	Either POST or GET
	PUT+GET	Send one or more files to the host and receive one or files from the host in return	Always POST
	DIR	Get a directory listing of available files from the host	Either POST or GET
	CONFIRM	Confirm, on the host, the receipt of one or more files	Always POST
	DELETE	Delete one or more files on the host	Either POST or DELETE
Local commands	SET	Change an action property value	-
	CLEAR	Clears an action string property value	-
	SYSTEM	Execute a local system command	-
	WAIT	Pause	-
	LCOPY	Copy one or more local files	-
	LDELETE	Delete one or more local files	-
	LREPLACE	Replaces bytes in one or more local files	-
	CHECK	Check for a transfer, file, or directory (VLTrader and Harmony only)	-
	SCRIPT	Execute a JavaScript File (VLTrader and Harmony only)	-

HTTP Configuration

First activate either a trading partner specific host or the generic HTTP or HTTP/s pre-configured host (see below). The generic HTTP host provides an interface over non-secure HTTP. If interfacing to a server that requires use of the Secure Socket Layer (SSL) over HTTP, then the generic HTTP/s host must be used.

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.
4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See HTTP Host on page 121.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See HTTP Mailbox on page 137.
   c) Click **Apply** to save your work.
6. For Cleo LexiCom users only: Enter trading partner configuration information.
   a) Click the new host in the tree pane.
   b) Enter trading partner configuration information on the **Indentifier** tab in the content pane. See HTTP Trading Partner on page 138.
   c) Click **Apply** to save your work.
7. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See HTTP Command Reference on page 139.
   c) Click **Apply** to save your work.
8. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the product to prompt to you click **Apply** if you try to leave the page. However, in the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

HTTP Host

A host's parameters specify its location and how it is reached.

The product uses the information you provide in the **General** and **HTTP** tabs to build HTTP URLs when an action is run.

HTTP Host: General Tab

The product uses the information you provide in the **General** and **HTTP** to build HTTP URLs when an action is run.

Server Address

Either a fully qualified name (recommended) or an IP address for the HTTP host.

Port

The HTTP command port. You can specify either a specific port number or `-1` to indicate the default port for HTTP (80) or HTTP/s (443).

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` -

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For the Cleo VLTrader and Cleo Harmony applications, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and/or Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Note: If the host has an external association, the default directories might be managed outside of VersaLex applications and not shown here.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

HTTP Host: HTTP Tab

The product uses the information you provide in the **General** and **HTTP** to build HTTP URLs when an action is run.

HTTP/HTTPs

For HTTPs servers only.

Possible values: `HTTP` or `HTTPs` - If the server requires Secure Socket Layer (SSL), select `HTTPs`. .

Check certificate server name

Only available if you select `HTTPs`. Verifies that the server name in the received SSL server certificate matches the server name actually connected to.

Method

Select a method for each command supported by the server. See HTTP and HTTP/s Hosts on page 120.

- The server might not require `CONNECT` (login) because:
  - The server may not need to identify the client, or
  - Instead, the other commands may have parameters that identify the client, or
  - Over SSL, the server may make use of client certificates to identify the client.
- The server must at least support `PUT` and/or `GET`.
- If the server supports `GET`, it usually will support `DIR`; otherwise it is difficult to get files without first knowing which files to get.
- The server might support `CONFIRM` or `DELETE` (usually not both).
- The server might support `REQUEUE`.

If the `DIR` command is supported by an `HTTP POST` method, information concerning how to parse the directory listing returned by the server is required. This information is potentially used by `GET` or `CONFIRM` or `DELETE` commands to extract the available file "identifiers" one-by-one from the directory listing.

- Line delimiter* - set of one or more characters that marks the end of a line in the directory
- Header lines - number of header lines to be ignored at the beginning of the directory.
- Field delimiter* - set of one or more characters that separates fields in a line
- File identified - location in the line of the available file "identifier"
  - at position - the file id always starts at this column position (first column in line is 1)
  - by tag - the file id always follows this set of one or more characters
  - at field # - the file id is always this field # (first field in line is 1)

* Special escape sequences can be used to identify certain characters:

`\s` - space character
`\t` - tab character
`\n` - newline character
`\r` - carriage return character
`\\` - slash character

Path

Supply the server **Path** for each of the commands. Depending on the server implementation and the methods used, some or all the paths might be the same or some or all might be different.

Parameters

Headers

Specify required and optional **Parameters** and **Headers** for each of the commands.

Add custom parameters and additional headers as needed. The values for these will be available on the receiving side either through the properties passed to the ILexiComIncoming Java API or by accessing `ISessionScript.getTrigger()` in a JavaScript action scheduled for a new file arrives event.

If the `Content-type` is `multipart/form-data`, any configured headers will become `form-data` parts.

Rule	Syntax	Example
If the parameter/header has one static value. If a parameter value includes an ampersand (&) or a vertical bar (|) or if a header value includes a comma (,) or a vertical bar (|), precede with a backslash (\& or \, or \\|).	name=value	key=1
If the parameter/header contains a macro variable, it must be enclosed within two percent signs (e.g., "%index%"). See Using macro variables on page 59 (Destination File context) for further details on macro usage. Note that "macros" should not be confused with "keywords" (e.g., "%dir) that are also supported within the parameter/header values.	name=value	key=MY_NAME_%index%_%date%
If the parameter/header can have one or more possible values, separate with vertical bars (|). To include a description with a possible value, separate the value and description with two percent signs (%%).	name=|value1|...|	type=|EDI|X12|
If the parameter/header can have unknown values	name=	user=
If the parameter/header value, when entered, should be masked, precede with an asterisk (*)	*name=	*psw=
If the parameter/header is optional, enclose with brackets ([...])	[name=value] [name=|value1|...|] [name=] [*name=]	[type=|EDI|X12|]
If the parameter/header should be sent to the server even when a value has not been entered, precede it with a plus sign (+) and enclose with brackets ([…])	[+name=]	[+value=]

Rule	Syntax	Example
If the parameter is not a name=value pair but just a value, include the = before the value	=value	=true
If more than one parameter, separate with ampersands (&)	name=value&name=value	user=&*pswd=
If more than one header, separate with commas (,)	name=value,name=value	recvr=%tp,type=|EDI|X12|
If the parameter/header value can potentially be filled in via a trading partner branch (LexiCom) or the Trading Partner table (VLTrader and Harmony), use the keyword %tp	name=%tp	recvr=%tp
If the parameter/header value is the contents of the source file being transferred, use the keyword %file	name=%file	file=%file
If the parameter/header value is the name of the source file being transferred, use the keyword %file.name	name=%file.name	filename=%file.name
If the parameter/header value is the extension of the source file being transferred, use the keyword %file.extension	name=%file.extension	filetype=%file.extension
If the parameter/header value can potentially be filled in from the results of a DIR command (one-by-one), use the keyword %dir	name=%dir	filename=%dir
If the parameter/header value should include a uniquely generated message identifier, use the keyword %messageID.	name=%messageID	id=%messageID
If the parameter/header value should always be sent to the server with no value, use the keyword %empty.	name=%empty	attribute=%empty

HTTP Host: Advanced Tab

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for HTTP or HTTP/s include:

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0` - `n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Delete Zero Length Files

Indicates whether files received that are zero-length (<= 5 bytes) should be deleted rather than processed.

Possible values: `On` or `Off`

Default value: `Off`

Disable TE Headers

When selected, disables the TE and Transfer Encoding request headers.

Possible values: `On` or `Off`

Default value: `Off`

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On`

`Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

- `\r` - carriage return
- `\n` - new line (linefeed)
- `\f` - form feed
- `\t` - horizontal tab
- `\0` - null
- `\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0 - n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Get Number of Files Limit

Limits the number of files retrieved from a server directory listing by one `GET` command.

Possible values: `0 - n`

`0` indicates no limit.

Default value: `0`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Full HTML PUT Response

Allows the full HTML response from the server to be logged rather than just the return status.

Possible values: `On` or `Off`

Default value: `Off`

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Next File On Fail

When a download fails, indicates whether a wildcarded `GET` should proceed to the next available file rather than terminate if the server is still connected.

Possible values: `On` or `Off`

Default value: `Off`

Omit Name Parameter From Content Type

When selected, the applicable file name is not included in the Content-Type header.

Possible values: `On` or `Off`

Default value: `Off`

Only Download If Directory Line Changed

When selected, the application only downloads a file as part of a `GET -DIR` command if the server's directory entry for the file has changed since the last download. If you cannot delete a file off the server after it is downloaded AND the directory listing returns a file's last modified time/date and size, then this will prevent it from re-downloading the file.

For this property to work properly, the same action must be used for each download, as the previous directory listing is saved with the specific action.

Possible values: `On` or `Off`

Default value: `Off`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512
```

Default value: `System Default`

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: `On` or `Off`

Default value: `On`

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: `On` or `Off`

Default value: `On`

PGP V3 Signature

Post Parameters On Request Line

Indicates that web server does not accept `POST` parameters via application/form-data or application/x-www-form-urlencoded content-types but instead requires that the `POST` parameters be on the HTTP request line.

This setting is ignored if the Content-type is explicitly set to multipart/format-data.

Possible values: `On` or `Off`

Default value: `Off`

Reset Connection After Timeout On Response

When enabled will cause an immediate reset on the socket (instead of a graceful close) when a `SocketTimeoutException` occurs.

Possible values: `On` or `Off`

Default value: `Off`

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

Reuse SSL Sessions Across Actions

If selected, and if no forward proxy is being used for this host, SSL sessions from previous connections to the same destination (address and port number) may be resumed to avoid costly negotiation. If unselected, only SSL sessions used in the current action to the same destination may be resumed. When unselected, a new SSL session is created for the initial command port connection.

Possible values: `On` or `Off`

Default value: `On`

Server Type

Indicates a specific HTTP server that requires special processing of the outbound message or the returned response.

Possible values: Any server from the supported list.

SSL Allow Legacy Renegotiation

When selected, legacy renegotiation is allowed. If this property is not selected, the extension described in RFC5746 is used for renegotiation and the server must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Possible values: `On` or `Off`

Default value: `On`

SSL Cipher

Indicates a specific cipher, or an ordered list of ciphers, to be used with the server for SSL key exchange, encryption, and hashing.

If not set (that is, left blank), the list of default ciphers (all standard ciphers, excluding anonymous and non-encrypting) is presented to the server and the server picks one. If a regular expression (enclosed in brackets) or a wildcard expression is specified, a list of implemented ciphers (all standard ciphers, including anonymous and non-encrypting) is presented to the server, based on the conditions of the pattern. For example, if a regular expression of `[.*ECDH.*]` is specified, then the list is a subset of all implemented ciphers that belong to the Elliptical-curve Diffie-Hellman group (for example, `ECDH` is in included in their string). In all cases, whenever a list is presented, it is always ordered by cryptographic strength, with the strongest listed first.

Based on the expression you type, the **List** button shows the resulting set of ciphers in the **SSL Cipher List** dialog box. Within this dialog box, you can view the list or select a specific cipher. If you select a cipher, then its value is displayed in this field.

Possible values:

Blank
a specific cipher picked from the SSL Cipher List dialog box
a regular/wildcard expression

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed. By default, this field is blank, designating that Cleo Harmony, Cleo VLTrader, or Cleo LexiCom will select the most recent version (currently TLS 1.3).

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed when selecting an SSL cipher. To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128`, or `256` (depending on the requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed. SSL 3.0 is the default value for compatibility with servers that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

Default value: `SSL 3.0`

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Store Raw Sent Message

When this property is enabled, a copy of the outbound message is stored in the OFTP/sent directory.

Possible values: `On` or `Off`

Default value: `Off`

Successful Put Response Phrase

Even if the server response code is a 200 level response, if the configured phrase is not found anywhere in the content of the server response, the PUT is not considered successful.

Possible values: Any string. The comparison to the server response is not case-sensitive.

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

System Default
TripleDES
AES-128
AES-192
AES-256

Default value: System Default

Zip Comment

Specifies the comment to be added to the zip archive file in LCOPY -ZIP operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for LCOPY -ZIP operations. If System Default is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

System Default
9 - (Best Compression)
8
7
6
5
4
3
2
1
0 - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for LCOPY -ZIP -REC operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (*) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: On or Off

Default value: On

HTTP Mailbox

A mailbox's parameters allow you access to the host system.

HTTP Mailbox: HTTP Tab

Specify default values for various command parameters and headers.

The parameters and headers listed are those identified in the host **HTTP** tab that have neither static values nor special %file and %dir associations.

Provide **Default Values** for any of the parameters and headers for mailbox-level actions. Unless an overriding value is specified within the command in an action, these default values are used.

HTTP Mailbox: Authenticate Tab

If the target server requires WWW authentication, select the appropriate type and provide the required username and password and optionally realm.

HTTP Mailbox: Security Tab

The **HTTP** and **HTTP/s** radio buttons are read-only. They reflect the settings from the host **HTTP** tab.

If **HTTP** is selected, no further action is necessary on this tab.

If **HTTP/s** is selected, the target server can issue client certificates. In this case, import the client certificate using Certificate Manager (see Certificate management on page 661) and then specify (or browse for) the imported **Certificate Alias** and **Password**.

HTTP Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information about payload file packaging.

HTTP Trading Partner

Note: This section applies to the Cleo LexiCom application only. (Cleo Harmony and Cleo VLTrader application users should use the Trading Partner Table to specify this Trading Partner Identifier. See Managing Trading Partners on page 631.)

A trading partner's parameters define a unique identifier on the host system. Create a new trading partner under the host.

1. Right-click the host in the *active* tree pane.
2. Select **New Trading Partner** to create a new lower branch. Then, optionally, type a new alias in the content pane panel and click **Apply**.

HTTP Trading Partner: Identifier Tab

Trading partners are provided as a convenience. Rather than having to repeat the trading partner's identifier perhaps multiple times in various commands, the identifier can be specified once and the trading partner alias referenced as needed.

The trading partner alias is more human-readable and in the command dialog editor, trading partner aliases are available through pull-down menus.

Note: If the target server interface does not require that a trading partner be identified via a parameter or header value in any of the HTTP commands, then there is no need to create trading partner branches. This is usually the case when the file content itself (like EDIX12) identifies the trading partner (receiver) id.

HTTP Action

An action's parameters capture a repeatable transaction for your mailbox on the host system. Create a new action under the mailbox.

HTTP Action: Action Tab

Use the **Action** tab to configure commands within an action.

The commands specified on the host **HTTP** tab (plus the local commands) are available for use. See Composing an action on page 89 and HTTP Command Reference on page 139.

If a parameter or header value on the host **HTTP** tab has been marked with the keyword `%tp`, the value specified for the parameter or header in the action can be `%trading partner`, where *trading partner* is the alias of one of the trading partners under the host (LexiCom) or a Trading Partner from the Trading Partners Table (VLTrader and Harmony). When the command is run, the trading partner's identifier is filled in for the value.

Note: If a parameter or header value has an embedded space, a `\s` must be used to represent the space within the command For example, `%OPQ\scompany` represents `%OPQ company`. This is done automatically in the dialog editor. If a space is left in the value, the command is not parsed correctly.

HTTP Command Reference

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

CONFIRM

Confirm, on the host, the receipt of one or more files

```
CONFIRM -DIR name=value,...
```

-DIR

Confirm file(s) received using directoy listing from the host.

If the `DIR` command is not supported on the server, the argument is not applicable and cannot be used. See to HTTP Configuration on page 121.

name =value,...

HTTP parameter=value and header=value pair.

The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See HTTP Configuration on page 121. An optional parameter or header is enclosed in brackets ([...]).

CONNECT

Connect (login) to the host

```
CONNECT name=value,...
```

name =value

HTTP parameter=value and header=value pairs

The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See HTTP Configuration on page 121. An optional parameter or header is enclosed in brackets ([...]).

DELETE

Delete one or more files on the host.

```
DELETE -DIR "source" parm/header=value,...
```

-DIR

Delete one or more files using a directory listing from the host.

If the `DIR` command is not supported on the server, the argument is not applicable and cannot be used. See to HTTP Configuration on page 121.

"*source*"

Remote source path

- If the underlying HTTP method for the command on the server is POST, the argument is not applicable and cannot be used. See HTTP Configuration on page 121.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

name =value,...

HTTP parameter=value and header=value pair.

The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See HTTP Configuration on page 121. An optional parameter or header is enclosed in brackets ([...]).

DIR

Get a directory listing of available files from the host.

```
DIR "source" "destination" name=value,...
```

"*source*"

Remote source path

- If the underlying HTTP method for the command on the server is POST, the argument is not applicable and cannot be used. See HTTP Configuration on page 121.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Local destination path.

- Path can be to a filename (unless the `-DIR` option is used) or to a directory.
- If you specify a relative path, the command uses the default inbox.
- If you do not specify a path, the command generates messges rather than files.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

name =value,...

HTTP parameter=value and header=value pair.

The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See HTTP Configuration on page 121. An optional parameter or header is enclosed in brackets ([...]).

GET

Receive one or more files from the host.

```
GET -DIR -CON -DEL -UNI|-APE "source" "destination" name=value,...
```

-DIR

Get one or more files using a directory listing from the host.

-CON

If the command is successful, confirm on the host that file was received. If the `CONFIRM` command is not supported on the server, the argument is not applicable and cannot be used. See HTTP Configuration on page 121.

-DEL

If the command is successful, delete host files. If the DELETE command is not supported on the server, the argument is not applicable and cannot be used. See HTTP Configuration on page 121

-UNI

Ensure the copied filename is unique.

-APE

If local filename exists, append copied file to existing file.

"source"

Remote source path

- If the underlying HTTP method for the command on the server is POST, the argument is not applicable and cannot be used. See HTTP Configuration on page 121.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"destination"

Local destination path.

- Path can be to a filename (unless the `-DIR` option is used) or to a directory.
- If you specify no path or a relative path, the command uses the default inbox.
- One `*` is supported with canned prefix and/or suffix in filename.
- You can use macro variables. See Using macro variables on page 59 (Destination File context) for a list of the applicable macros.
- You can use `%HTTP.header.XXXX%` macro where *XXXX* references an HTTP header name in the server's response and is replaced with the header's value.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

name =value,...

HTTP parameter=value and header=value pair.

The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See HTTP Configuration on page 121. An optional parameter or header is enclosed in brackets ([...]).

HTTP Comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.

- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

PUT

Send one or more files to the host.

```
PUT -DEL -UNI "source" "destination" name=value,...
```

-DEL

If `PUT` is successful, delete local file.

-UNI

Ensure remote filename unique

"*source*"

Source path

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses default outbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

destination

Remote destination path. Use of macro variables is supported. See Using macro variables on page 59 (Destination File context) for a list of the applicable macros.

name =value

HTTP parameter=value and header=value pairs

The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See HTTP Configuration on page 121. An optional parameter or header is enclosed in brackets ([...]).

PUT+GET

Send one or more files to the host and receive one or more files from the host in return.

```
PUT+GET -DEL -UNI|-APE "source" "destination" name=value,...
```

-DEL

If the command is successful, delete the local file.

-UNI

Ensure the local filename is unique.

-APE

If local filename exists, append to existing file.

"*source*"

Local source path

- Path can be to a filename or to a directory
- You can use * and ?, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default outbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Local destination path.

- Path can be to a filename or to a directory.
- If you specify no path or a relative path, the command uses the default inbox.
- One * is supported with canned prefix and/or suffix in filename.
- You can use macro variables. See Using macro variables on page 59 (Destination File context) for a list of the applicable macros.
- You can use %HTTP.header.XXXX% macro where *XXXX* references an HTTP header name in the server's response and is replaced with the header's value.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

name =value,...

HTTP parameter=value and header=value pair.

The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See HTTP Configuration on page 121. An optional parameter or header is enclosed in brackets ([...]).

SCRIPT

See SCRIPT command on page 951 for information about this command.

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"path"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

AS2 Hosts

The AS2 standard provides the ability to securely transport EDI (and other data, including binary and XML) to a remote host.

This guarantees that the message has not been changed in-transit and is received and can be read only by the intended trading partner. A Message Disposition Notification receipt (MDN) further guarantees that the intended trading partner has received the message.

AS2 uses the HTTP protocol as its transport mechanism to send files over the Internet. Cleo VersaLex software uses the `PUT` (HTTP POST) action command to transport the secure data to the remote host.

CleoVersaLex software supports AS2 versions 1.0, 1.1, 1.2, and 1.3.

AS2 Process Map

This section outlines the configuration necessary to set up the Generic AS2 host.

- AS2 Configuration on page 147
- Acquiring your trading partner's signing and encryption certificates on page 86
- Determining and providing your URL information on page 85
- Creating and providing your signing/encryption certificates on page 86
- Complete configuration of:
  - Local Listener on page 750
  - AS2 Host Configuration on page 148
  - AS2 Mailbox Configuration on page 166
  - Composing an action on page 89
- Testing Your AS2 Installation on page 171

AS2 Configuration

A host describes the remote server of your trading partner to which messages will be sent. The host's parameters specify its location and how it is reached. Your remote trading partner should provide information to you in the form of a URL, which is used to configure the host parameters.

To configure a generic AS2 pre-configured host:

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.

4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See AS2 Host Configuration on page 148.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.

b) Enter mailbox-level configuration information on the tabs in the content pane. See AS2 Mailbox Configuration on page 166.
c) Click **Apply** to save your work.

6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See AS2 Action on page 170.
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the product to prompt to you click **Apply** if you try to leave the page. However, in the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

AS2 Host Configuration

A host describes the remote server of your trading partner to which messages will be sent. The host's parameters specify its location and how it is reached. Your remote trading partner should provide information to you in the form of a URL, which you will use to configure the host parameters.

This section describes how to configure a generic AS2 pre-configured host.

AS2 Host: General Tab

Server Address

Either a fully qualified name (recommended) or an IP address.

This is the address of your trading partner's server that will receive your messages.

Port

The port on the server where your trading partner will receive your messages.

Default value: `80` for HTTP and `443` for HTTPs (SSL)

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` - Use either a direct connection to the internet or a VPN.

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Specifying default host directories on page 700 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For the Cleo VLTrader and Cleo Harmony applications, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and Outbox. See Specifying default

host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Note: If the host is has an external association, the default directories might be managed outside of the Cleo Harmony application and not shown here.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

AS2 Host: AS2 Tab

Partner Is CEM-Capable

Specifies whether the trading partner is capable of sending and receiving certificates through Certificate Exchange Messaging (CEM) and allows you to enable **Send** in **Certificate Exchange**. See Exchanging certificates with your trading partner on page 672.

Possible values:

- `True`: Indicates your trading partner specifies their AS2 product is capable of processing CEM messages but they have not yet sent messages with the header designating their AS2 product's CEM capability.

  Note: This field should only be manually set to *True* if your trading partner has specifically stated that their AS2 product is CEM-Capable.
- `False`: Indicates your trading partner is not CEM-capable. However, when messages are received from a trading partner with the appropriate header designating that it is CEM-capable, this value is automatically changed to *True*.
- `False and Ignore Further Detection`: Indicates your trading partner is not CEM-capable and disables automatic updating of this value based on inbound trading partner messages.

Default value: `False`

Override AS2 Service Filename Preservation MDN Response Settings

Use **Override AS2 Service Filename Preservation MDN Response Settings** to select settings different from the system settings defined in the **AS2 Service > AS2 Tab** (see Configuring AS2 Service on page 767,) and then use **Generate Filename Preservation MDN Responses** to toggle Filename Preservation for this trading partner.

Filename Preservation is a feature designed for trading relationships requiring stringent file-naming rules. AS2 products complying with Filename Preservation use the *Content-Disposition* header within the message payload to name the file and when this feature is enabled, a file name must be included in the payload and must conform to specific file-naming rules. Additionally, this feature detects when a file name has already been used within a designated period of time (defined in the AS2 Service: AS2 Tab) and alerts the trading partner with the appropriate warning or error disposition in the returned MDN.

When selected and different from the system setting, the **Duplicate Filename Action** is also enabled, allowing the following choices:

- **Retain as Unique, Return Warning**: A warning will be returned to the trading partner in the MDN, the message payload will be stored in the *rejectbox* subdirectory (it will not be made available for back-end processing) and an error will be logged.
- **Reject Payload, Return Error**: An error will be returned to the trading partner in the MDN, no payload will be stored and an Exception will be logged.

Note: Whenever **Generate Filename Preservation MDN Responses** is selected (either using or overriding the system setting), **Overwrite duplicate file names** and **Use default file name** are disabled.

Overwrite duplicate file names

Allows for unique naming of stored files. When this check box is selected, any files that exist in the specified inbox will be overwritten. When cleared, incoming files with the same name as one that already exists will be appended with a unique number beginning with 1 and incremented each time a new file is saved.

Use default file name

Allows the incoming file to be given the name specified in its associated field. Use this option to override the file name specified by the sender. This feature is useful in situations where the received file name must be something other than its original file name, and is common for IBM i / iSeries (AS/400) platforms where the file name must be specified with a .mbr extension. This field can also include any of the supported macros allowing for the incoming file to be named, for example, with a date-time stamp. Subdirectory path identifiers (i.e., '/' or '\') can also be used in conjunction with macros to allow filtering of the incoming file to a specific subdirectory under the inbox based on the value of the macro variable. See Using macro variables on page 59 (Destination File context) for a discussion of all applicable macros.

Note: If a subdirectory path is specified and it does not already exist, it will automatically be created as needed unless the subdirectory path is under an inbox on the AS/400 Native File System. In that case, the physical file denoting the subdirectory path (in the form: DIRECTORY.FILE) must be created under the specified inbox before files can be written to it.

Add Content-Type Directory to Inbox

allows for sorting of incoming messages based on content-type to a subdirectory (under the Inbox specified on the **General** tab). Specify each of the Content-Types that you would like directed to specific subdirectories by entering a name in the **Directory** field. Directory entries may be made for Content-Types of: EDIFACT, X12, XML, Binary, Plain Text, EDI Consent and Other (a default catch-all for messages with all other Content-Types you could receive). The same subdirectory can be used for multiple Content-Types. You can also leave Directory entries blank, which will cause any received messages of that Content-Type to be stored in the Inbox specified on the **General** tab.

For IBM i / iSeries (AS/400) usage, see AS/400 Setup and installation on page 703 or AS/400 Network Access Setup on page 980 for information on configuring the Content-Type Inbox settings to access the Native File System (NFS).

Note: If you use this feature, incoming messages will be placed in the specified folder based on the content type specified in the HTTP header of the message. The Cleo Harmony application does not check the actual content of the message to determine its content type.

AS2 Host: HTTP Tab

Outbound

Indicates whether you use SSL or not for outbound file transfers.

HTTP

Do not require use SSL

HTTP/s

Require SSL for outbound file transfers.

If you select HTTP/s, you can select **Check certificate server name**

Inbound

HTTP/s only

Require your trading partner to use Secure Socket Layer (SSL) for inbound file transfers.

Command

In most cases the `CONNECT` command is not used and should be left blank. In rare instances, CONNECT is required by the remote server to identify the client, particularly if SSL has not been used.

Method

The only valid **Method** for AS2 commands is `PUT` ("`POST`").

Path

The server **Path** for the `PUT` command.

If the remote server is also using the Cleo Harmony application, the path is either `/as2` for newer installations or `/` for older installations. The resource path must be properly specified in order for your trading partner's AS2 installation to process messages from you. Given the URL provided by your remote trading partner in the form:

`http(s)://remote-host:port/`***`resource-path`***`?optional-parameters`

Enter the bolded portion in this field (if it was supplied).

Parameters

By default, no **Parameters** are specified for sending AS2 messages. If parameters are required, they must be obtained from your trading partner when the trading relationship is established. Given the URL provided by your remote trading partner in the form:

`http(s)://remote-host:port/resource-path?`***`optional-parameters`***

Enter the bolded portion in this field (if it was supplied).

Headers

At a minimum, the following **Headers** must always be specified in order to properly send AS2 messages:

- **AS2-From** - the alias of the sender of the AS2 message.
- **AS2-To** - the alias of the receiver of the AS2 message.

Note: The **AS2-From** / **AS2-To** fields are determined and agreed upon as part of the initial setup of the trading relationship. These fields could be company-specific, such as DUNS number, or

could simply be an agreed-upon identification string. The **AS2-From** / **AS2-To** combination is case-sensitive and must be unique across all hosts defined in your system, since this combination is used to determine into which Inbox messages are stored when received from remote hosts.

- **Subject** - identifies the message and is returned in the human-readable section of an MDN, if requested.
- **Content-Type** - specifies the format of the message being sent and is used by the sending and receiving applications to properly assemble and parse the message. Currently supported content types (in the pull-down menu) are:
  - EDIFACT
  - X12
  - XML
  - Binary
  - Plain Text
  - EDI Consent

Note: Entering a value for the **Content-Type** header is optional. If **Content-Type** is not specified or if multiple payloads are attached in the message, the **Content-Type** is detected based first on file content and then the file extension. Detectable types include `application/edifact`, `application/edi-x12`, `application/edi-tradacoms`, `application/xml` (text/xml), `application/pdf`, `application/msword`, `application/x-msexcel`, `application/rtf`, `application/zip`, `image/bmp`, `image/gif`, `image/tiff`, `image/jpeg`, `text/plain`, `text/html`, and `video/mpg`.

These header fields are filled in at the Mailbox or Action level and specify values to be set in the HTTP headers that precede the body (actual content) of the message to be sent.

AS2 Host: Advanced Tab

The host's **Advanced** tab contains several property settings fields. These settings typically do not affect your ability to connect to a host. However, you might want to change some of these settings when configuring a runtime environment.

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for AS2 include:

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Allow Duplicate Incoming Message IDs

Ignores messages with duplicate message IDs and allows reprocessing of the message.

Possible values: `On` or `Off`

Default value: `Off`

Async MDN Preferred Port

When non-zero, defines the preferred port on which asynchronous MDNs will be returned from the trading partner.

Note: This setting will always override any port settings defined on the Listener and AS2 Service panels; and VLProxy's reverse-proxy port, if applicable.

Possible values: `1 – 65535`

Default value: `0`

Async MDN Resends

When sending a payload that has requested an asynchronous MDN, specifies the maximum number of attempts that will be made to resend the payload after the specified "Async MDN Timeout" has been exceeded and the MDN has still not been received.

When returning an asynchronous MDN in response to a received payload, specifies the maximum number of attempts that will be made to resend the asynchronous MDN to the trading partner (e.g., when the outbound connection cannot be established).

Possible values: Any value `-1`, `0` or `> 0`. When set to a value other than the default (-1), this value overrides the setting in the Local Listener.

Default value: `-1`

Async MDN Retry Delay

When resending an asynchronous MDN because the initial attempt to send it has failed, specifies the number of seconds to wait in between those resend attempts.

Possible values: Any value `0` or `> 0`

Default value: `60`

Async MDN Timeout

The maximum time (in minutes) to wait for an asynchronous MDN to be received before either resending the payload (if Async MDN Resends > 0 in either the Host or Listener) or logging an error.

Possible values: Any value `-1`, `0` or `> 0`. When set to a value other than the default (-1), this value overrides the setting in the Local Listener.

Default value: `-1`

Base64 Encode Content

Base64 is the encoding format used by Multi-purpose Internet Mail Extension (MIME) for transmitting non-text material over text-only communications channels. Base64 is based on a 64-character subset of US-ASCII, enabling 6 bits to be represented per printable character.

Possible values: `On` or `Off`

Default value: `Off`

Canonicalize Inbound Signed Content

When this option is selected, a canonicalizer is used to ensure that '\r' and '\n' characters always occur together as '\r\n'. This option may be used when the inbound signature hash verification fails and the trading partner is using OpenSSL to sign its messages.

Possible values: `On` or `Off`

Default value: `Off`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0` - `n`

Default value: `0`

Compression- Signing Order

When both signing and compression are enabled, indicates which is applied first.

Possible values: `Sign then compress` or `Compress then sign`

Default value: `Sign then compress`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Delete Zero Length Files

Indicates whether files received that are zero-length (<= 5 bytes) should be deleted rather than processed.

Possible values: `On` or `Off`

Default value: `Off`

Disable TE Headers

When selected, disables the TE and Transfer Encoding request headers.

Possible values: `On` or `Off`

Default value: `Off`

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Repetitive Listener Failures

When "Email On Fail" is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host,

an email alert will be sent when the failure is resolved. Failure resolution email alerts will not be sent for general Listener failures since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Repetitive Listener Failures

When `Execute On Fail` is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, the `Execute On Fail` command will be executed again when the failure is resolved. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure. Executions of the "Execute On Fail" command for resolution of general Listener failures will not be done since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *`n`* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0 - n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: 0

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of 0 does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: 0 - n

Default value: 0

Outbox Sort

Controls the order in which multiple files are transferred for a PUT command. If System Default is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For Alphabetical ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

System Default
Alphabetical
Date/Time Modified

Default value: System Default

Outgoing Insert EOL Between Interchanges

If Fixed Record Outgoing Insert EOL is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: On or Off

Default value: Off

Override Listener CEM Auto Accept Setting

When selected, overrides the Auto Accept Received Certificate (CEM) Advanced setting in the Listener allowing auto accepting of CEM requests to be allowed or disallowed on a per host basis. See Exchanging certificates with your trading partner on page 672.

Possible values: On or Off

Default value: Off

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If System Default is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

System Default

ZIP
ZLIB

Default value: System Default

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If System Default is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish

Default value: System Default

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If System Default is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512

Default value: System Default

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: On or Off

Default value: On

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: On or Off

Default value: On

PGP V3 Signature

Put Multiple Files Limits

Limits the number of files included in each generated multipart message when using the `PUT -MUL` option. The limit is only applied when sending out of a single directory; when sending multipart out of separate subdirectories, the files are kept as a group and not broken up into separate messages.

Possible values: `-1 - n`

`-1` indicates no limit.

Default value: `-1`

Reset Connection After Timeout On Response

When enabled will cause an immediate reset on the socket (instead of a graceful close) when a `SocketTimeoutException` occurs.

Possible values: `On` or `Off`

Default value: `Off`

REST Enabled

Allows the host to be accessible through the REST API. This feature is only supported on **AS2**, **AS4**, **FTP** and **SSH FTP** and *only when the host has exactly one mailbox*.

When this setting is enabled, new mailboxes cannot be created and the existing mailbox cannot be cloned, disabled, or removed.

Possible values: `On` or `Off`

Default value: `On` for **AS2**. **AS4**, **FTP** and **SSH FTP** when the host has exactly one mailbox. `Off` in all other cases.

Resume Failed Transfers

When selected and a transfer fails (and Command Retries > 0), attempt to resume the transfer on a retry. If OpenPGP is enabled on the packaging tab (see Configuring mailbox packaging on page 79), the entire file is transferred instead of resuming with a partial file. The server must support the `FEAT`, `SIZE`, and `REST STREAM` extensions to FTP. For more information, visit http://tools.ietf.org/html/rfc3659.

Possible values: `On` or `Off`

Default value: `Off`

Retain Temporary Inbound Message Files

Leaves any files that are used while processing inbound messages in the `temp\` folder. The default action is to delete these files after processing has completed. These files may be helpful for problem diagnosis.

Note: These temporary files are retained for seven days.

Possible values: `On` or `Off`

Default value: `Off`

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

RSA-OAEP Key Algorithm Parameter

Represents the type of mask generation and hash generation functions that are applied when the `RSAES-OAEP` key algorithm is in use. See RFC4055 for a further description of the mask and hash generation functions.

Possible values: `MGF1-SHA1`, `MGF1-SHA256`, `MGF1-SHA512`

Default value: `MGF1-SHA1`

SSL Allow Legacy Renegotiation

When selected, legacy renegotiation is allowed. If this property is not selected, the extension described in RFC5746 is used for renegotiation and the server must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Possible values: `On` or `Off`

Default value: `On`

SSL Cipher

Indicates a specific cipher, or an ordered list of ciphers, to be used with the server for SSL key exchange, encryption, and hashing.

If not set (that is, left blank), the list of default ciphers (all standard ciphers, excluding anonymous and non-encrypting) is presented to the server and the server picks one. If a regular expression (enclosed in brackets) or a wildcard expression is specified, a list of implemented ciphers (all standard ciphers, including anonymous and non-encrypting) is presented to the server, based on the conditions of the pattern. For example, if a regular expression of `[.*ECDH.*]` is specified, then the list is a subset of all implemented ciphers that belong to the Elliptical-curve Diffie-Hellman group (for example, `ECDH` is in included in their string). In all cases, whenever a list is presented, it is always ordered by cryptographic strength, with the strongest listed first.

Based on the expression you type, the **List** button shows the resulting set of ciphers in the **SSL Cipher List** dialog box. Within this dialog box, you can view the list or select a specific cipher. If you select a cipher, then its value is displayed in this field.

Possible values:

Blank
a specific cipher picked from the SSL Cipher List dialog box
a regular/wildcard expression

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed. By default, this field is blank, designating that Cleo Harmony, Cleo VLTrader, or Cleo LexiCom will select the most recent version (currently TLS 1.3).

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed when selecting an SSL cipher. To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128`, or `256` (depending on the requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed. SSL 3.0 is the default value for compatibility with servers that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

Default value: `SSL 3.0`

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Store Raw Sent Message

When this property is enabled, a copy of the outbound message is stored in the OFTP/sent directory.

Possible values: `On` or `Off`

Default value: `Off`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Use Content Type For File Extension

By default, inbound messages that do not specifically contain the name of the target file to be saved are stored using the value of the `Message-ID` (of that message) with the `.file` extension. When this option is selected,

inbound messages without a target file name specifier is stored using the `Message-ID` and the appropriate file extension based on the Content-Type of the message.

Possible values: `On` or `Off`

Default value:

`Off` for existing hosts
`On` for newly cloned hosts

Use Folded Headers For Outbound Messages

Enables or disables automatic line wrapping of HTTP headers exceeding 76 characters. By default headers are not folded since some non-Cleo product remote hosts using Microsoft Internet Information Server (IIS) cannot handle folded headers properly. Unless your host has been pre-configured to enable folded headers, leave this setting cleared!

Possible values: `On` or `Off`

Default value: `Off`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

`System Default`
`TripleDES`
`AES-128`
`AES-192`
`AES-256`

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`

4
3
2
1
0 - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

AS2 Mailbox Configuration

A mailbox's parameters allow you access to the remote host and define the security of the file being sent. You can use the AS2 mailbox wizard to configure for the most common setup. See Using the wizard to create a host or mailbox on page 79. The following sections describe the mailbox parameters.

AS2 Mailbox: AS2 Tab

Note: By default, AS2 hosts have the **REST Enabled** advanced property set to `On`, which prevents the host from having more than one mailbox. If you want more than one mailbox for this host, set the **REST Enabled** advanced property to `Off`. See AS2 Host: Advanced Tab on page 152.

The mailbox's **AS2** tab allows you to select the desired encryption and signing for sending messages and the optional desired security for receiving messages. If an MDN receipt is desired, you can also select the format and delivery method of that receipt.

Request

Specify the S/MIME format for messages to send to the remote host.

- Unsigned / unencrypted (neither **Encrypted** nor **Signed** selected)
- Signed (only **Signed** selected)
- Encrypted (only **Encrypted** selected)
- Signed / Encrypted (both **Signed** and **Encrypted** selected)

Receipt

Enables the **MDN Receipt** section. See MDN Receipt on page .

Encryption Algorithm

When **Encrypted** is selected, the **Encryption Algorithm** field is enabled and allows you to choose the encryption algorithm for the message to be sent to the remote host. The remote host must be able to decrypt the message using the algorithm you choose. For a non-Cleo Harmony trading partner, it is important to verify that your trading partner can use the selected algorithm prior to sending an encrypted message. The default encryption algorithm is `TripleDES`. See Cryptographic Services on page 975 for more information on choosing an encryption algorithm.

Key Algorithm

When **Encrypted** is selected, the **Key Algorithm** field is enabled and allows you to choose the algorithm to encrypt the content encryption key with the public key of your trading partner's encryption certificate. Your trading partner uses the private key of their encryption certificate to decrypt the content encryption key that is subsequently used to decrypt the content of the message.

Possible values:

- `RSA` (default)
- `RSAES-OEAP`

Signature Algorithm

When **Signed** is selected, the **Signature Algorithm** is used to encrypt the hash value of the signature with the private key of your signing certificate. Your trading partner uses the public key of your signing certificate to decrypt the hash value of the signature that authenticates you as the sender of the message. When **RSA** is selected, the selected **Hash/MIC Algorithm** is used to determine the appropriate signature algorithm, for example, `rsaEncryption`, `sha256WithRSAEncryption`, `sha384WithRSAEncryption` or `sha512WithRSAEncryption`. If **RSASSA-PSS** is selected, the combination of the private key of your signing certificate and the hash algorithm is used in conjunction with the RSASSA-PSS algorithm to secure the signature.

Possible values:

- `RSA` (default)
- `RSASSA-PSS`

Hash/MIC Algorithm

When the **Signed** option in the **Request** section is selected, the combination of the signature algorithm and the selected hash algorithm is used to secure the signature.

Note: If the RSASSA-PSS signature algorithm is used and the SHA-512 hash algorithm is selected, the strength of the signature algorithm of your signing certificate must be SHA256withRSA or better.

When the Signed option in the MDN Receipt section is selected, the selected Hash/MIC Algorithm is used to compute the independent Message Integrity Check (MIC) that is returned in the MDN Receipt.

Possible values:

- `SHA-1` (default)
- `MD5` (cryptographically weak and should not be used unless no other Hash/MIC algorithm is available)
- `SHA-256`
- `SHA-384`
- `SHA-512`

Compress Content

Compresses the message using ZLIB compression. Compression is generally used for large files so that the message will conserve bandwidth and be transferred more efficiently and securely over the Internet.

Inbound Message Security

Indicates how inbound messages should be received.

Select any combination of **Force Encryption**, **Force Signature** and **Force MDN Signature** to check the level of inbound message security. If the message is not received according to the corresponding message security settings, the message is rejected and an error is logged.

By default, no settings are selected. If no settings are selected, the security level of the message is not checked.

See AS2 Checklist on page 979, item 13 for determining the type of request being sent.

MDN Receipt

Attributes of the Message Disposition Notification (MDN) receipt you requested.

Message Disposition Notifications can be returned Synchronously (as part of the same HTTP session, that is, the MDN is returned during the acknowledgement phase of the message response) or Asynchronously (as part of a new HTTP session, that is, just the HTTP status message is returned during the acknowledgment phase of

the message response and the MDN is returned later in a separate HTTP POST message.) The receiver must be capable of handling the specified delivery method; some non-Cleo Harmony hosts may not be able to return either a synchronous or asynchronous MDN. This information must be obtained and noted during the initial set-up of the trading relationship. Cleo Harmony can handle either method of delivery.

Signed

Compute and remember an independent hash over the content of the sent message using the Hash/MIC Algorithm you select. The trading partner returns the MDN with a digital signature; and computes an independent MIC value over the content of the message it received (using the same MIC algorithm) and returns this value as a base64-encoded value in the human-readable portion of the MDN. When the MDN is received, the original MIC is compared against the received MIC. When the MIC values match, the sender is guaranteed that the message read by the trading partner is identical to the message that came from the sender and was not modified in any way.

Forward MDN to Email

Forward a copy of the MDN received via HTTP or HTTPS (either synchronously or asynchronously) to the email address specified in the **Email Address** field. When the asynchronous SMTP option is selected, the **Forward MDN to Email** field is disabled.

An additional feature available in Cleo Harmony is the ability to forward a copy of the MDN received via HTTP or HTTPS (either synchronously or asynchronously) to an email recipient when **Forward MDN to Email** is selected.

Synchronous

Return the MDN as part of the same HTTP session, that is, the MDN is returned during the acknowledgment phase of the message response. You must determine whether the receiver can handle this delivery method and plan accordingly.

Asynchronously

Return the MDN as part of a new HTTP session, that is, just the HTTP status message is returned during the acknowledgment phase of the message response and the MDN is returned later in a separate HTTP `POST` message.

When you select **Asynchronous**, you can choose the method used to process the message returned:

- **HTTP**: The MDN is received and processed by the local non-secure listener configured in the Local Listener Panel.
- **HTTPS**: The MDN is received and processed by the local SSL listener configured in the Local Listener Panel.
- **SMTP**: The MDN is emailed to the trading partner.

Note: When you select `SMTP`, you must provide the **Email Address** where the MDN will be sent. The **Email Address** field is only enabled for editing when you select `SMTP` as the delivery method.

See AS2 Checklist on page 979, items 17 and 18, for determining the MDN delivery method.

See AS2 Checklist on page 979, items 15 and 16, to determine the type of MDN response that will be requested.

AS2 Mailbox: Certificates Tab

Use this tab to associate a trading partner's signing and encryption certificates with this mailbox and to override your own Local Listener's signing and encryption certificates, if necessary.

Acquire your trading partner's signing/encryption certificates and provide your trading partner with your signing/encryption certificates. See Acquiring your trading partner's signing and encryption certificates on page 86 and Creating and providing your signing/encryption certificates on page 86.

Trading Partner's Certificates

Encryption Certificate

The name of the file containing your Trading Partner's encryption certificate. Specify a value or click **Browse** to navigate to the file you want to select.

Signing Certificate

Select the check box to enable the field.

The name of the file containing your Trading Partner's signing certificate. Specify a value or click **Browse** to navigate to the file you want to select.

If you do not specify a signing certificate, the Cleo Harmony application uses all the certificates in its certificate store to determine if the signature of the incoming data message is trusted.

Use encryption certificate

Indicates that your trading partner uses the same certificate for signing and encryption, which is the general practice among most trading partners. When you select this check box, the **Signing Certificate** field is populated with the same certificate you selected in the **Encryption Certificate** field.

If the remote host is capable of receiving Certificate Exchange Messages (CEM) or you want to email your certificates to your trading partner, you can send your user and SSL certificates to the remote host by clicking **Exchange Certificates**.

My Certificates

Override Local Listener Certificates

Enables fields where you specify signing and encryption certificates to use with this particular partner instead of the certificates you configured for the Local Listener. See Configuring certificates for Local Listener on page 758.

If you override the default certificates, you must also exchange the certificates you specify here with your partner.

Signing Certificate Alias

The name of the signing certificate registered with the Cleo Harmony application through the Certificate Manager. The certificate must be the same as the one exchanged with your remote trading partners, unless you want to override it at the Mailbox level. See Local HTTP Users Configuration on page 834.

Click **Browse** to view and select a certificate. Enter the **Password** for your signing certificate's private key.

Encryption Certificate Alias

The certificate for decrypting your trading partner’s messages, if you have created or obtained a separate certificate.

Click **Browse** to view and select a certificate. Enter the **Password** for your encryption certificate.

Use signing certificate

Select this check box to use the same certificate for signing and decrypting your trading partner's messages. The **Encryption Certificate Alias** and **Password** are populated to match the **Signing Certificate Alias** and disabled.

Exchange Certificates

Invokes the **Certificate Exchange** dialog box. If you override the default the certificates, you must exchange these alternate certificates with your trading partner.

AS2 Mailbox: HTTP Tab

Use the mailbox's **HTTP** tab to assign default values to message headers.

For example, your AS2 name (`AS2-From`) and your trading partner's AS2 name (`AS2-To`) as well as the `Subject` and `Content-Type` of the documents to be transferred.

Default Value

You can assign a default value for each of the headers defined on the **AS2 Host: HTTP** tab. (See AS2 Host: HTTP Tab on page 151.) Unless an overriding value is specified within the command in an action, these default values are used. (See AS2 Checklist on page 979: item 5 for the **AS2-From** value, item 6 for the **AS2-To** value, and item 14 for the default **Content-Type** value.)

At a minimum, the following **Headers** must always be specified in order to properly send AS2 messages:

- **AS2-From** - the alias of the sender of the AS2 message.
- **AS2-To** - the alias of the receiver of the AS2 message.

  Note: The **AS2-From** / **AS2-To** fields are determined and agreed upon as part of the initial setup of the trading relationship. These fields could be company-specific, such as DUNS number, or could simply be an agreed-upon identification string. The **AS2-From** / **AS2-To** combination is case-sensitive and must be unique across all hosts defined in your system, since this combination is used to determine into which Inbox messages are stored when received from remote hosts.
- **Subject** - identifies the message and is returned in the human-readable section of an MDN, if requested.
- **Content-Type** - the format of the message being sent and is used by the sending and receiving applications to properly assemble and parse the message. Currently supported content types (in the pull-down menu) are:
  - EDIFACT
  - X12
  - XML
  - Binary
  - Plain Text
  - EDI Consent

  Note: Entering a value for the **Content-Type** header is optional. If **Content-Type** is not specified or if multiple payloads are attached in the message, the **Content-Type** is detected based first on file content and then the file extension. Detectable types include `application/edifact`, `application/edi-x12`, `application/edi-tradacoms`, `application/xml` (text/xml), `application/pdf`, `application/msword`, `application/x-msexcel`, `application/rtf`, `application/zip`, `image/bmp`, `image/gif`, `image/tiff`, `image/jpeg`, `text/plain`, `text/html`, and `video/mpg`.

AS2 Mailbox: Authenticate Tab

If the target server requires WWW authentication, select the appropriate type and provide values for **Username** and **Password** and, optionally, **Realm**.

AS2 Mailbox: Security Tab

If you specified HTTP/s in the host's **HTTP** tab, a remote host might issue client certificates. In this case, import the client certificate using **Certificate Manager** and then use the **AS2 Mailbox Security** tab specify (or browse for) the imported Client Certificate's alias and password. See Certificate management on page 661.

AS2 Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information regarding packaging of payload files.

AS2 Trading Partner

A trading partner's parameters define a unique identifier on the host system. By default, the **Trading Partner** branch is not created since it is not needed for AS2 transactions.

AS2 Action

An action's parameters define a repeatable transaction for your mailbox defined for the host system.

AS2 Action: Action Tab

See Composing an action on page 89 and HTTP Command Reference on page 139. See AS2 Host: Advanced Tab on page 152 for information about the available property values.

Sending Multiple Files within the Same Payload

By default, AS2 messages contain a single file within the payload (i.e., the message being sent). However, some supply chains require that multiple files that are related to each other (perhaps with different content types) be sent together within the same message.

To send multiple files within the same payload:

1. Select **Multiple file payload** from the Command Wizard or include the `-MUL` option on the `PUT` command line.
2. Group the related files to be sent either in your designated outbox or within a subdirectory under your designated outbox. Files that you do not want to be sent should not be stored in this subdirectory.
3. Optionally, enter the **Destination** file names. This field can include any of the supported macros allowing for the outgoing files to be named, for example, with a date-time stamp. See Using macro variables on page 59 (Destination File context) section for information about applicable macros.
4. Run the action.

   Inbound messages containing multiple files within the same payload are stored together in a subdirectory under the designated inbox.

   The directory is named in the form:

   ```
   YYYYMMDD-HHMMSS-CCC
   ```

   where:

YYYY	current year
MM	current number of the month (01-12)
DD	current day of the month
HH	current hour
MM	current minute
SS	current second
CCC	current fraction of a second

Testing Your AS2 Installation

Before you attempt to have a trading relationship with a partner, you should successfully test and validate that you can and receive messages at your local installation. This helps you narrow down connectivity issues caused by firewall problems and not by improper installation and configuration.

1. The **AS2-To** and **AS2-From** must have the same values in order for the file being sent to be properly stored in your configured Inbox. (Refer to the Loop Test **General** tab for current Inbox settings.)
2. Verify that the encryption certificate defined on the Local Listener panel (Encryption Certificate Alias) matches the one defined in the Trading Partner's **Encryption Certificate** field on the Loop Test **Certificates** tab.
3. Verify that your Local Listener is running.
4. If you've chosen asynchronous SMTP delivery or Forward MDN to Email, verify you have provided a valid email address in the **Email Address** field on the mailbox **AS2** tab.

5. Click the green arrow on the toolbar in the **Action** tab to run the test command. Messages similar to the ones shown below appear in the messages pane in the lower portion of your Cleo Harmony application.

This transaction log describes the following events that occurred when the command was executed:

- The command `PUT test.edi` was invoked
- The file (`test.edi`) was sent to from the outbox\ directory under the Cleo Harmony directory tree
- The file was assembled into a message that was both signed and encrypted using the TripleDES encryption method
- The **AS2-From** and **AS2-To** headers were both set to **LOOPTEST**
- The received message was identical to the message that was sent (signified by matching MIC codes)
- An MDN was received and was stored in the `mdn\` subdirectory under the Cleo Harmony directory tree

AS2-Specific Directories

The following additional directories are created either during the AS2 installation or as needed by the application:

Directory	Purpose
lostandfound\	Default inbox where incoming payload will be deposited when the application can't determine where to put it.

Directory	Purpose
AS2\	Location where raw (unprocessed) incoming and outgoing messages are stored. Incoming messages are located in the **AS2\received** directory and outgoing messages are located in **the AS2\sent** directory. These files can be helpful in diagnosing problems. Old files should be deleted or archived by the user, if necessary. The **AS2\unsent** directory contains raw header, data and message setup information files. These files are used if a message needs to be retransmitted and are deleted automatically by the application once the message transfer has either completed successfully or has failed due to timeouts, exceptions, or the number of retries has been exhausted. The **AS2\mdn** directory contains subdirectories for received (and optionally sent) MDNs. This directory may be changed on the AS2 Service Panel. MDNs may be automatically archived by the application or manually archived by the user from the **MDNs** tab on the listener panel. Archived MDNs are stored in `AS2\mdn\received\archive\mdn.zip` or `AS2\mdn\sent\archive\mdn.zip`. The **AS2\data** directory contains AS2msgs.txt and AS2files.txt files used by the application to determine the receipt of duplicate messages and duplicate file names. Entries in these files are retained for the time intervals configured on the **AS2 Service** page. See Local Listener AS2 Service on page 767. When a message is received from a trading partner who has enabled the **AS2 Restart** feature (i.e., the inbound message contains a valid Etag header), the **AS2\restart** directory will contain a header file named with the Etag value and a .as2restart extension and the partially received message file (named with Etag value and a _rcv extension). These files can be used to resume a transfer from the previous point of failure. When the entire message has been successfully received these files are removed; otherwise they will be retained for 24 hours after the last failure.
temp\	Temporary location where incoming messages can be stored while they are being processed by the application. By default, they are deleted automatically once the message has been completely processed; however these files can be kept for problem diagnosis by using the **Retain Temporary Inbound Message Files** host-level Advanced property. (These temporary files will automatically be deleted after 7 days.)

AS2 Firewall Considerations

Note: This section refers to your firewall settings, and not settings within VersaLex. You should contact your systems administrator with questions pertaining to your firewall.

If your server is behind a firewall and/or your trading partner's server is behind a firewall, it will be necessary to configure the firewalls to allow VersaLex to properly exchange messages with your remote trading partner. Depending on the type of firewall set up, the following settings in your firewall should be modified:

1. Incoming and outgoing messages should be allowed from and to your remote trading partner's IP addresses or qualified host name.
2. The port for your trading partner's remote server should be opened for outgoing messages.

3. The port(s) that you configured for your Local Listener should be opened to allow incoming messages.

AS2 Troubleshooting

Following is a list of potential problems while using VersaLex for AS2. The list covers general problems only. For technical support, please call 1-866-444-2536 or email support@cleo.com.

Note: Technical support is on a paid subscription basis. Refer to the section **Cleo Technical Support Subscription Programs** for information.

Problem	Possible Cause	Possible Solution
Could not listen on port XXXX - Address in use: JVM_BIND (Generated when an attempt is made to start the Local Listener.)	Port XXXX defined on the listener's HTTP panel is already being used by another application.	Use the "netstat -an" command (if available) to verify that the port is in use. Stop the listener, if it is running. Define a different port on the HTTP panel and restart the listener.
Result: Error - Method GET is not implemented by this server (Generated by the Local Listener receiving incoming messages)	A remote user is attempting to access your Local Listener using a web browser by entering your URL in the form: http://your-host-address:your-port/your-resource-path/ The VersaLex Listener is only capable of processing HTTP POST requests, but messages from web browsers are sent as HTTP GET requests.	If the message is coming from a bona fide trading partner, ask them to send you messages using POST requests instead of GET requests. If the message is from an unknown/unwanted source, modify your firewall settings to reject messages from the incoming IP address or change the setting for the **Unknown Partner Message Action** in the Local Listener's **Advanced** tab to either **Ignore** or **Reject**.
Result: Connection refused: connect	Remote server is currently not running or is not listening on the specified port.	Contact your trading partner regarding the availability of the server and verify the configured host and port settings are correct.
Result: Operation timed out: connect	Remote server is running but is not able to receive messages from you.	Verify firewall settings on the sending and receiving ends are properly configured.
Result: Timeout waiting for response	The action is unable to fully complete (i.e., complete transfer to remote host, decryption and/or signature verification) within the specified ConnectionTimeout period.	Increase the default ConnectionTimeout value on the **Host/Advanced** panel or increase the ConnectionTimeout value for the individual Action.

Problem	Possible Cause	Possible Solution
Result: Warning - Undefined AS2-To/AS2-From Relationship (Generated by the Local Listener receiving incoming messages)	The incoming **AS2-To** and **AS2-From** header values do not match exactly with local **AS2-From** and **AS2-To** settings or the settings have not yet been defined. **Note:** Your **AS2-To** value should be your trading partner's **AS2-From** value and your **AS2-From** value should be your trading partner's **AS2-To** value.	Verify that there is an entry for the designated **AS2-From** / **AS2-To** setting. Verify your **AS2-To** header value matches your trading partner's **AS2-From** header value and vice versa. These values are case-sensitive and there must be only one instance of the pair defined in your installation.
Result: Warning - MDN processing warnings occurred at the remote host. See MDN for further details. (Generated when sending a message to the remote host.)	A warning occurred at the remote host. The message was still correctly processed. Commonly reported warnings are Undefined AS2-To / AS2-From Relationship and Duplicate file received.	View the associated MDN to diagnose the cause of the warning and perform any corrective action as necessary.
Result: Error - MDN processing errors occurred at the remote host: authentication failed - see MDN for further details (Generated when sending a message to the remote host.)	The remote host was unable to verify the signature of your signed message.	Verify that you have successfully sent your signing certificate to your trading partner and that it was properly installed at the remote host.
Result: Exception - Certificate chain not trusted! (Generated when receiving a message from a remote host.)	Some of the certificates listed in the signature of the received message are missing in VersaLex's store of trusted certificates.	Verify that all CA certificates used by your trading partner's signing certificate have been received and installed in VersaLex.
Result: Exception - The signature could not be verified! (Generated when receiving a message from a remote host.)	The Local Listener was unable to verify the signature of a remote host's signed message.	Verify that you have successfully received and installed your trading partner's signing certificate.
Result: Exception - The trading partner's encryption certificate could not be found! (Generated when attempting to send an encrypted message to a remote host.)	VersaLex was unable to find the **Trading Partner's Encryption Certificate** defined on the Mailbox's Certificate Panel.	Verify the file defined on the Mailbox's Certificate panel exists and has not been accidentally deleted. Click **Browse** to choose a new encryption certificate.

Problem	Possible Cause	Possible Solution
Result: Error - MDN processing errors occurred at the remote host: decryption failed - see MDN for further details (Generated when sending a message to the remote host.)	The remote host was unable to decrypt your encrypted message.	Verify that you have successfully installed your trading partner's encryption certificate and have properly selected that certificate on the Mailbox's **Certificate** panel. Verify the remote host is able to decrypt messages according to the Encryption Method specified on the Mailbox's **AS2** panel.
Result: Exception - The message could not be decrypted! (Generated when receiving a message from a remote host.)	The Local Listener was unable to decrypt a remote host's encrypted message.	Verify that you have successfully received and installed your trading partner's encryption certificate.
WARNING: Source file is zero-length. (Generated when sending a message to the remote host.)	An attempt was made to send a file with no content. The file will still be sent, but there may be unexpected results on the receiving end.	Verify that the intent is to send files of zero-length and ignore any error messages generated due to this condition.

AS3 Hosts

Use generic AS3 Hosts to specify an AS3 installation based on a specific AS3/FTP server product.

This includes the product's specific server choreography, or the commands needed to successfully log in to the remote server and send and receive files. The product choreography for each generic AS3 host was established during AS3 interoperability testing with the server products, and a generic host for all interoperability-certified AS3 products is included in the VersaLex installation. Since these hosts were created for a test environment, you might need to adjust some settings and commands to establish successful file transfers in a production environment. If it is available, use a pre-configured host specific to your trading partner's remote server. This makes for a faster and easier set up of your installation.

The AS3 standard provides the ability to securely transport EDI (and other data, including binary and XML) to a remote host over FTP, guaranteeing that the message has not been changed in-transit and has been received and can be read only by the intended trading partner. An Message Disposition Notification (MDN) receipt further guarantees that the intended trading partner has received the message.

AS3 uses the FTP protocol as its transport mechanism to send and receive files over the Internet. VersaLex uses the `PUT/GET` action commands to transport the secure data to/from the remote host.

AS3 Configuration

A host describes the remote server of your trading partner to which messages will be sent. The host's parameters specify its location and how it is reached. Your remote trading partner should have provided information to you in the form of a URL, which you will use to configure the host parameters.

This section describes how to configure a generic AS3 pre-configured host.

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.
4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See AS3 Host on page 178.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See AS3 Mailbox on page 196.
   c) Click **Apply** to save your work.
6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See AS3 Action on page 201.
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the product to prompt to you click **Apply** if you try to leave the page. However, in the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

AS3 Host

The following sections describe how to configure any of the generic AS3 hosts. A host describes the remote server of your trading partner to which messages will be sent. The host's parameters specify its location and how it is reached.

AS3 Host: General Tab

The host **General** tab for an AS3 Host contains the fields described in detail below. The default values of these fields vary per generic or pre-configured host. For pre-configured hosts, the fields on the **General** tab typically remain unchanged unless you need to either connect through a forward proxy or change the Default Directories.

Server Address

Either a fully qualified name (recommended) or an IP address.

This is the address of your trading partner's server that will receive your messages.

Port

The port on the server where your trading partner will receive your messages.

Default value: `80` for HTTP and `443` for HTTPs (SSL)

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` - Use either a direct connection to the internet or a VPN.

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For Cleo VLTrader and Cleo Harmony, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Note: If the host is has an external association, the default directories might be managed outside of Cleo Harmony and not shown here.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

AS3 Host: AS3 Tab

Use the **AS3** tab to specify values for AS3-specific parameters.

Overwrite duplicate file names

Disabled for AS3.

Use default file name

Disabled for AS3.

Add Content-Type Directory to Inbox

Allows you to sort incoming messages based on content-type to a subdirectory under the Inbox specified on the **General** tab. Specify each of the Content-Types you want to direct to specific subdirectories by entering a name in the **Directory** field. You can specify directories for Content-Types of: EDIFACT, X12, XML, Binary, Plain Text, EDI Consent and Other (a default for messages with all other Content-Types you might receive). You can specify the same subdirectory for multiple Content-Types. You can also leave Directory entries blank, which causes any received messages of that Content-Type to be stored in the Inbox specified on the **General** tab.

For IBM i / iSeries (AS/400) usage, see AS/400 Setup and installation on page 703 or AS/400 Network Access Setup on page 980 for information on configuring the Content-Type Inbox settings to access the Native File System (NFS).

Note: If you use this feature, incoming messages are placed in the specified folder based on the content type specified in the HTTP header of the message. Cleo Harmony does not check the actual content of the message to determine its content type.

AS3 Host: FTP Tab

Security Modes

If the AS3/FTP server requires use of the Secure Socket Layer (SSL), select a security mode.

Possible values:

- `None` - Indicates non-secure transfers; commands and data are clear-text.
- `SSL Implicit` - For servers that support only SSL connections.
- `SSL Explicit` - For servers that support SSL through the use of either the `AUTH SSL` or `AUTH TLS` command.

Default value: `SSL Explicit`

Default Data Type

The data type used when transferring files to and from the FTP server. The only valid **Data Type** for AS3 commands is **Binary**.

Data Channel Mode

The default behavior for opening data port connections between the AS3 client and AS3/FTP server.

Active mode

Client listens for an inbound connection from the server during data transfers. The **Low Port** / **High Port**, if left at 0/0, will be a random number between 1024-65535; otherwise specify a specific range. Because this is active mode, this port range must be open inbound on your firewall.

Passive mode

Server listens for an outbound connection from the client during data transfers. The server indicates the IP address and port number. The AS3/FTP server will cycle through port numbers, usually a subset of `1024-65535`. **Substitute Passive IP Address** indicates that VersaLex should ignore the IP address specified by the server and reuse the command port address instead. This might be necessary if the server is advertising an internal rather than an external IP address.

AS3 Host: Advanced Tab

The host's **Advanced** tab contains several property settings fields. These settings typically do not affect the ability to connect to a host. However, you might want to change some of these settings when configuring a runtime environment.

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for AS3 include:

Abort In Process Transfers

Indicates that the FTP server supports the `ABORT` command when a data transfer is interrupted.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Allow Duplicate Incoming Message IDs

Ignores messages with duplicate message IDs and allows reprocessing of the message.

Possible values: `On` or `Off`

Default value: `Off`

Avoid List Command When Space In Path

When using the retrieving nested subdirectories (`GET -REC` option) and any of the nested subdirectories have spaces, indicates that the FTP server does not properly handle spaces in the `LIST` command path and that CDs should be used to avoid the issue.

Possible values: `On` or `Off`

Default value: `Off`

Base64 Encode Content

Base64 is the encoding format used by Multi-purpose Internet Mail Extension (MIME) for transmitting non-text material over text-only communications channels. Base64 is based on a 64-character subset of US-ASCII, enabling 6 bits to be represented per printable character.

Possible values: `On` or `Off`

Default value: `Off`

Canonicalize Inbound Signed Content

When this option is selected, a canonicalizer is used to ensure that '\r' and '\n' characters always occur together as '\r\n'. This option may be used when the inbound signature hash verification fails and the trading partner is using OpenSSL to sign its messages.

Possible values: `On` or `Off`

Default value: `Off`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0 - n`

Default value: `0`

Compression- Signing Order

When both signing and compression are enabled, indicates which is applied first.

Possible values: `Sign then compress` or `Compress then sign`

Default value: `Sign then compress`

Connection Keep Alive Timeout (seconds)

Allows the connection to the server to remain open while the message is being processed by sending `NOOP` commands every *n* seconds. This setting may be lowered if the connection to the server is being closed before the message can be fully processed.

Possible values: `1` - `n`

`0` or a negative value disables attempts to keep the connection open.

Default value: `60`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Data Socket Accept Timeout

The amount of time allowed for each read operation on the data port.

Possible values: `0` - `600` seconds, where `0` indicates no timeout.

Default value: `150` seconds

Delete Zero Length Files

Indicates whether files received that are zero-length (<= 5 bytes) should be deleted rather than processed.

Possible values: `On` or `Off`

Default value: `Off`

Disable Address Resolution

Indicates to connect directly to an IP address if the IP address is known and a DNS lookup is not desired.

Possible values: `On` or `Off`

Default value: `Off`

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Explicit SSL Command

Indicates the AUTH command to be used when the Security Mode specified on the Host/FTP tab is "SSL Explicit".

Possible values:

- `AUTH SSL`
- `AUTH TLS`
- `AUTH TLS-C`
- `AUTH TLS-P`

Default value: Depends on the requirements of the trading partner's FTP server.

Explicit SSL Post Command

A command or set of commands to be issued after the Explicit SSL Command and login sequence. The `PBSZ` and `PROT` commands ("PBSZ 0;PROT P") are required by some servers regardless of the AUTH type used and are necessary for data channel protection (AUTH TLS or AUTH TLS-C).

If multiple FTP commands are needed after the AUTH command, set this property to **all** of the commands separated by semicolons (;).

Note: For legacy reasons, this property applies to all connections whether secure or not, with the configured commands executing right after login.

File List Parse Method

The NLST commands on some FTP servers do not return a standard file list.

Possible values: `Tradanet` or `GXS NBT`

Default value: None

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0` - `n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Get Number of Files Limit

Limits the number of files retrieved from a server directory listing by one `GET` command.

Possible values: `0` - `n`

`0` indicates no limit.

Default value: `0`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Ignore Exception After Quit

Indicates to ignore any I/O errors that occur when attempting to read the SMTP server response after issuing a `QUIT` command.

Possible values: `On` or `Off`

Default value: `Off`

Ignore Retrieve Error Code

Indicates an FTP server response code (after an FTP `RETR` request) that should not be treated as an error condition. This property is useful when the absence of a file on the server is not considered an error.

CAUTION: If the server uses the same error code for multiple reasons, this property can potentially mask unknown error conditions.

Possible values: Three-digit error code value.

You can specify multiple error codes separated by commas (,) or semicolons (;). Alternatively, you can use a regular expression (denoted by enclosing it in square brackets '[]') instead of a three-digit error code. For example, `[550.*No such file.*]` would ignore `550` errors containing 'No Such File'. If it is necessary to include a ',' or ';' in the regular expression, the character would need to be escaped (`\x2C` or `\x3B`) instead of using a comma or semicolon. See Using wildcards and regular expressions on page 69 for additional information.

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

Include Filename In Store Unique Command

Indicates whether the FTP server expects a starting filename to be included when using the store unique option (`PUT -UNI`).

Possible values: `On` or `Off`

Default value: `Off`

Interim Retrieve

Indicates to set result of any successfully retrieved file to `Interim Success` rather than `Success`. This would normally be used when transfer logging is being monitored by a backend system to allow coordination of any post processing of the received file that needs to occur prior to setting the transfer status to `Success`.

Possible values: `On` or `Off`

Default value: `Off`

Issue Command After Opening Data Connection

Indicates to issue the retrieve, store, or list command until after the data port connection has been established rather than before.

Possible values: `On` or `Off`

Default value: `Off`

Keepalive Noop Command (seconds)

Indicates the amount of time in-between issuing `NOOP` commands on the command port while a transfer is active on the data port. 0 indicates to not issue `NOOP`s.

Possible values: `0 - n`

Default value: 0

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Next File On Fail

When a download fails, indicates whether a wildcarded `GET` should proceed to the next available file rather than terminate if the server is still connected.

Possible values: `On` or `Off`

Default value: `Off`

Only Retrieve First Available File

Indicates a `GET *` should only retrieve the first available file from the server.

Possible values: `On` or `Off`

Default value: `Off`

Only Retrieve Last Available File

Indicates a `GET *` should only retrieve the last available file from the server.

Possible values: `On` or `Off`

Default value: `Off`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

Password Automatic Update (days)

If greater than zero and `Password Update Format` has been set, the number of days after which the software will generate and apply a new FTP password.

Possible values:`0-n days`

Default value: `0 days`

Password Update Format

If supported by the server, the format of the `PASS` command value when changing a user's password. The server dictates the format.

Use `%old%` and `%new%` keywords to specify the format, for example, `%old%/%new%`.

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512
```

Default value: `System Default`

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: `On` or `Off`

Default value: `On`

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: On or Off

Default value: On

PGP V3 Signature

Post Get Command

Post Put Command

In an action, specify commands to be executed only after a successful GET or PUT as post-get or post-put commands, respectively. When using this property, use a SET command within the action **before the GET or PUT command** rather than the **Advanced** tab.

The Post Put Command can be set to QUIT, which allows a disconnect and reconnect between file uploads when necessary.

If multiple FTP commands are needed after the GET or PUT, set this property to **all** of the commands separated by semicolons (;). If a specific FTP command needs to contain a semicolon, enclose that specific FTP command in quotes ("). Use of macro variables is supported. Refer to Using macro variables on page 59 (Post/Pre Command context) for a list of the applicable macros.

Pre Get Command

Pre Put Command

In an action, specify commands to be executed before a GET or PUT as pre-get or pre-put commands, respectively. This has the benefit of keeping the log results relative to just GETs and PUTs (especially important for Cleo VLTrader and Cleo Harmony GET transfer logging). In addition, for the PUT, it avoids connecting and logging into the server when there are no files to send. When using this property, use a SET command within the action **before the GET or PUT command** rather than the **Advanced** tab.

If multiple FTP commands are needed prior to the GET or PUT, set this property to **all** of the commands separated by semicolons (;). If a specific FTP command needs to contain a semicolon, enclose that specific FTP command in quotes ("). Use of macro variables is supported. See Using macro variables on page 59 (Post/Pre Command context) for a list of the applicable macros.

Pre Put Change Directory

For PUT commands whose destination contains a directory path, forces an explicit CWD request to the destination directory path prior to issuing the STORE request.

Some FTP servers treat directories as logical rather than physical directories, and require directories be set only through a CWD request.

Possible values: On or Off

Default value: Off

Pre Put Command For First File Only

If a Pre Put Command is specified, indicates whether to execute them before each file being transferred by the PUT or only before the first file transfer.

Possible values: On or Off

Default value: On

Resume Failed Transfers

When selected and a transfer fails (and Command Retries > 0), attempt to resume the transfer on a retry. If OpenPGP is enabled on the packaging tab (see Configuring mailbox packaging on page 79), the entire file is transferred instead of resuming with a partial file. The server must support the FEAT, SIZE, and REST STREAM extensions to FTP. For more information, visit http://tools.ietf.org/html/rfc3659.

Possible values: On or Off

Default value: Off

Retain Temporary Inbound Message Files

Leaves any files that are used while processing inbound messages in the `temp\` folder. The default action is to delete these files after processing has completed. These files may be helpful for problem diagnosis.

Note: These temporary files are retained for seven days.

Possible values: `On` or `Off`

Default value: `Off`

Retrieve Directory Sort

Used to control the order in which files are downloaded from the FTP server. Using this property does cause the LIST command rather than the NLST command to be used when VersaLex is determining the available file list – which might be a problem if the server responds with different lists (e.g. NLST only lists files not previously downloaded while LIST lists all files regardless). Windows and Unix/Linux FTP servers are supported.

Possible values:

```
Alphabetical (ascending)
Alphabetical (descending)
Date/Time Modified (ascending)
Date/Time Modified (descending)
Size (ascending)
Size (descending)
```

Retrieve Last Failed File First

If a file download previously failed and you are attempting to `GET` a list of files again, this property indicates whether the previously failed file should be attempted first.

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

Reuse SSL Session

Indicates the command port SSL session should be reused when possible for any subsequent data port SSL connections. This setting does not affect the reuse of command port SSL sessions.

Possible values: `On` or `Off`

Default value: `Off`

Reuse SSL Sessions Across Actions

If selected, and if no forward proxy is being used for this host, SSL sessions from previous connections to the same destination (address and port number) may be resumed to avoid costly negotiation. If unselected, only SSL sessions used in the current action to the same destination may be resumed. When unselected, a new SSL session is created for the initial command port connection.

Possible values: `On` or `Off`

Default value: `On`

RSA-OAEP Key Algorithm Parameter

Represents the type of mask generation and hash generation functions that are applied when the `RSAES-OAEP` key algorithm is in use. See RFC4055 for a further description of the mask and hash generation functions.

Possible values: `MGF1-SHA1`, `MGF1-SHA256`, `MGF1-SHA512`

Default value: `MGF1-SHA1`

SSL Allow Legacy Renegotiation

When selected, legacy renegotiation is allowed. If this property is not selected, the extension described in RFC5746 is used for renegotiation and the server must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Possible values: `On` or `Off`

Default value: `On`

SSL Cipher

Indicates a specific cipher, or an ordered list of ciphers, to be used with the server for SSL key exchange, encryption, and hashing.

If not set (that is, left blank), the list of default ciphers (all standard ciphers, excluding anonymous and non-encrypting) is presented to the server and the server picks one. If a regular expression (enclosed in brackets) or a wildcard expression is specified, a list of implemented ciphers (all standard ciphers, including anonymous and non-encrypting) is presented to the server, based on the conditions of the pattern. For example, if a regular expression of `[.*ECDH.*]` is specified, then the list is a subset of all implemented ciphers that belong to the Elliptical-curve Diffie-Hellman group (for example, `ECDH` is in included in their string). In all cases, whenever a list is presented, it is always ordered by cryptographic strength, with the strongest listed first.

Based on the expression you type, the **List** button shows the resulting set of ciphers in the **SSL Cipher List** dialog box. Within this dialog box, you can view the list or select a specific cipher. If you select a cipher, then its value is displayed in this field.

Possible values:

Blank
a specific cipher picked from the SSL Cipher List dialog box
a regular/wildcard expression

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed. By default, this field is blank, designating that Cleo Harmony, Cleo VLTrader, or Cleo LexiCom will select the most recent version (currently TLS 1.3).

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed when selecting an SSL cipher. To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128`, or `256` (depending on the requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed. SSL 3.0 is the default value for compatibility with servers that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

Default value: `SSL 3.0`

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Store Raw Sent Message

When this property is enabled, a copy of the outbound message is stored in the OFTP/sent directory.

Possible values: `On` or `Off`

Default value: `Off`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Use Content Type For File Extension

By default, inbound messages that do not specifically contain the name of the target file to be saved are stored using the value of the `Message-ID` (of that message) with the `.file` extension. When this option is selected,

inbound messages without a target file name specifier is stored using the `Message-ID` and the appropriate file extension based on the Content-Type of the message.

Possible values: `On` or `Off`

Default value:

`Off` for existing hosts
`On` for newly cloned hosts

Use EPRT and EPSV

Indicates to use Extended Port (EPRT) and Extended Passive (EPSV) commands for IPv6-style network addressing. EPRT/EPSV is used regardless of this setting if the host address is or resolves to an IPv6-style address.

Possible values: `On` or `Off`

Default value: `Off`

Use External IP Address in PORT request

Indicates for active (aka port) mode that the external rather than the local IP address should be included in data port requests to the FTP server.

Possible values: `On` or `Off`

Default value: `Off`

Use Folded Headers For Outbound Messages

Enables or disables automatic line wrapping of HTTP headers exceeding 76 characters. By default headers are not folded since some non-Cleo product remote hosts using Microsoft Internet Information Server (IIS) cannot handle folded headers properly. Unless your host has been pre-configured to enable folded headers, leave this setting cleared!

Possible values: `On` or `Off`

Default value: `Off`

Use NLST

During a `GET *` command, indicates that VersaLex should use an `NLST` command rather than `LIST` when getting the list of files available for download.

Possible values: `On` or `Off`

Default value: `On`

Use SMIME Over FTP Headers

Allows message compatibility with non-standard (pre-AS3) servers. When set, the AS3-To and AS3-From headers specified for that trading partner are translated to To and From headers before the message is sent.

Possible values: `On` or `Off`

Default value: `Off`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
AES-128
AES-192
AES-256
```

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

AS3 Mailbox

Mailbox parameters allow you access to the remote host and define the security of files being sent.

You can use the AS3 mailbox wizard to configure your system for the most common setup. See Using the wizard to create a host or mailbox on page 79.

AS3 Mailbox: AS3 Tab

Select encryption and signing for sending messages and optional security for receiving messages. If an MDN receipt is required, you can also select the format and delivery method of that receipt.

Request

Specify the S/MIME format for messages to send to the remote host.

- Unsigned / unencrypted (neither **Encrypted** nor **Signed** selected)
- Signed (only **Signed** selected)
- Encrypted (only **Encrypted** selected)
- Signed / Encrypted (both **Signed** and **Encrypted** selected)

Receipt

Enables the **MDN Receipt** section. See MDN Receipt on page .

Encryption Algorithm

When **Encrypted** is selected, the **Encryption Algorithm** field is enabled and allows you to choose the encryption algorithm for the message to be sent to the remote host. The remote host must be able to decrypt the message using the algorithm you choose. For a non-Cleo Harmony trading partner, it is important to verify that your trading partner can use the selected algorithm prior to sending an encrypted message. The default encryption method is `TripleDES`. See Cryptographic Services on page 975 for more information on choosing an encryption algorithm.

Key Algorithm

When **Encrypted** is selected, the **Key Algorithm** field is enabled and allows you to choose the algorithm to encrypt the content encryption key with the public key of your trading partner's encryption certificate. Your trading partner uses the private key of their encryption certificate to decrypt the content encryption key that is subsequently used to decrypt the content of the message.

Possible values:

- `RSA` (default)
- `RSAES-OEAP`

Signature Algorithm

When **Signed** is selected, the **Signature Algorithm** is used to encrypt the hash value of the signature with the private key of your signing certificate. Your trading partner uses the public key of your signing certificate to decrypt the hash value of the signature that authenticates you as the sender of the message. When **RSA** is selected, the selected **Hash/MIC Algorithm** is used to determine the appropriate signature algorithm; for example, `rsaEncryption`, `sha256WithRSAEncryption`, `sha384WithRSAEncryption` or `sha512WithRSAEncryption`. If **RSASSA-PSS** is selected, the combination of the private key of your signing certificate and the hash algorithm is used in conjunction with the RSASSA-PSS algorithm to secure the signature.

Possible values:

- `RSA` (default)
- `RSASSA-PSS`

Hash/MIC Algorithm

When **Signed** in the **Request** section is selected, the combination of the signature algorithm and the selected hash algorithm is used to secure the signature.

Note: If the RSASSA-PSS signature algorithm is used and the SHA-512 hash algorithm is selected, the strength of the signature algorithm of your signing certificate must be SHA256withRSA or better.

When the **Signed** option in the **MDN Receipt** section is selected, the selected **Hash/MIC Algorithm** is used to compute the independent Message Integrity Check (MIC) that is returned in the MDN Receipt.

Possible values:

- `SHA-1` (default)
- `MD5` (cryptographically weak and should not be used unless no other Hash/MIC algorithm is available)
- `SHA-256`
- `SHA-384`
- `SHA-512`

Compress Content

When **Compress** is selected, the message will be compressed using ZLIB compression. Compression is generally used for large files so that the message will conserve bandwidth and be transferred more efficiently and securely over the Internet.

Inbound Message Security

Indicates how inbound messages should be received.

Select any combination of **Force Encryption**, **Force Signature** and **Force MDN Signature** to check the level of the inbound message security. If the message is not received according to the corresponding message security settings, the message is rejected and an error is logged.

By default, no settings are selected. If no settings are selected, the security level of the message is not checked.

MDN Receipt

Attributes of the Message Disposition Notification (MDN) receipt you requested.

Message Disposition Notifications can only be returned Asynchronously in AS3 as part of a new FTP `PUT` or `GET` command.

Signed

Compute and remember an independent hash over the content of the sent message using the **Hash/MIC Algorithm** you select. The trading partner returns the MDN with a digital signature; and computes an independent MIC value over the content of the message it received (using the same MIC algorithm) and returns this value as a base64-encoded value in the human-readable portion of the MDN. When the MDN is received, the original MIC is compared against the received MIC. When the MIC values match, the sender is guaranteed that the message read by the trading partner is identical to the message that came from the sender and was not modified in any way.

Forward MDN to Email

Forward a copy of the MDN received to the email address specified in the **Email Address** field.

Synchronous

Disabled for AS3.

Asynchronously

The only option available for AS3.

Return the MDN as part of a new FTP session, that is, only the FTP status message is returned during the acknowledgment phase of the message response and the MDN is returned later in a separate FTP `PUT` or `GET` command.

AS3 Mailbox: Certificates Tab

Associate a trading partner's signing and encryption certificates with this AS3 mailbox and override the signing and encryption certificates defined in the Local Listener, if necessary.

You must acquire your trading partner's signing and encryption certificates and provide yours to your trading partner. See Acquiring your trading partner's signing and encryption certificates on page 86 and Creating and providing your signing/encryption certificates on page 86.

Trading Partner's Certificates

Encryption Certificate

The name of the file containing your Trading Partner's encryption certificate. Specify a value or click **Browse** to navigate to the file you want to select.

Signing Certificate

Select the check box to enable the field.

The name of the file containing your Trading Partner's signing certificate. Specify a value or click **Browse** to navigate to the file you want to select.

If you do not specify a signing certificate, the Cleo Harmony application uses all the certificates in its certificate store to determine if the signature of the incoming data message is trusted.

Use encryption certificate

Indicates that your trading partner uses the same certificate for signing and encryption, which is the general practice among most trading partners. When you select this check box, the **Signing Certificate** field is populated with the same certificate you selected in the **Encryption Certificate** field.

If the remote host is capable of receiving Certificate Exchange Messages (CEM) or you want to email your certificates to your trading partner, you can send your user and SSL certificates to the remote host by clicking **Exchange Certificates**.

My Certificates

Override Local Listener Certificates

Enables fields where you specify signing and encryption certificates to use with this particular partner instead of the certificates you configured for the Local Listener. See Configuring certificates for Local Listener on page 758.

If you override the default certificates, you must also exchange the certificates you specify here with your partner.

Exchange Certificates

Displays the Certificate Exchange dialog box, which allows you to send your user and SSL certificates to your trading partner. See Exchanging certificates with your trading partner on page 672.

Signing Certificate Alias

The name of the signing certificate registered with the Cleo Harmony application through the Certificate Manager. The certificate must be the same as the one exchanged with your remote trading partners, unless you want to override it at the Mailbox level. See Local HTTP Users Configuration on page 834.

Click **Browse** to navigate to and select a certificate. Enter the **Password** for your signing certificate's private key.

Encryption Certificate Alias

The certificate for decrypting your trading partner’s messages, if you have created or obtained a separate certificate.

Click **Browse** to navigate to and select a certificate. Enter the **Password** for your encryption certificate.

Use signing certificate

Select this check box to use the same certificate for signing and decrypting your trading partner's messages. The **Encryption Certificate Alias** and **Password** are populated to match the **Signing Certificate Alias** and disabled.

Exchange Certificates

Invokes the **Certificate Exchange** dialog box. If you override the default the certificates, you must exchange these alternate certificates with your trading partner.

Overriding AS3 Local Listener Certificates

By default, the certificates you configured on the **Certificates** tab of the Local Listener panel will be the certificates used to sign messages sent to your trading partner and decrypt messages received from your trading partner. See Configuring certificates for Local Listener on page 758.

Use **Override Local Listener Certificates** to select alternate certificates for signing and decrypting messages with this particular trading partner. If you do override the default the certificates, don't forget to export and exchange these alternate certificates with your trading partner.

AS3 Mailbox: FTP Tab

Login

User Name

Password

FTP Account

Credentials for authentication to the FTP server. Select **No Password Required** if there is no password required for authentication.

FTP Account is optional.

Headers

AS3-From

AS3-To

Enter the **AS3-From** and **AS3-To** names for this trading relationship.

Note: The values in the **AS3-From** and **AS3-To** fields are determined and agreed upon as part of initially setting up the trading relationship. These fields can be company-specific, such as DUNS number, or an agreed-upon identification string. The **AS3-From** / **AS3-To** combination is case-sensitive and must be unique across all hosts defined in your system because it is used to determine in which Inbox messages are stored when received from remote hosts.

Subject

Identifies the message and is returned in the human-readable section of an MDN, if requested.

Content-Type

Optional. The format of the message being sent. Used by the sending and receiving applications to properly assemble and parse the message. Choose from the following:

- EDIFACT
- X12
- XML
- Binary
- Plain Text
- EDI Consent

Note: If **Content-Type** is not specified or if multiple payloads are attached in the message, the **Content-Type** is detected based first on file content and then the file extension. Detectable types include `application/edifact`, `application/edi-x12`, `application/edi-tradacoms`, `application/xml` (text/xml), `application/pdf`, `application/msword`, `application/x-msexcel`, `application/rtf`, `application/zip`, `image/bmp`, `image/gif`, `image/tiff`, `image/jpeg`, `text/plain`, `text/html`, and `video/mpg`.

AS3 Mailbox: Security Tab

If a **Security Mode** is specified in the host's FTP tab, a remote host can issue client certificates. If so, import the client certificate using Certificate management on page 661 and then specify or browse for the imported certificate's alias and password.

AS3 Action

An action's parameters define a repeatable transaction for your mailbox designated for the host system.

AS3 Action: Action Tab

Use the **Action** tab to configure commands within the action. See Composing an action on page 89. See also FTP Command Reference on page 113 for further information.

Verifying Your AS3 Names

When configuring a client to exchange messages with a Cleo VLTrader or Cleo Harmony AS3 server, you can use the following SITE command to verify the client has correctly defined the AS3-To and AS3-From names. The command syntax is:

```
SITE VERIFY AS3-To: 'your-AS3-To-name', AS3-From: 'your-AS3-From-name'
```

If your AS3 names are properly configured, the server returns a positive response. Otherwise, a failure response is returned.

When using a VersaLex client, you can use the `%as3.to%` and `%as3.from%` macros in place of `your-AS3-To-name` and `your-AS3-From-name`, and so on.

```
SITE VERIFY AS3-To: %as3.to%, AS3-From: %as3.from%
```

Note: See Using macro variables on page 59 for further information.

AS3-Specific Directories

The following additional directories are created either during the AS3 installation or as needed by the application:

Directory	Purpose
`lostandfound\`	Default inbox where incoming data is deposited when the application cannot determine where to put it.

Directory	Purpose
AS3\	Location where raw (unprocessed) incoming and outgoing messages are stored. Incoming messages are located in the **AS3\received** directory and outgoing messages are located in the **AS3\sent** directory. These files can be helpful in diagnosing problems. Old files should be deleted or archived by the user, if necessary. The **AS3\unsent** directory contains raw header, data and message setup information files. These files are used if a message needs to be retransmitted, and are deleted automatically by the application once the message transfer has either completed successfully or has failed due to timeouts, exceptions, or the number of retries has been exhausted. The **AS3\mdn** directory contains subdirectories for received (and optionally sent) MDNs. This directory can be changed on the AS3 Service Panel. MDNs can be automatically archived by the application or manually archived by the user from the **MDNs** tab on the listener panel. Archived MDNs are stored in `AS3\mdn\received\archive\mdn.zip` or `AS3\mdn\sent\archive\mdn.zip`. The **AS3\data** directory contains an `AS3msgs.txt` file used by the application to determine the receipt of duplicate messages. Entries in this file are retained for the time interval configured on the AS3 Service panel .
temp\	Temporary location where incoming messages can be stored while being processed by the application. By default, they are deleted automatically once the message has been completely processed; however, these files can be kept for problem diagnosis by using the **Retain Temporary Inbound Message Files** host-level Advanced property. These temporary files will automatically be deleted after 7 days.

AS4 Hosts

AS4 Configuration

This section describes how to configure a generic AS4 host.

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

Note: The original pre-configured host remains in the pre-configured tree.

4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See AS4 Host configuration on page 203.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See AS4 Mailbox configuration on page 218.
   c) Click **Apply** to save your work.
6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See AS4 Action configuration on page 226.
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the product to prompt to you click **Apply** if you try to leave the page. However, in the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

AS4 Host configuration

The following sections describe how to configure the generic AS4 hosts. A host describes your trading partner's remote server to which messages are sent. The host's parameters specify its location and how it is reached.

AS4 Host: General Tab

The host **General** tab for an AS4 Host contains the fields described in detail below. The default values of these fields vary depending on whether the host is generic or pre-configured. For pre-configured hosts, these typically remain unchanged unless you need to either connect through a forward proxy or change the Default Directories.

Server Address

Either a fully qualified name (recommended) or an IP address.

This is the address of your trading partner's server that will receive your messages.

Port

The port on the server where your trading partner will receive your messages.

Note: The **Server Address** and **Port** settings are reflected as read-only through the **PMode.Protocol.Address** setting.

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` - Use either a direct connection to the internet or a VPN.

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For Cleo VLTrader and Cleo Harmony, see URI File System interface overview on page 955 for information about how you can use a Cleo-provided or custom URI for the Inbox and Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Note: If the host is has an external association, the default directories might be managed outside of Cleo Harmony and not shown here.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

AS4 Host: AS4 Tab

Use the **AS4** tab to specify values for AS4-specific parameters.

Overwrite duplicate file names

Allows for unique naming of stored files. When this check box is selected, any files that exist in the specified inbox will be overwritten. When the check box is cleared, an incoming file with the same name as one that already exists is made unique according to the **Unique File Algorithm** as set under **System Options** > **Other**.

Note: This setting does not apply to inbound database payload.

Use default file name

Select the check box and specify the name you want to use for incoming files by default.

You can use any of the supported macros (Destination File context) allowing for the incoming file to be named, for example, with a date-time stamp. For more information about macro variables and the destination file context, see Using macro variables on page 59 and Context Definitions on page 61.

If you select `Use default file name` and your default string includes any variant of the `%sourcefile%` macro, the source file name is determined as follows:

- If the `Content-Disposition` header exists and it contains a "filename" attribute, then this value is used.
- If the `Content-Type` header exists and it contains a "name" attribute, then this value is used.
- If the `Content-Id` header exists, then this value is used.

If you do not select `Use default file name`, then the incoming file name will be determined as follows:

- If the `Content-Disposition` header exists and it contains a "filename" attribute, then this value is used.
- If the `Content-Type` header exists and it contains a "name" attribute, then this value is used.
- If the `Content-Id` header exists, then use this value.
- Otherwise, the incoming message ID, plus the ".file" extension is used.

Note: This setting does not apply to inbound database payload.

Note: When the incoming file is tied to an attachment, the Content-xxx headers are those that directly precede the attachment. When the incoming payload is tied to a body payload, the Content-xxx headers are those at the top level of the HTTP request.

Note: For outbound, to add the setting of the "name" attribute on the `Content-Type` header, you can simply append it, along with an optional macro (Destination File context). For example, `application/octetstream; name=%sourcefile%`

AS4 Host: HTTP Tab

Use the **AS4** tab to specify values for HTTP-specific parameters.

Outbound

Indicates whether you use SSL or not for outbound file transfers.

HTTP

Do not require use SSL

HTTP/s

Require SSL for outbound file transfers.

If you select HTTP/s, you can select **Check certificate server name**.

Inbound

HTTP/s only

Require your trading partner to use Secure Socket Layer (SSL) for inbound file transfers.

Command

Lists the commands available to AS4. `PUT` will initiate a push operation and `GET` will initiate a pull operation.

Method

Specifies the HTTP verb to be used. The only valid **Method** for AS4 commands is `POST`.

Path

The server **Path** for the command.

If the remote server is also using the Cleo Harmony application, the path should be `/as4`. The resource path must be properly specified in order for your trading partner's system to process messages from you. Given the URL provided by your remote trading partner in the form:

`http(s)://remote-host:port/`***`resource-path`***`?optional-parameters`

Enter the bolded portion in this field (if it was supplied).

Parameters

By default, no **Parameters** are specified for sending AS4 messages. If parameters are required, they must be obtained from your trading partner when the trading relationship is established. Given the URL provided by your remote trading partner in the form:

`http(s)://remote-host:port/resource-path?`***`optional-parameters`***

Enter the bolded portion in this field (if it was supplied).

Headers

The **Header** fields are filled in at the Mailbox level and specify values to be set in the HTTP headers that precede the body (actual content) of the message to be sent.

The following **Header** can optionally be specified when sending AS4 messages:

- **Content-Type** - throughout the entire AS4 message, there are several Content-Type settings, many of which are predetermined and cannot be changed. This Content-Type header is used to control the value of the MimeType property, as packaged within `<eb:PartInfo/eb:PartProperties/eb:Property@name>`, along with the `@MimeType` attribute of the `<xenc:EncryptedData>` element when using SOAP with Attachments (SwA) packaging. The **Content-Type** value should represent the native format of the payload before any processing, for example, compression. If the payload format is unknown, a content-type setting of `application/octet-stream` is recommended as it generally represents all types of data. If this optional parameter is not specified, then a default is determined based on whether SOAP with Attachments (SwA) packaging (application/octet-stream) or `<Body>` payload (text/xml) is being used.

AS4 Host: Advanced Tab

While the fields on the host's **Advanced** tab typically do not affect your ability to connect to a host, you might want to change some of these settings when configuring a runtime environment.

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for AS4 include:

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Bundle All Outbox Files For Pull Operations

Indicates whether all files within the outbox should be returned in response to a Pull Request Signal. When `off`, only a single file will be returned within the packaged User Message response. This file will always be the oldest file in the outbox. When `on`, all files in the outbox will be returned within the packaged User Message response.

Possible values: `On` or `Off`

Default value: `Off`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

This value is reflected as read-only through the **PMode.ReceptionAwareness.Retry** and **PMode.ReceiptionAwareness.MaxRetries** settings.

Possible values: `0` - `n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *`n`* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0` - `n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

Perform Schema Validation

When selected, inbound XML content on responses only is processed through XML schema validation.

Possible values: `On` or `Off`

Default value: `On`

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512
```

Default value: `System Default`

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: `On` or `Off`

Default value: `On`

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: `On` or `Off`

Default value: `On`

PGP V3 Signature

Put Multiple Files Limits

Limits the number of files included in each generated multipart message when using the `PUT -MUL` option. The limit is only applied when sending out of a single directory; when sending multipart out of separate subdirectories, the files are kept as a group and not broken up into separate messages.

Possible values: `-1 - n`

`-1` indicates no limit.

Default value: `-1`

Reset Connection After Timeout On Response

When enabled will cause an immediate reset on the socket (instead of a graceful close) when a `SocketTimeoutException` occurs.

Possible values: `On` or `Off`

Default value: `Off`

REST Enabled

Allows the host to be accessible through the REST API. This feature is only supported on **AS2**, **AS4**, **FTP** and **SSH FTP** and *only when the host has exactly one mailbox*.

When this setting is enabled, new mailboxes cannot be created and the existing mailbox cannot be cloned, disabled, or removed.

Possible values: `On` or `Off`

Default value: `On` for **AS2**. **AS4**, **FTP** and **SSH FTP** when the host has exactly one mailbox. `Off` in all other cases.

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

Reuse SSL Sessions Across Actions

If selected, and if no forward proxy is being used for this host, SSL sessions from previous connections to the same destination (address and port number) may be resumed to avoid costly negotiation. If unselected, only SSL sessions used in the current action to the same destination may be resumed. When unselected, a new SSL session is created for the initial command port connection.

Possible values: `On` or `Off`

Default value: `On`

Security Token Reference Type

Controls the type of security token reference that is placed in outgoing User Messages and Receipt Signals. For more information on token references, see the OASIS "Web Services Security X.509 Certificate Token Profile" standard.

Possible values: `Binary Security Token`, `Subject Key Identifier`, or `Issuer and Serial Number`

Default value: `Binary Security Token`

SSL Allow Legacy Renegotiation

When selected, legacy renegotiation is allowed. If this property is not selected, the extension described in RFC5746 is used for renegotiation and the server must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Possible values: `On` or `Off`

Default value: `On`

SSL Cipher

Indicates a specific cipher, or an ordered list of ciphers, to be used with the server for SSL key exchange, encryption, and hashing.

If not set (that is, left blank), the list of default ciphers (all standard ciphers, excluding anonymous and non-encrypting) is presented to the server and the server picks one. If a regular expression (enclosed in brackets) or a wildcard expression is specified, a list of implemented ciphers (all standard ciphers, including anonymous and non-encrypting) is presented to the server, based on the conditions of the pattern. For example, if a regular expression of `[.*ECDH.*]` is specified, then the list is a subset of all implemented ciphers that belong to the Elliptical-curve Diffie-Hellman group (for example, `ECDH` is in included in their string). In all cases, whenever a list is presented, it is always ordered by cryptographic strength, with the strongest listed first.

Based on the expression you type, the **List** button shows the resulting set of ciphers in the **SSL Cipher List** dialog box. Within this dialog box, you can view the list or select a specific cipher. If you select a cipher, then its value is displayed in this field.

Possible values:

Blank
a specific cipher picked from the SSL Cipher List dialog box
a regular/wildcard expression

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed. By default, this field is blank, designating that Cleo Harmony, Cleo VLTrader, or Cleo LexiCom will select the most recent version (currently TLS 1.3).

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed when selecting an SSL cipher. To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128`, or `256` (depending on the requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed. SSL 3.0 is the default value for compatibility with servers that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

Default value: `SSL 3.0`

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Store Raw Ping Message

Indicates whether copies of the "raw" outgoing requests and corresponding incoming responses for PING operations are stored in the `AS4\ping` folder. These files can be useful in diagnosing problems, however, generally this property should be off to conserve disk space.

Possible values: `On` or `Off`

Default value: `Off`

Store Raw Sent Message

Indicates whether copies of the "raw" outgoing requests and corresponding incoming responses are stored in the `AS4\sent+received` folder. These files can be useful in diagnosing problems, however, generally this property should be `off` to conserve disk space.

Possible values: `On` or `Off`

Default value: `Off`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Use MIME Packaging For Signal Messages

Indicates whether or not MIME packaging should be used for signal messages (that is, Receipt Signals, Error Signals, and Pull Request Signals).

Possible values: `On` or `Off`

Default value: `Off`

Use Soap With Attachments Formatting

Indicates whether or not Soap With Attachments (SwA) formatting should be used when packaging outgoing User Messages. For information on SwA formatting, see http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SwAProfile.pdf.

Possible values: `On` or `Off`

Default value: `On`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

`System Default`
`TripleDES`
`AES-128`
`AES-192`
`AES-256`

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`

2
1
0 - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

AS4 Mailbox configuration

Mailbox parameters allow you access to the remote host and define the security of files being sent.

AS4 Mailbox: AS4 Tab

Note: By default, AS4 hosts have the **REST Enabled** advanced property set to `On`, which prevents the host from having more than one mailbox. If you want more than one mailbox for this host, set the **REST Enabled** advanced property to `Off`. See AS4 Host: Advanced Tab on page 206.

The mailbox's **AS4** tab allows you to to configure a Usage Profile, along with all the associated AS4 Processing Mode (P-Mode) settings.

Usage Profile

To assist with the job of configuring all the required P-Mode settings, you can select a profile that provides the default values for many of the P-Mode fields. Profiles that are available:

- AS4 profile
- eDelivery profile
- PEPPOL profile

Profile

Displays the name of the current profile.

The initial setting for this field is `None`. Although it's not required to select a profile, it is recommended.

Set Profile Defaults...

Click this button to display a list of profiles from which you can load processing mode settings.

Note: The settings configured here will override any existing settings already in place.

Ping...

Click this button to run a simple connectivity test by sending a User Message with a single payload to your trading partner. This payload is created dynamically and is wrapped within an XML-formatted file called "`PING.xml`". The PING operation is part of a feature that is provided in compliance with the eDelivery 1.14 "Test Service" feature. Below are some notes to consider related to outbound/inbound PING operations:

- All mailbox PMode settings and all host Advanced property settings are considered for PING operations. These include, for example, signing, encryption, and compression.
- All outbound/inbound PING operations are not logged as a transfer. Therefore, they will not be seen in any transfer reporting features.
- When the **Store Raw Ping Message** advanced property is set, all inbound payloads that are associated with a PING operation are stored under the `AS4/ping` folder.

- Receipts may or may not be exchanged as part of the PING operation, depending upon the active PMode settings. If Receipts are exchanged and the **Store Raw Ping Message** advanced property is set, they are stored under the `AS4/ping/receipts` folder.

Processing Mode (P-Mode) parameters

P-Mode parameters define how User Messages and Signal Messages should be processed. These parameters define either elements that are expected to be found in the messages or expected processing behavior.

This section contains a series of tabs on which you can enter values for various settings related to AS4 Processing Modes. Each tab contains a set of related fields, as defined by the AS4 specifications.

General tab

PMode.ID

An optional identifier for this P-Mode agreement, used primarily for the convenience of P-Mode management.

PMode.Agreement

A reference to the agreement governing all message exchange.

PMode.Agreement.Type

Additional information indicating how the parties will interpret the Agreement value.

PMode.Initiator.Party

Identifies the VersaLex party ID for this relationship.

Outbound User Messages use this value as the `<eb:PartyInfo/eb:From/eb:PartyId>` element value.

For inbound User Messages, the receiving message handler (MSH) takes the values of the `<eb:PartyInfo/eb:To/eb:Party>` and the `<eb:PartyInfo/eb:From/eb:Party>` elements and searches every AS4 mailbox for matches to **PMode.Initiator.Party** and **PMode.Responder.Party** settings, respectively. It does this in order to associate the inbound message with the proper recipient. If a match is not made, the request is not accepted. If more than one mailbox matches, the request is also not accepted. For this reason, the to/from settings must be unique within every AS4 mailbox of the VersaLex instance.

PMode.Initiator.Party.Type

The domain of names to which the string in the content of the `<eb:PartyId>` element belongs. The value of the type attribute must be mutually agreed to and understood by each of the parties.

PMode.Initiator.Role

Identifies the VersaLex role for this relationship. An outbound User Message will use this value as the `<eb:PartyInfo/eb:From/eb:Role>` element value.

PMode.Initiator.Authorization.username

This value defines the VersaLex username for this relationship. If an incoming User Message or Pull Request contains a `UsernameToken`, then this value is used to match to the incoming `<wsse:Username>` value.

PMode.Initiator.Authorization.password

This value defines the VersaLex password for this relationship. If an incoming User Message or Pull Request contains a `UsernameToken`, then this value is used to match to the incoming `<wsse:Password>` value.

PMode.Responder.Party

The trading partner party ID for this relationship.

Outbound User Messages use this value as the <eb:PartyInfo/eb:To/eb:PartyId> element value.

For inbound User Messages, the receiving message handler (MSH) takes the values of the <eb:PartyInfo/eb:To/eb:Party> and the <eb:PartyInfo/eb:From/eb:Party> elements and searches every AS4 mailbox for matches to **PMode.Initiator.Party** and **PMode.Responder.Party** settings, respectively. It does this in order to associate the inbound message with the proper recipient. If a match is not made, the request is not accepted. If more than one mailbox matches, the request is also not accepted. For this reason, the to/from settings must be unique within every AS4 mailbox of the VersaLex instance.

PMode.Responder.Party.Type

The domain of names to which the string in the content of the <eb:PartyId> element belongs. The value of the type attribute must be mutually agreed and understood by each of the parties.

PMode.Responder.Role

The trading partner role for this relationship. Outbound User Messages use this value as the <eb:PartyInfo/eb:To/eb:Role> element value.

PMode.Responder.Authorization.username

This value defines the VersaLex username for this relationship. If an incoming User Message contains a UsernameToken, and this User Message is in response to a Pull Request, then this value is used to match to the incoming <wsse:Username> value. This value may be the same as **PMode.Initiator.Authorization.username**.

PMode.Responder.Authorization.password

This value defines the VersaLex password for this relationship. If an incoming User Message contains a UsernameToken, and this User Message is in response to a Pull Request, then this value is used to match to the incoming <wsse:Password> value. This value may be the same as **PMode.Initiator.Authorization.password**.

PMode.MEP

The type of ebMS message exchange pattern (MEP) associated with this P-Mode.

PMode.MEPbinding

Read-only.

The transport channel binding assigned to the MEP (for example, push, pull).

Protocol tab

PMode.Protocol.Address

Read-only.

The server address and port of the receiving message handler (MSH). You can only change it through the host General configuration.

PMode.Protocol.SOAPVersione

Read-only.

The SOAP version to be used. SOAP 1.2 is supported.

Business Info tab

PMode.BusinessInfo.Service

The name of the service to which the User Message is intended to be delivered.

PMode.BusinessInfo.Service.Type

Additional information indicating how the parties will interpret the Service value.

PMode.BusinessInfo.Action

The name of the action the User Message is intended to invoke.

PMode.BusinessInfo.Properties[]

A table that contains a list of key-value pairs added to the User Message within the `<eb:MessageProperties>` element.

Note: For the eDelivery and PEPPOL profiles, these two properties are required:

- **originalSender**
- **finalRecipient**

PMode.BusinessInfo.MPC

When using a Message Partition Channel (MPC) in conjunction with Pull Requests, this value provides this connection's unique MPC identification. This value maps to the `@mpc` attribute of the `<eb:PullRequest>` element. If left blank, the default MPC is used.

Error Handling tab

PMode.ErrorHandling.Report.AsResponse

Indicates whether an error generated on reception of a User Message must be returned as a synchronous response over the same SOAP message exchanged pattern (MEP).

PMode.ErrorHandling.Report.ProcessErrorNotifyConsumer

Read-only.

Indicates whether the Consumer of User Message should be notified when an error occurs in the receiving message handler (MSH), during processing of the received User Message. By default and relative to how Cleo Harmony operates, this setting is always true as processing errors are always logged.

PMode.ErrorHandling.Report.ProcessErrorNotifyProducer

Read-only.

Indicates whether the Producer of a User Message should be notified when an error occurs in the sending message handler (MSH), during processing of the User Message to be sent. By default and relative to how Cleo Harmony operates, this setting is always true as processing errors are always logged.

PMode.ErrorHandling.Report.DeliveryFailuresNotifyProducer

Read-only.

Indicates whether the Producer of a User Message must be notified when the delivery to Consumer fails. By default and relative to how Cleo Harmony operates, this setting is always true as transmission errors are always logged.

PMode.ErrorHandling.Report.MissingReceiptNotifyProducer

Read-only.

Indicates whether the Producer of a User Message must be notified when the required receipt is not received. By default and relative to how Cleo Harmony operates, this setting is always true as transmission errors are always logged.

Security tab

PMode.Security.WSSVersion

Read-only.

The version of WS-Security you want to use. WSS 1.1.1 is supported.

PMode.Security.X509.Sign

Indicates whether User Messages and Pull Requests should be signed by a sending message handler (MSH). Also indicates whether Receipt Signals should be signed by a receiving MSH..

Select this check box to enable the other fields in this section of the tab.

Note: All of the security signing properties apply to both the sending MSH (for example, sending a User Message) and the receiving MSH (for example, returning a Receipt Signal) where applicable.

PMode.Security.X509.Sign.Element.Body

Indicates whether the <eb:Body> element should be included in the signature.

PMode.Security.X509.Sign.Element.Messaging

Indicates whether the <eb:Messaging> element should be included in the signature.

PMode.Security.X509.Sign.Attachment

Indicates whether attachments should be included in the signature.

PMode.Security.X509.Signature.Certificate

Read-only on this screen. It can be changed only through the host Certificates configuration.

The filename of the trading partner's certificate (stored in the certs/ folder). The public key of this certificate is used for validation of incoming signatures.

Note: If a signing certificate is not provided, then incoming content that is signed must contain a <wsse:BinarySecurityToken> element, which provides the certificate. It is this certificate's public key that is then used for signature validation.

PMode.Security.X509.Signature.HashFunction

The hash function to be used for signing.

PMode.Security.X509.Signature.Algorithm

The algorithm to be used for signing.

PMode.Security.X509.Encryption.Encrypt

Indicates whether User Messages should be encyrpted.

Per the eDelivery and PEPPOL specifications and, by reference, per the AS4 Profile specification, encryption takes place only on payloads (either body payload or attachment payload). No component of the <eb:Messaging> element is encrypted. If security is required for this element, transport level security should be used.

Select this check box to enable other fields in this section of the tab.

PMode.Security.X509.Encryption.Certificate

Read-only on this screen. It can be changed only through the host Certificates configuration.

The filename of the trading partner's certificate (stored in the certs/ folder). This certificate's public key is used to encrypt outgoing messages.

PMode.Security.X509.Encryption.Algorithm

The algorithm to be used for data encryption.

PMode.Security.X509.Encryption.KeyTransportAlgorithm

The algorithm to be used for key encryption.

PMode.Security.X509.Encryption.KeyTransportAlgorithm.Parameter

Represents both the mask generation and digest generation functions. This setting only applies when the RSA-OAEP key transport algorithm has been selected.

PMode.Security.SendReceipt

Indicates whether a Receipt signal should be used to acknowledge successful receipt of a User Message. This applies to User Messages received asynchronously or User Messages received synchronously in response to a Pull Request Signal.

Note: Regarding signing of receipts, the Cleo Harmony AS4 server will always sign receipts if **PMode.Security.X509.Sign** is set to `true`.

Select this check box to enable the other fields in this section of the tab.

PMode.Security.SendReceipt.ReplyPattern

The mode in which a Receipt Signal should be sent.

- `Callback` indicates the receipt should be sent asynchronously.
- `Response` indicates the receipt should be sent synchronously.

Note: When sending a receipt to acknowledge receipt of a User Message sent in response to a Pull Request Signal, this transmission will always be sent asynchronously.

PMode.Security.SendReceipt.NonRepudiation

Indicates whether a Receipt Signal should contain an `<ebbp:NonRepudiationInformation>` (NRI) element. The NRI element can only be included if the original User Message is signed, as it contains references to the User Message digests. If the original User Message is unsigned, then the complete `<eb:UserMessage>` element from the inbound request is included instead, regardless of this setting.

PMode.Security.PModeAuthorize

This setting indicates whether outbound Pull Requests and initiating User Messages (not User Messages sent in response to a Pull Request) should contain a `<wsse:UsernameToken>`.

Select this check box to enable the other fields in this section of the tab.

PMode.Security.UsernameToken.username

For outbound processing of Pull Requests and initiating User Messages, if PModeAuthorize is 'true', this value defines the trading partner username that should go into the <wsse:Username> element of the `<wsse:UsernameToken>`.

PMode.Security.UsernameToken.password

For outbound processing of Pull Requests and initiating User Messages, if PModeAuthorize is 'true', this value defines the trading partner password that should go into the `<wsse:Password>` element of the `<wsse:UsernameToken>`.

PMode.Security.UsernameToken.Digest

This setting indicates whether the `<wsse:Password>` value should be a base64-encoded, SHA-1 hash value of the password.

PMode.Security.UsernameToken.Nonce

This setting indicates whether a nonce value should be included in the `<wsse:UsernameToken>` element.

PMode.Security.UsernameToken.Created

This setting indicates whether a created timestamp should be included in the `<wsse:UsernameToken>` element.

Payload Sercice tab

PMode.PayloadService.CompressionType

Indicates whether User Messages should be compressed (`application/gzip`) or uncompressed (`<None>`).

Reception Awareness tab

PMode.ReceptionAwareness

Indicates whether the sending message handler (MSH) expecting a receipt (related to a sent message) should generate an error if no receipt is received.

Select this check box to enable the rest of the fields on the tab.

PMode.ReceptionAwareness.Retry

Read-only. It can be changed only through the host Advanced properties (Command Retries > 0).

Indicates whether the sending message handler (MSH) should retry to send a User Message if a receipt is not received, either synchronously or asynchronously.

PMode.ReceptionAwareness.Retry.MaxRetries

Read-only. It can be changed only through the host Advanced properties (Command Retries).

Indicates how many times the sending message handler (MSH) should retry to send a User Message if a receipt is not received, either synchronously or asynchronously.

Note: This setting only applies to User Messages sent as part of a PUSH operation, not those sent in response to a PULL operation.

PMode.ReceptionAwareness.Retry.Period

Read-only. It can be changed only through the host Advanced properties (Retry Delay).

Indicates the amount of time (in seconds) the sending message handler (MSH) should wait between retry attempts. This setting governs the policy for both synchronous (response) or asynchronous (callback) responses.

PMode.ReceptionAwareness.DuplicateDetection

Indicates whether the receiving message handler (MSH) should track received message IDs (`<eb:MessageInfo>/<eb:MessageId>`) in order to prevent duplicates from being available to the Consumer.

This means, in addition to *detecting* duplicates, the receiving MSH *eliminates* duplicates by blocking them from being received. An appropriate Error Signal is provided to the sending MSH when this occurs.

PMode.ReceptionAwareness.DuplicateDetection.MaxWindow

Indicates the number of days the receiving message handler (MSH) should store message IDs for the purpose of duplicate detection.

AS4 Mailbox: Certificates Tab

Use this tab to associate a trading partner's signing and encryption certificates with this mailbox and to override your own Local Listener's signing and encryption certificates, if necessary.

Acquire your trading partner's signing/encryption certificates and provide your trading partner with your signing/encryption certificates. See Acquiring your trading partner's signing and encryption certificates on page 86 and Creating and providing your signing/encryption certificates on page 86.

Trading Partner's Certificates

Encryption Certificate

The name of the file containing your Trading Partner's encryption certificate. The public key of this certificate is used to encrypt payloads of outgoing User Messages.

Specify a value or click **Browse** to navigate to the file you want to select.

Note: This value is reflected as read-only through the **PMode.Security.X509.Encryption.Certificate** setting.

Signing Certificate

Select the check box to enable the field.

The name of the file containing your Trading Partner's signing certificate. The public key of this certificate is used to validate incoming signatures.

Specify a value or click **Browse** to navigate to the file you want to select.

Note: If a signing certificate is not provided, then incoming content that is signed must contain a `<wsse:BinarySecurityToken>` element, which provides the certificate. It is this certificate's public key that is then used for signature validation.

Note: This value is reflected as read-only through the **PMode.Security.X509.Signature.Certificate** setting.

Use encryption certificate

Indicates that your trading partner uses the same certificate for signing and encryption, which is a common practice among trading partners. When you select this check box, the **Signing Certificate** field is populated with the same certificate you selected in the **Encryption Certificate** field.

My Certificates

Override Local Listener Certificates

Enables fields where you specify signing and encryption certificates to use with this particular partner instead of the certificates you configured for the Local Listener. See Configuring certificates for Local Listener on page 758.

If you override the default certificates, you must also exchange the certificates you specify here with your partner.

Signing Certificate Alias

The name of the signing certificate registered with the Cleo Harmony application through the Certificate Manager. This certificate is used to sign selected components (as configured through the `PMode.Security.X509.Sign` settings) of outbound User Messages and Receipt Signals.

Click **Browse** to view and select a certificate. Enter the **Password** for your signing certificate's private key.

Encryption Certificate Alias

The name of the encryption certificate registered with the Cleo Harmony application through the Certificate Manager. This certificate is used to decrypt inbound User Messages.

Click **Browse** to view and select a certificate. Enter the **Password** for your encryption certificate.

Use signing certificate

Select this check box to use the same certificate for signing and decrypting your trading partner's messages. The **Encryption Certificate Alias** and **Password** are populated to match the **Signing Certificate Alias** and disabled.

Exchange Certificates

Invokes the **Certificate Exchange** dialog box. If you override the default the certificates, you must exchange these alternate certificates with your trading partner.

AS4 Mailbox: HTTP Tab

The mailbox's **HTTP** tab allows you to configure a **Content-Type** setting that can be used to control several values within the packaging.

It is recommended that you set this type according to the native payload type, before any processing, for example, compression. If the payload type is unknown, a content-type setting of `application/octet-stream` is recommended as it generally represents all types of data. If this optional parameter is not specified, then a default is determined based on whether SOAP with Attachments (SwA) packaging (`application/octet-stream`) or `<Body>` payload (`text/xml`) is being used.

To control the setting of the `CharacterSet` property within the `<eb:PartProperties>`, you can append a `charset` parameter after the `content-type` value. For example, `application/octet-`

`stream;charset=UTF-16`. In this case, `CharacterSet` will be set to `UTF-16`. If you do not add this optional parameter, `CharacterSet` defaults to `UTF-8`.

AS4 Mailbox: Security Tab

The **HTTP** and **HTTP/s** radio buttons are read-only. They reflect the settings from the host HTTP tab.

If **HTTP** is selected, no further action is necessary on this tab.

If **HTTP/s** is selected, the target server can issue client certificates. In this case, import the client certificate using Certificate Manager (See Certificate management on page 661) and then specify (or browse for) the imported Certificate Alias and Password.

AS4 Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information regarding packaging of payload files.

AS4 Action configuration

An action's parameters define a repeatable transaction for your mailbox designated for the host system.

AS4 Action: Action Tab

See Composing an action on page 89 and AS4 Command Reference. See AS4 Host: Advanced Tab on page 206 for information about the available property values.

AS4 Command Reference

PUT

Send one or more files to the bank server.

```
PUT -MUL -DEL "source"
```

-MUL

Multiple file payload (attachments).

-DEL

If `PUT` is successful, delete the local file.

"*source*"

Local source path

- Path can be to a filename or to a directory.
- `*` and `?`, or a regular expression, are supported in filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default outbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

Note: The PUT command wizard will display an optional `mpc` parameter. This parameter is reserved for future use and it not used at this time.

GET

The GET command causes an AS4 Pull Request to be issued to the trading partner. The Pull Request synchronously returns one User Message, which may contain one or more payloads. Generally, the oldest payload on the trading partner's queue is returned.

```
GET
```

The `GET` command has no options because it always requests just a single User Message. There is an optional `mpc` parameter, however, that can be used to target a specific message partition channel. This value must match the **PMode.BusinessInfo.MPC** setting of your trading partner. When the `mpc` parameter is not specified, then **PMode.Security.PModeAuthorize** must be used to authenticate the request.

After the `GET` completes successfully, the source file is deleted by the trading partner.

Received file options, under **AS4 Host** > **AS4 Tab**, can be used to configure any special destination parameters for all received files, both solicited (through a `GET` command) and unsolicited (through a User Message push from the trading partner). See AS4 Host: AS4 Tab on page 204.

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"path"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.

- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.

- You can use * and ?, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use * and ?, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

CHECK

See CHECK command on page 943 for information about this advanced command.

SCRIPT

See to SCRIPT command on page 951 for information about this advanced command.

AS4 Comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

ebXML Hosts

The ebXML Message Service (ebMS) standard provides the ability to securely transport EDI (and other data, including binary and XML) to a remote host.

This guarantees that the message has not been changed in transit and is received and can be read only by the intended trading partner. A returned acknowledgment further guarantees that the intended trading partner has received the message.

ebMS uses the HTTP protocol as its transport mechanism to send files over the Internet. VersaLex uses the PUT (HTTP POST) action command to transport the secure data to the remote host.

ebXML Configuration

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.
4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See ebXML Host on page 231.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See ebXML Mailbox on page 249.
   c) Click **Apply** to save your work.
6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See ebXML Action on page 252.
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the product to prompt to you click **Apply** if you try to leave the page. However, in the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

ebXML Host

A host describes the remote server of your trading partner to which messages will be sent. The host's parameters specify its location and how it is reached. Your remote trading partner should have provided information to you in the form of a URL, which you will use to configure the host parameters.

This section describes how to configure the Generic ebXML pre-configured host.

ebXML Host: General Tab

The fields on the **General** tab typically remain unchanged unless you need to connect through a forward proxy or change the **Default Directories**.

Server Address

Either a fully qualified name (recommended) or an IP address.

This is the address of your trading partner's server that will receive your messages.

Port

The port on the server where your trading partner will receive your messages. If no port number is included in your trading partner's URL, default values are assumed.

Default value: `80` for HTTP and `443` for HTTPs (SSL)

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See Specifying default host directories on page 700 for information about setting the system default.
- `Direct Internet Access or VPN` - Use either a direct connection to the internet or a VPN.

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For the Cleo VLTrader and Cleo Harmony applications, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Note: If the host is has an external association, the default directories might be managed outside of the Cleo Harmony application and not shown here.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

ebXML Host: ebXML Tab

Store raw sent

Save the content of the HTTP header and raw (unprocessed) message sent to the remote host. The files are stored in the `ebXML\sent+received` directory under the root path. These files can be useful in diagnosing problems, but should be disabled if disk space needs to be conserved. Click **Resend** to send a duplicate of a previously stored raw message to the trading partner.

Use default file name

Allows the incoming file to be given the name specified in its associated field. Use this option to override the file name specified by the sender. This feature is useful in situations where the received file name must be something other than its original file name, and is common for IBM i / iSeries (AS/400) platforms where the file name must be specified with a .mbr extension. This field can also include any of the supported macros allowing for the incoming file to be named, for example, with a date-time stamp. Subdirectory path identifiers (for example, '/' or '\') can also be used in conjunction with macros to allow filtering of the incoming file to a specific subdirectory under the inbox based on the value of the macro variable. See Using macro variables on page 59 (Destination File context) for a discussion of all applicable macros.

Note: If a subdirectory path is specified and it does not already exist, it will automatically be created as needed unless the subdirectory path is under an inbox on the AS/400 Native File System. In that case, the physical file denoting the subdirectory path (in the form: DIRECTORY.FILE) must be created under the specified inbox before files can be written to it.

Add Content-Type Directory to Inbox

Allows you to sort incoming messages based on content-type to a subdirectory under the Inbox specified on the **General** tab. Specify each of the Content-Types you want to direct to specific subdirectories by entering a name in the **Directory** field. You can specify directories for Content-Types of: EDIFACT, X12, XML, Binary, Plain Text, EDI Consent and Other (a default for messages with all other Content-Types you might receive). You can specify the same subdirectory for multiple Content-Types. You can also leave Directory entries blank, which causes any received messages of that Content-Type to be stored in the Inbox specified on the **General** tab.

For IBM i / iSeries (AS/400) usage, see AS/400 Setup and installation on page 703 or AS/400 Network Access Setup on page 980 for information on configuring the Content-Type Inbox settings to access the Native File System (NFS).

Note: If you use this feature, incoming messages are placed in the specified folder based on the content type specified in the HTTP header of the message. The Cleo Harmony application does not check the actual content of the message to determine its content type.

ebXML Host: CPA Tab

CPA Id

Identifies the Collaboration-Protocol Agreement (CPS) between you and your trading partner. VersaLex does not actually implement the CPP/CPA portion of the ebXML specification, but a unique CPA Id must still be agreed upon between trading partners. The CPA Id can be a concatenation of the From and To Party Ids, a URI prefixed with the Internet domain name of one of the parties, a namespace offered and managed by some other naming or registry service, or some other mutually agreed to naming convention.

To Party Id(s)

Your trading partner's identifiers. One or more party ids can be listed (URI, email address, DUNS number, etc.) If the type attribute is not given in a party id, the value must be a URI.

My Party Id(s)

Your identifiers. If you need to override the default values from the Local Listener (because this trading partner requires different settings), select **Override Local Listener\ebMS CPA** check box and supply alternate values.

ebXML Host: HTTP Tab

Outbound

Indicates whether you use SSL or not for outbound file transfers.

HTTP

Do not require use SSL

HTTP/s

Require SSL for outbound file transfers.

If you select HTTP/s, you can select **Check certificate server name**

Inbound

HTTP/s only

Require your trading partner to use Secure Socket Layer (SSL) for inbound file transfers.

Command

In most cases the `CONNECT` command is not used and should be left blank. In rare instances, CONNECT is required by the remote server to identify the client, particularly if SSL has not been used.

Method

The only valid **Method** for AS2 commands is `PUT` ("`POST`").

Path

The server **Path** for the `PUT` command.

If the remote server is also using the Cleo Harmony application, the path is `/ebMS`. The resource path must be properly specified in order for your trading partner's ebMS installation to process messages from you. Given the URL provided by your remote trading partner in the form:

`http(s)://remote-host:port/`***`resource-path`***`?optional-parameters`

Enter the bolded portion in this field (if it was supplied).

Parameters

By default, no **Parameters** are specified for sending ebMS messages. If parameters are required, they must be obtained from your trading partner when the trading relationship is established. Given the URL provided by your remote trading partner in the form:

`http(s)://remote-host:port/resource-path?`***`optional-parameters`***

Enter the bolded portion in this field if it was supplied.

Headers

These header fields are filled in at the Mailbox and/or Action level and specify the values set in the HTTP headers that precede the body of the message sent.

At a minimum, the only **Header** required is the `SOAPAction: "ebXML"` header. **Content-Type:** is optional and can be specified at the mailbox and/or action level.

Note: Entering a value for the **Content-Type** header is optional. If **Content-Type** is not specified or if multiple payloads are attached in the message, the **Content-Type** is detected based first on file content and then the file extension. Detectable types include `application/edifact`, `application/edi-x12`, `application/edi-tradacoms`, `application/xml` (text/xml), `application/pdf`, `application/msword`, `application/x-msexcel`, `application/rtf`, `application/zip`, `image/bmp`, `image/gif`, `image/tiff`, `image/jpeg`, `text/plain`, `text/html`, and `video/mpg`.

These header fields are filled in at the Mailbox and/or Action level and specify the values set in the HTTP headers that precede the body of the message sent.

ebXML Host: Advanced Tab

Use the Advanced tab to configure certain properties for your ebXML host.

The host's **Advanced** tab contains several property settings fields. These settings typically do not affect the ability to connect to a host. However, some of these settings might need to be changed when configuring a runtime environment.

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for ebMS include:

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Allow Incoming Request With Missing Role Element

When set to "On", this option allows an incoming request without a role element value to be processed if it otherwise matches a configured ebMS mailbox.

Possible values: `On` or `Off`

Default value: `Off`

Always Send Multipart Messages

Indicates to always send a multipart MIME message to the trading partner, even when there is only one attachment in the message.

Possible values: `On` or `Off`

Default value: `On`

Async Ack Resends

Specifies the number of attempts that will be made to resend a transaction for which the asynchronous acknowledgment has not been received within the specified timeout period.

Possible values: Any value `-1`, `0` or `> 0`. When set to a value other than the default (-1), this value overrides the setting in the Local Listener.

Default value: `-1`

Async Ack Timeout

The maximum time (in minutes) to wait for an asynchronous acknowledgment before either resending the transaction (if Async Ack Resends > 0 in either the Host or Listener) or logging an error.

Possible values: Any value `-1`, `0` or `> 0`. When set to a value other than the default (-1), this value overrides the setting in the Local Listener.

Default value: `-1`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0 - n`

Default value: `0`

Compression- Signing Order

When both signing and compression are enabled, indicates which is applied first.

Possible values: `Sign then compress` or `Compress then sign`

Default value: `Sign then compress`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0 - n` seconds

`0` indicates no timeout

Default value: `150` seconds

Conversation Id XML Payload Element

When set, indicates the element name or names in the XML payload whose value should be used as the ebMS `ConversationId` value. When multiple element values are to be concatenated and/or when additional, constant character values are needed, the element names must be enclosed in < and >. If a specified element appears more than once in the payload, the first element value is used.

Possible values: Element namespace and local name (for example, `ed:ReferenceId`) or just local name. For example, `ReferenceId`.

For multiple elements and/or additional characters, enclose each element name in < and >. For example, `<UID>_<ReferenceId>`.

Disregard Incoming Preserve Message Order Request

When set to false, indicates that a received ebMS message containing the Message Order option will be rejected as not supported.

When set to true, the VersaLex system will accept an incoming request containing the Message Order option, but message order delivery inbound will not be strictly enforced.

Possible values: `On` or `Off`

Default value: `Off`

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Repetitive Listener Failures

When "Email On Fail" is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, an email alert will be sent when the failure is resolved. Failure resolution email alerts will not be sent for general Listener failures since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Enclose Content Type Start With <>

Indicates whether the Content-Type start parameter value for an outgoing ebMS multipart/related message should contain enclosing angle brackets. The examples shown in the ebMS v2 specification are inconsistent, and some implementations might only accept one format or the other. VersaLex will accept either format for incoming messages.

Possible values: `On` or `Off`

Default value: `Off`

Encryption-Signing Order

When both encryption and compression are enabled, indicates which is applied first.

Possible values:

- `Sign then encrypt`
- `Encrypt then sign`

Default value: `Sign then encrypt`

Encryption Algorithm

The method used to encrypt/decrypt payload.

Possible values:

- `AES/128`
- `AES/192`
- `AES/256`
- `SEED`
- `TripleDES`

Default value: `TripleDES`

Encryption Encrypted Key Id

Include the specified value as the Id attribute of the <xenc:EncryptedKey> element in the encrypted data.

Possible values: Any text

Encryption Include Certificate

Indicates to include the encryption certificate as an <ds:X509Certificate> element in the encrypted data

Possible values: `On` or `Off`

Default value: `Off`

Encryption IV

Specifies the initialization vector (IV) to be used for encryption/decryption. If specified, the configured IV is NOT added to or expected at the beginning of <CipherValue>.

The configured value must be prefixed with either a `c` or `x` to indicate whether the value following the prefix should be treated as a character or hexadecimal string, respectively.

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Repetitive Listener Failures

When `Execute On Fail` is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, the `Execute On Fail` command will be executed again when the failure is resolved. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure. Executions of the "Execute On Fail" command for resolution of general Listener failures will not be done since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0` - `n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Message Id Length

If set to a positive number, truncates the generated ebMS message ID if necessary.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Outbound Message Time To Live (hours)

Indicates how long a message has to be delivered before it is considered expired.

Possible values: `1 - 720`

Default value: `24`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
```

SHA-384
SHA-512

Default value: System Default

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: On or Off

Default value: On

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: On or Off

Default value: On

PGP V3 Signature

Profile Support

Indicates that an industry-specific business profile applies to this trading partner.

Possible values:

CDC PHIN - Centers for Disease Control and Prevention Public Health Information Network
STAR - Standards for Technology in Automotive Retail XML BODs
HL7 - Health Level Seven
TCD Super Gateway

Default value: None

Put Multiple Files Limits

Limits the number of files included in each generated multipart message when using the PUT -MUL option. The limit is only applied when sending out of a single directory; when sending multipart out of separate subdirectories, the files are kept as a group and not broken up into separate messages.

Possible values: -1 - n

-1 indicates no limit.

Default value: -1

Ref To Message Id XML Payload Element

When set indicates the element name or names in the XML payload whose value should be used as the ebMS RefToMessageId value. When multiple element values are to be concatenated and/or when additional, constant character values are needed, the element names must be enclosed in angle brackets (< and >). If a specified element appears more than once in the payload, the first element value is used.

Element namespace and local name (for example, ed:ReferenceId) or just local name (for example, ReferenceId). For multiple elements and/or additional characters, enclose each element name in angle brackets (< and >) (for example, <UID>_<ReferenceId>).

Reset Connection After Timeout On Response

When enabled will cause an immediate reset on the socket (instead of a graceful close) when a SocketTimeoutException occurs.

Possible values: On or Off

Default value: Off

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

Reuse SSL Sessions Across Actions

If selected, and if no forward proxy is being used for this host, SSL sessions from previous connections to the same destination (address and port number) may be resumed to avoid costly negotiation. If unselected, only SSL sessions used in the current action to the same destination may be resumed. When unselected, a new SSL session is created for the initial command port connection.

Possible values: `On` or `Off`

Default value: `On`

Signing Hash Algorithm

Specifies the signature hash algorithm used when signing an outgoing ebMS message. If not specified, the private key's signature hash algorithm is used by default. This setting affects both the signature and digest method algorithms. Only applies to RSA private keys.

Possible values:

`SHA-1`
`SHA-256`
`SHA-384`
`SHA-512`

Sign XML Payload If Signing

Indicates to sign XML payload in addition to signing the ebMS SOAP envelope.

Possible values: `On` or `Off`

Default value: `Off`

Sign XML Payload Omit XML Declaration

Indicates when signing to omit the XML declaration at the top of the XML payload

Possible values: `On` or `Off`

Default value: `Off`

SSL Allow Legacy Renegotiation

When selected, legacy renegotiation is allowed. If this property is not selected, the extension described in RFC5746 is used for renegotiation and the server must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Possible values: `On` or `Off`

Default value: `On`

SSL Cipher

Indicates a specific cipher, or an ordered list of ciphers, to be used with the server for SSL key exchange, encryption, and hashing.

If not set (that is, left blank), the list of default ciphers (all standard ciphers, excluding anonymous and non-encrypting) is presented to the server and the server picks one. If a regular expression (enclosed in brackets) or a wildcard expression is specified, a list of implemented ciphers (all standard ciphers, including anonymous and non-encrypting) is presented to the server, based on the conditions of the pattern. For example, if a regular

expression of `[.*ECDH.*]` is specified, then the list is a subset of all implemented ciphers that belong to the Elliptical-curve Diffie-Hellman group (for example, `ECDH` is in included in their string). In all cases, whenever a list is presented, it is always ordered by cryptographic strength, with the strongest listed first.

Based on the expression you type, the **List** button shows the resulting set of ciphers in the **SSL Cipher List** dialog box. Within this dialog box, you can view the list or select a specific cipher. If you select a cipher, then its value is displayed in this field.

Possible values:

Blank
a specific cipher picked from the SSL Cipher List dialog box
a regular/wildcard expression

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed. By default, this field is blank, designating that Cleo Harmony, Cleo VLTrader, or Cleo LexiCom will select the most recent version (currently TLS 1.3).

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed when selecting an SSL cipher. To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128`, or `256` (depending on the requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed. SSL 3.0 is the default value for compatibility with servers that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

Default value: `SSL 3.0`

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-CHECK commands: When Terminate On Fail is on, if a command fails, Email On Fail and Execute On Fail, if set, are processed, and then the action stops. When Terminate On Fail is off, if a command fails, Email On Fail and Execute On Fail, if set, are processed, and the action continues.

Regarding CHECK commands: Terminate On Fail is only honored if the ConditionsMet parameter is set and the result of the CHECK is classified as Error. The CHECK command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: On or Off

Default value: On

Unzip Use Path

Indicates whether or not zip entry paths should be used for LCOPY -UNZIP operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: On or Off

Default value: On

Wait For Execute On

Indicates whether execution should wait for processing to complete within an Execute On Fail, Execute On Successful Copy, Execute On Successful Receive, or Execute On Successful Send command. Note that this option does not apply to native AS400 execution.

Possible values: On or Off

Default value: On

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If System Default is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
AES-128
AES-192
AES-256
```

Default value: System Default

Zip Comment

Specifies the comment to be added to the zip archive file in LCOPY -ZIP operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for LCOPY -ZIP operations. If System Default is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

```
System Default
```

9 - (Best Compression)
8
7
6
5
4
3
2
1
0 - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

ebXML Mailbox

Mailbox parameters allow you access to the remote host and define the security of files being sent.

ebXML Mailbox: ebXML Tab

Select options for encryption and signing outbound messages and security for inbound messages. Select the acknowledgment format if necessary.

Encrypted

Enable or disable TripleDES encryption when sending messages. See Cryptographic Services on page 975 for general information about encryption.

Signed

Enable or disable signing messages when sending them.

Ack

Enables the **Acknowledgment** section and includes a request for an acknowledgment (receipt) from your trading partner.

Compressed

Compress the message using GZIP compression. Compression is generally used for large files to conserver bandwidth and make the transfer more efficient and secure.

Synchronous Reply

Require requested acknowledgments and any ebXML errors be returned synchronously, using the same HTTP session as the HTTP response. If **Synchronous Reply** is cleared, requested acknowledgments and any ebXML errors will be returned asynchronously by your trading partner, as part of a new HTTP session in an HTTP request.

Eliminate Duplicates

Your trading partner checks for duplicate message IDs. If a duplicate is discovered, the message payload is ignored.

Preserve Message Order

Your trading partner ensures that messages are processed in proper sequence. VersaLex does not currently support preserving message order on incoming messages.

Acknowledgment

Signed

Request a signed acknowledgment.

Forward Ack to Email

An additional VersaLex feature is the ability to forward a copy of the acknowledgment received either synchronously or asynchronously to an email recipient when **Forward Ack to Email** is selected.

Inbound Message Security

When you select any of the options in this section,

Force Encryption

Force Signature

When you select **Force Encryption** or **Force Signature**, all inbound messages are checked for the required security level. An error is logged and the message is rejected if the message is not received according to the corresponding message security settings. If either setting is not selected (default), the message is not checked for conformance with that security setting.

Honor Reply Requests

Accept requests for replies for messages that match the setting you choose from the following:

- **Any** - accept any message.
- **Asychronous** - accept only messages with asynchronous reply requests.
- **Synchronous** - accept only messages with synchronous reply requests.

Description

Optional. Provide a human readable description of the outgoing messages.

Ping

Click to check if the trading partner's message service is currently accepting messages.

Message Status

Click to check the status of a previously sent message.

ebXML Mailbox: CPA Tab

Whether you specify `to` and `from` roles explicitly or leave the fields blank, an ebXML mailbox corresponds to one and only one collaboration role within the CPA. Multiple mailboxes under one ebXML host must have different `from` roles and/or different services.

To Role

Optional. Identifies your trading partner's authorized role (for example, buyer, seller, or dealer) usually via a URI.

To Service

To Action

These values must match your trading partner's settings. Required if you are sending messages to your trading partner using this mailbox.

From

This section contains fields you can use to override values you set at the Local Listener level.

Override Local Listener\ebMS CPA

Enables several fields in which you can provide values to override ebMS/CPA parameters set at the Local Listener level.

My Role

Identifies your authorized role (for example, buyer, seller, or dealer) usually using a URI. If necessary, your normal role can be overridden in the ebXML host and mailbox respectively for a specific trading partner.

My Service(s)

Messages received from your trading partner must match these values. If you list more than one service, each one must be on its own line. If necessary, your normal services can be overridden in the ebXML mailbox for a specific trading partner.

My Action(s)

Messages received from your trading partner must match these values. If you list more than one action, each one must be on its own line. If necessary, your normal actions can be overridden in the ebXML mailbox for a specific trading partner.

ebXML Mailbox: Certificates Tab

Associate a trading partner's signing and encryption certificates with this ebXML mailbox and override the signing and encryption certificates defined in the Local Listener, if necessary.

You must acquire your trading partner's signing and encryption certificates and provide yours to your trading partner. See Acquiring your trading partner's signing and encryption certificates on page 86 and Creating and providing your signing/encryption certificates on page 86.

Trading Partner's Certificates

Signing Certificate

The name of the file containing your Trading Partner's signing certificate. Specify a value or click **Browse** to navigate to the file you want to select.

If you do not specify a signing certificate, the Cleo Harmony application uses all the certificates in its certificate store to determine if the signature of the incoming data message is trusted.

Encryption Certificate

The name of the file containing your Trading Partner's encryption certificate. Specify a value or click **Browse** to navigate to the file you want to select.

Use encryption certificate

Indicates that your trading partner uses the same certificate for signing and encryption, which is the general practice among most trading partners. When you select this check box, the **Signing Certificate** field is populated with the same certificate you selected in the **Encryption Certificate** field.

My Certificates

Override Local Listener Certificates

Enables fields where you specify signing and encryption certificates to use with this particular partner instead of the certificates you configured for the Local Listener. See Configuring certificates for Local Listener on page 758.

If you override the default certificates, you must also exchange the certificates you specify here with your partner.

Exchange Certificates

Displays the Certificate Exchange dialog box, which allows you to send your user and SSL certificates to your trading partner. See Exchanging certificates with your trading partner on page 672.

Signing Certificate Alias

The name of the signing certificate registered with the Cleo Harmony application through the Certificate Manager. The certificate must be the same as the one exchanged with your remote trading partners, unless you want to override it at the Mailbox level. See Local HTTP Users Configuration on page 834.

Click **Browse** to navigate to and select a certificate. Enter the **Password** for your signing certificate's private key.

Encryption Certificate Alias

The certificate for decrypting your trading partner's messages, if you have created or obtained a separate certificate.

Click **Browse** to navigate to and select a certificate. Enter the **Password** for your encryption certificate.

Use signing certificate

Select this check box to use the same certificate for signing and decrypting your trading partner's messages. The **Encryption Certificate Alias** and **Password** are populated to match the **Signing Certificate Alias** and disabled.

Exchange Certificates

Invokes the **Certificate Exchange** dialog box. If you override the default the certificates, you must exchange these alternate certificates with your trading partner.

ebXML Mailbox: HTTP Tab

The mailbox's **HTTP** tab allows you to assign a **Content-Type** for the documents to be transferred.

You can include optional parameters in valid **Content-Type** values by adding a semi-colon (;) after the value followed by the name=value pair(s). Multiple parameters must be separated by semicolons. For example, to include a 'charset' parameter for the 'XML' **Content-Type** value, edit the XML field like this:

```
XML; charset=utf-8
```

During the packaging phase of the message, the XML value is converted to 'application/xml' and any optional parameters are appended. Parameters are only appended to the **Content-Type** of the payload parts.

If a **Content-Type** is not specified, VersaLex will attempt to detect the content type.

ebXML Mailbox: Security Tab

If HTTP/s is specified in the host's **HTTP** tab, a remote host can issue client certificates. In this case, import the client certificate and then specify or browse for the imported certificate's alias and password. See Certificate management on page 661.

ebXML Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information regarding packaging of payload files.

ebXML Trading Partner

A trading partner's parameters define a unique identifier on the host system. By default, the **Trading Partner** branch is not created since it is not necessary for ebXML transactions.

ebXML Action

An action's parameters capture a repeatable transaction for your mailbox on the host system. Create a new action under the mailbox.

ebXML Action: Action Tab

Use the **Action** tab to configure commands within the action. See Composing an action on page 89. See also HTTP Command Reference on page 139.

Testing Your ebXML Installation

You can test your ebXML installation by configuring a host that will send messages to your Local Listener, therefore looping the messages back to yourself. Before attempting a trading relationship, you should test and validate that you can send and receive messages at your local installation. This will help narrow down connectivity issues that are due to firewall problems and not due to improper installation and configuration.

1. Configure the ebXML Message Service in the Local Listener. See Configuring ebXML Message Service on page 772.
2. Clone and activate the Generic ebXML preconfigured host and rename it to **Looptest ebXML**.
3. Configure the ebXML Looptest host:
   a) In the host **General** tab, set the **Server Address** to "localhost" and the **Port #** to the Local Listener's HTTP port (usually 5080).
   b) In the host **CPA** tab, set the **CPA Id** to "looptest" and set the **To Party Id(s)** to match the Local Listener \ebMS CPA **My Party Id(s)**.
   c) In the mailbox **CPA** tab, set the **To Role** to match the Local Listener\ebMS CPA **My Role**. Also set the **To Service** and **To Action** to match one of the Local Listener\ebMS CPA **My Service(s)** and **My Action(s)**.
   d) In the action **Action** tab, change the PUT command's source file to be "test\test.edi" and remove the `-DEL` option.
4. In the action **Action** tab, run the action. Messages similar to the ones shown below will appear in the messages pane in the lower portion of your Cleo Harmony application.

```
16:54:10  <send>myMailbox@Looptest ebXML  Run: type="Interactive"
16:54:11  <send>myMailbox@Looptest ebXML  Command: "PUT testtest.edi" type="HTTP" line=2
16:54:11  <send>myMailbox@Looptest ebXML    Detail: "Connecting to http://localhost:5080..."
16:54:11  <send>myMailbox@Looptest ebXML    File: "outboxtesttest.edi" direction="Local->Host" number=1 of 1 fileSize=1533 fileTimeS
16:54:11  <send>myMailbox@Looptest ebXML    HTTP: "POST /ebMS"
16:54:11  <send>myMailbox@Looptest ebXML    Detail: "SOAPAction: "ebXML""
16:54:11  <send>myMailbox@Looptest ebXML    Detail: "Sending plain (unsigned / uncompressed / unencrypted) message..." level=1
16:54:11  <send>myMailbox@Looptest ebXML    Detail: "Sent MessageId=20050110-225411-00225-3@aevett1.dficomm.dficom.com"
16:54:11  <send>myMailbox@Looptest ebXML    Detail: "LocalPort: 1487 / RemotePort: 5080" level=1
16:54:11  <send>myMailbox@Looptest ebXML      Transfer: kB/sec=27.584 kBytes=3.586 seconds=0.13
16:54:11  <send>myMailbox@Looptest ebXML    Detail: "Waiting for response..." level=1
16:54:11  Local Listener(33)  ebMS: "Message received from 127.0.0.1"
16:54:11  Local Listener(33)    Detail: "LocalPort: 5080 / RemotePort: 1487" level=1
16:54:11  Local Listener(33)    Detail: "Validating SOAP envelope..." level=3
16:54:13  Local Listener(33)    Detail: "Received MessageId=20050110-225411-00225-3@aevett1.dficomm.dficom.com"
16:54:13  Local Listener(33)    Detail: "ebXML message is for 'Looptest ebXML\myMailbox'."
16:54:13  Local Listener(33)    Detail: "ebXML message is a 'Receive' action."
16:54:13  Local Listener(33)    Detail: "This is payload" level=1
16:54:13  Local Listener(33)    File: "<Payload1>" direction="Host->Local" destination="inboxtest137.edi" number=1 of 1 transferID="ebX
16:54:13  Local Listener(33)      Transfer: kB/sec=2.685 kBytes=4.913 seconds=1.83
16:54:13  <send>myMailbox@Looptest ebXML    Response: "204 No Content"
16:54:13  <send>myMailbox@Looptest ebXML    Result: "Success" "No acknowledgment requested."
16:54:13  Local Listener(33)    Response: "204 No Content"
16:54:13  <send>myMailbox@Looptest ebXML  End
16:54:13  Local Listener(33)    Result: "Success"
```

5. If signing and encryption is desired:
   a) First export the Local Listener Signing and Encryption Certificate(s) into the Cleo Harmony `certs\` directory.
   b) Then in the mailbox **Certificates** tab, set the Trading Partner's Certificates to these certificates.

c) In the mailbox **ebXML** tab, select **Signed** and **Encrypted**.

d) In the action **Action** tab, rerun the action. Messages similar to the ones shown below should now appear.

```
17:04:57  <send>myMailbox@Looptest ebXML  Run: type="Interactive"
17:04:57  <send>myMailbox@Looptest ebXML  Command: "PUT test\test.edi" type="HTTP" line=2
17:04:57  <send>myMailbox@Looptest ebXML    Detail: "Connecting to http://localhost:5080..."
17:04:57  <send>myMailbox@Looptest ebXML    File: "outbox\test\test.edi" direction="Local->Host" number=1 of 1 fileSize=1533 fileTimeS
17:04:57  <send>myMailbox@Looptest ebXML    HTTP: "POST /ebMS"
17:04:57  <send>myMailbox@Looptest ebXML    Detail: "SOAPAction: "ebXML""
17:04:58  <send>myMailbox@Looptest ebXML    Detail: "Sending signed and encrypted message..." level=1
17:04:58  <send>myMailbox@Looptest ebXML    Detail: "Sent MessageId=20050110-230457-00549-4@aevett1.dficomm.dficom.com"
17:04:58  <send>myMailbox@Looptest ebXML    Detail: "LocalPort: 1498 / RemotePort: 5080" level=1
17:04:58  <send>myMailbox@Looptest ebXML      Transfer: kB/sec=9.087 kBytes=7.542 seconds=0.83
17:04:58  <send>myMailbox@Looptest ebXML    Detail: "Waiting for response..." level=1
17:04:58  Local Listener(34)  ebMS: "Message received from 127.0.0.1"
17:04:58  Local Listener(34)    Detail: "LocalPort: 5080 / RemotePort: 1498" level=1
17:04:58  Local Listener(34)    Detail: "Validating SOAP envelope..." level=3
17:04:59  Local Listener(34)    Detail: "Received MessageId=20050110-230457-00549-4@aevett1.dficomm.dficom.com"
17:04:59  Local Listener(34)    Detail: "ebXML message is for 'Looptest ebXML\myMailbox'."
17:04:59  Local Listener(34)    Detail: "ebXML message is a 'Receive' action."
17:04:59  Local Listener(34)    Detail: "This is signed payload" level=1
17:05:00  Local Listener(34)    Detail: "This is encrypted payload" level=1
17:05:00  Local Listener(34)    File: "<Payload1>" direction="Host->Local" destination="inbox\test138.edi" number=1 of 1 transferID="ebX
17:05:00  Local Listener(34)      Transfer: kB/sec=4.11 kBytes=9.577 seconds=2.33
17:05:02  <send>myMailbox@Looptest ebXML    Response: "204 No Content"
17:05:02  <send>myMailbox@Looptest ebXML    Result: "Success" "No acknowledgment requested."
17:05:02  <send>myMailbox@Looptest ebXML  End
17:05:02  Local Listener(34)    Response: "204 No Content"
17:05:02  Local Listener(34)    Result: "Success" "Signature verified"
```

6. Set other ebXML options as desired.

ebXML-Specific Directories

The following additional directories will be created either during the ebXML installation or as needed by the application:

Directory	Purpose

ebXML\	The `ebXML\ack` directory contains subdirectories for received (and optionally sent) acknowledgments. This directory can be changed on the ebXML Message Service Panel. Acknowledgments can be automatically archived by the application or manually archived by the user from the "Acks" tab on the listener panel. Archived acknowledgments are stored in `ebXML\ack\received\archive\ack.zip` or `ebXML\ack\sent\archive\ack.zip`. The `ebXML\data` directory contains an ebXMLmsgs.txt file that is used by the application to determine the receipt of duplicate messages. Entries in this file are retained for the time interval configured on the ebXML Message Service. The `ebXML\schemas` directory contains XML schema (.xsd) files that describe the format of various ebXML documents. The `ebXML\sent+received` directory contains "raw" (unprocessed) incoming and outgoing messages. These files can be helpful in diagnosing problems. Old files should be deleted or archived by the user, if necessary. The `ebXML\unsent` directory contains raw header, data and message setup information files. These files are used if a message needs to be retransmitted and are deleted automatically by the application once the message transfer has either completed successfully or has failed due to timeouts, exceptions or exhausting the number of retries.
lostandfound\	Default inbox where incoming data will be deposited when the application cannot determine where to put it.
temp\	Temporary location where large incoming messages or compressed messages may be stored while they are being processed by the application. These are deleted automatically once the message has been completely processed. This directory is only created if large messages or compressed messages need to be processed.

SSH FTP Hosts

Use the SSH FTP host to specify a client file transfer interface to an SSH FTP server.

Not all SSH FTP servers will support or require the full set of host commands allowed by VersaLex. At a minimum, the server must support PUT and/or GET. The following action commands are available on VersaLex:

Table 12: Host commands

Command	Purpose	Underlying SSH FTP method
PUT	Send one or more files to the host	GET
GET	Receive one or more files from the host	PUT
DIR	Get a directory listing of available files from the host	LIST
CD	Changes the current directory on the host	CD
QUOTE *command*	Sends a raw command to the server	command Supported commands include: CHGRP CHMOD CHOWN MKDIR MKDIRS PWD RENAME RM RMDIR STAT SYMLINK

Table 13: Local commands

Command	Purpose	Underlying SSH FTP method
SYSTEM	Execute a local system command	-
WAIT	Pause	-
SET	Sets a property	
CLEAR	Clears a string property	
LCOPY	Copy one or more local files	-
LDELETE	Delete one or more local files	-
LREPLACE	Replace bytes in one or more local files	-

Command	Purpose	Underlying SSH FTP method
CHECK	Check for a transfer, file, or directory (VLTrader and Harmony only)	-
SCRIPT	Execute a JavaScript File (VLTrader and Harmony only)	-

SSH FTP Configuration

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.

4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See SSH FTP Host on page 257.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See SSH FTP Mailbox on page 273.
   c) Click **Apply** to save your work.
6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See SSH FTP Action on page 275.
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the product to prompt to you click **Apply** if you try to leave the page. However, in the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

SSH FTP Host

A host's parameters specify its location and how it is reached.

SSH FTP Host: General Tab

Server Address

Either a fully qualified name (recommended) or an IP address.

This is the address of your trading partner's server that will receive your messages.

Port

The port on the server where your trading partner will receive your messages. If no port number is included in your trading partner's URL, default values are assumed.

Possible values: Either a specific port number or `-1` to indicate the default port for SSH FTP (`22`)

Default value: `22`

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` - Use either a direct connection to the internet or a VPN.

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For the Cleo VLTrader and Cleo Harmony applications, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Note: If the host is has an external association, the default directories might be managed outside of the Cleo Harmony application and not shown here.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

SSH FTP Host: SSH FTP Tab

Host Key Verification

Host Key Verification compares the SSH FTP host key sent from the SSH FTP server to the value in the **Host Key** field. If the value in the **Host Key** field does not match the value returned from the SSH FTP server, the connection is terminated.

Verify Host Key

Select this check box to enable the **Host Key** field and the **Set Key** button, and allow host key verification.

Clear the **Verify Host Key** check box to disable fields and verification.

Host Key

The SSH FTP server certificate fingerprint retrieved from the SSH FTP server.

Click **Set Key** to connect to the SSH FTP server to retrieve the host key. If the host key is retrieved successfully, the **Host Key** field is updated with the server certificate fingerprint.

SSH FTP Host: Advanced Tab

Use the **Advanced** tab to configure certain properties for the SSH FTP host.

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols.

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Block Size

The block size to be used for file transfers. Some SSH FTP servers cannot transfer files with the default Block Size. If the server is able to transfer files smaller than the default Block Size, try using a smaller Block Size of 32767.

Possible values: Any value greater than zero.

Default value: `65535`

Buffer Requests

Indicates that commands can be buffered to minimize the command/response delays during file transfers when the round trip time is significant.

Possible values: `On` or `Off`

Default value: `On`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0` - `n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Create File Times

When creating files, sets the file creation and modified times to the current time. Used for compatibility with certain servers that cannot create files without the times specified.

Possible values: `On` or `Off`

Default value: `Off`

Delete Zero Length Files

Indicates whether files received that are zero-length (<= 5 bytes) should be deleted rather than processed.

Possible values: `On` or `Off`

Default value: `Off`

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0 - n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Get Number of Files Limit

Limits the number of files retrieved from a server directory listing by one `GET` command.

Possible values: `0 - n`

`0` indicates no limit.

Default value: `0`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Ignore Directory Listing Attributes

Enable this property to allow directory listings on non-directory paths.

Possible values: `On` or `Off`

Default value: `Off`

Ignore STAT Errors

Enable this property to ignore FXP_STAT errors that occur when opening a directory.

Possible values: `On` or `Off`

Default value: `Off`

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

Interim Retrieve

Indicates to set result of any successfully retrieved file to `Interim Success` rather than `Success`. This would normally be used when transfer logging is being monitored by a backend system to allow coordination of any post processing of the received file that needs to occur prior to setting the transfer status to `Success`.

Possible values: `On` or `Off`

Default value: `Off`

Key Exchange Data Limit (mbytes)

Maximum number of bytes allowed over a connection between key exchanges before a re-exchange is initiated. Set this value to zero to disable this limit from initiating a key exchange.

Possible values: `0 - n`

Default value: 1024

Key Exchange Time Limit (minutes)

Maximum number of minutes allowed over a connection between key exchanges before a re-exchange is initiated. Set this value to zero to disable this limit from initiating a key exchange.

Possible values: `0 - n`

Default value: 60

Large File Transfer

Select this option to use a large window size and send a `simple@putty.projects.tartarus.org` channel request to the server indicating that the server should also use a large window size, as there will only be one channel open on the connection.

Possible values: `On` or `Off`

Default value: `Off`

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Next File On Fail

When a download fails, indicates whether a wildcarded `GET` should proceed to the next available file rather than terminate if the server is still connected.

Possible values: `On` or `Off`

Default value: `Off`

Only Retrieve First Available File

Indicates a `GET *` should only retrieve the first available file from the server.

Possible values: `On` or `Off`

Default value: `Off`

Only Retrieve Last Available File

Indicates a `GET *` should only retrieve the last available file from the server.

Possible values: `On` or `Off`

Default value: `Off`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
```

`Date/Time Modified`

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

`System Default`
`ZIP`
`ZLIB`

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

`System Default`
`TripleDES`
`Blowfish`
`CAST5`
`DES`
`AES-128`
`AES-192`
`AES-256`
`Twofish`

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512
```

Default value: `System Default`

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: `On` or `Off`

Default value: `On`

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: `On` or `Off`

Default value: `On`

PGP V3 Signature

Post Get Command

Post Put Command

In an action, specify commands to be executed only after a successful `GET` or `PUT` as post-get or post-put commands, respectively. When using this property, use a `SET` command within the action **before the `GET` or `PUT` command** rather than the **Advanced** tab.

The Post Put Command can be set to `QUIT`, which allows a disconnect and reconnect between file uploads when necessary.

If multiple FTP commands are needed after the `GET` or `PUT`, set this property to **all** of the commands separated by semicolons (;). If a specific FTP command needs to contain a semicolon, enclose that specific FTP command in quotes ("). Use of macro variables is supported. Refer to Using macro variables on page 59 (Post/Pre Command context) for a list of the applicable macros.

Preferred Cipher Algorithm

Used to control the transport cipher algorithm preference. The preferred algorithm is used if the server also supports it.

Possible values:

```
3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour128
```

```
arcfour256
blowfish-cbc
cast128-cbc
twofish128-cbc
twofish192-cbc
twofish256-cbc
```

If no preference is specified, the cipher algorithms are presented to the server in this order:

`blowfish-cbc`, `3des-cbc`, `aes128-cbc`, `aes128-ctr`, `aes192-cbc`, `aes192-ctr`, `aes256-cbc`, `aes256-ctr`, `arcfour128`, `arcfour256`, `cast128-cbc`, `twofish128-cbc`, `twofish192-cbc`, `twofish256-cbc`

Preferred Compression Algorithm

Used to control the transport compression algorithm preference. The preferred algorithm is used if the server also supports it.

Possible values:

```
none
zlib
zlib@openssh.com
```

If no preference is specified, the compression algorithms are presented to the server in this order: `none`, `zlib`, `zlib@openssh.com`

Preferred Key Exchange Algorithm

Used to control the transport key exchange algorithm preference. The preferred algorithm is used if the server also supports it.

Possible values:

- `curve25519-sha256@libssh.org`
- `diffie-hellman-group-exchange-sha256`
- `diffie-hellman-group1-sha1`
- `diffie-hellman-group14-sha1`
- `ecdh-sha2-nistp256`
- `ecdh-sha2-nistp384`
- `ecdh-sha2-nistp521`

If no preference is specified, the key exchange algorithms are presented to the server in this order:

`curve25519-sha256@libssh.org`, `diffie-hellman-group-exchange-sha256`, `ecdh-sha2-nistp256`, `ecdh-sha2-nistp384`, `ecdh-sha2-nistp521`, `diffie-hellman-group14-sha1`, `diffie-hellman-group1-sha1`

Preferred MAC Algorithm

Used to control the transport MAC algorithm preference. The preferred algorithm is used if the server also supports it.

Possible values:

- `hmac-md5`
- `hmac-md5-96`
- `hmac-sha1`
- `hmac-sha1-96`

- hmac-sha2-256
- hmac-sha2-256-96
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-512
- hmac-sha2-512-96
- hmac-sha2-512-etm@openssh.com

If no preference is specified, the MAC algorithms are presented to the server in this order:

hmac-sha2-256, hmac-sha2-512, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1, hmac-sha2-256-96, hmac-sha2-512-96, hmac-sha1-96, hmac-md5, hmac-md5-96

Preferred Public Key Algorithm

Used to control the transport public key algorithm preference. The preferred algorithm is used if the server also supports it.

Possible values:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- rsa-sha2-256
- rsa-sha2-512
- ssh-dss
- ssh-dss-sha256
- ssh-dss-sha512
- ssh-ed25519
- ssh-rsa

Default value: None

If no preference is specified, the public key algorithms are presented to the server in this order: rsa-sha2-256, rsa-sha2-512, ssh-dss-sha256, ssh-dss-sha512, ssh-rsa, ssh-dss, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519

Note: The ssh-ed25519 algorithm is not supported in FIPS mode.

Pre Get Command

Pre Put Command

In an action, specify commands to be executed before a GET or PUT as pre-get or pre-put commands, respectively. This has the benefit of keeping the log results relative to just GETs and PUTs (especially important for Cleo VLTrader and Cleo Harmony GET transfer logging). In addition, for the PUT, it avoids connecting and logging into the server when there are no files to send. When using this property, use a SET command within the action **before the GET or PUT command** rather than the **Advanced** tab.

If multiple FTP commands are needed prior to the GET or PUT, set this property to **all** of the commands separated by semicolons (;). If a specific FTP command needs to contain a semicolon, enclose that specific FTP command in quotes ("). Use of macro variables is supported. See Using macro variables on page 59 (Post/Pre Command context) for a list of the applicable macros.

Pre Put Command For First File Only

If a Pre Put Command is specified, indicates whether to execute them before each file being transferred by the PUT or only before the first file transfer.

Possible values: `On` or `Off`

Default value: `On`

Preserve File Timestamps

When selected, the original file timestamp is retained for the destination file for `GET` and `PUT`.

Possible values: `On` or `Off`

Default value: `Off`

REST Enabled

Allows the host to be accessible through the REST API. This feature is only supported on **AS2**, **AS4**, **FTP** and **SSH FTP** and *only when the host has exactly one mailbox*.

When this setting is enabled, new mailboxes cannot be created and the existing mailbox cannot be cloned, disabled, or removed.

Possible values: `On` or `Off`

Default value: `On` for **AS2**. **AS4**, **FTP** and **SSH FTP** when the host has exactly one mailbox. `Off` in all other cases.

Resume Failed Transfers

When selected and a transfer fails (and Command Retries > 0), attempt to resume the transfer on a retry. If OpenPGP is enabled on the packaging tab (see Configuring mailbox packaging on page 79), the entire file is transferred instead of resuming with a partial file. The server must support the `FEAT`, `SIZE`, and `REST STREAM` extensions to FTP. For more information, visit http://tools.ietf.org/html/rfc3659.

Possible values: `On` or `Off`

Default value: `Off`

Retrieve Directory Sort

Used to control the order in which files are downloaded from the FTP server. Using this property does cause the LIST command rather than the NLST command to be used when VersaLex is determining the available file list – which might be a problem if the server responds with different lists (e.g. NLST only lists files not previously downloaded while LIST lists all files regardless). Windows and Unix/Linux FTP servers are supported.

Possible values:

```
Alphabetical (ascending)
Alphabetical (descending)
Date/Time Modified (ascending)
Date/Time Modified (descending)
Size (ascending)
Size (descending)
```

Retrieve Last Failed File First

If a file download previously failed and you are attempting to `GET` a list of files again, this property indicates whether the previously failed file should be attempted first.

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

Server Side Path Name

Optional. Default starting directory for a session. If you do not specify a value, session starts at `/`.

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

Window Size (bytes)

Maximum number of received bytes allowed before a window adjustment is required. When receiving (using a `GET` command), a typical Window Size setting would be equal to the largest expected file size or the default setting, whichever is greater. This setting will not normally affect sends, since the receiver (the server) requires the majority of adjustments.

Possible values: `0-n`

Default value: `131072`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
AES-128
AES-192
AES-256
```

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

SSH FTP Mailbox

A mailbox's parameters allow you access to the host system.

Note: This feature is being deprecated. For similar functionality, use a Users host. See Users Host on page 516 for more information.

SSH FTP Mailbox: SSH FTP Tab

Note: By default, SSH FTP hosts have the **REST Enabled** advanced property set to `On`, which prevents the host from having more than one mailbox. If you want more than one mailbox for this host, set the **REST Enabled** advanced property to `Off`. See SSH FTP Host: Advanced Tab on page 259.

You configure the **SSH FTP** mailbox using a Password and/or one of two Public Key Authentication (PKA) methods. Your Trading Partner should specify the required type(s) of authentication necessary to access your account.

To use PKA, you must create your authentication certificate (see Creating and providing your signing/encryption certificates on page 86) and then export an SSH FTP key to send to your trading partner in either OpenSSH FTP Public Key or SSH FTP Public Key (IETF) format. See Certificate management on page 661 and Exporting certificates on page 668. See also Private key authentication on page 274.

User Name

Password

Credentials for authentication to the remote server.

Use Public Key Authentication

Enables fields necessary to use public key authentication with a user certificate. See Private key authentication on page 274.

Exchange Certificates

Displays the Certificate Exchange dialog box, which allows you to send your certificates to your trading partner. See Exchanging certificates with your trading partner on page 672.

Certificate Alias

Certificate Password

Credentials used to access the user certificate for PKA.

Use Key From File

Enables fields necessary to use PKA with an existing SSH private key file. This option is only available when you select **Use Public Key Authentication**. See Private key authentication on page 274.

Private Key File

Private Key Password

Name of and the password protecting the SSH private key file to use for PKA.

Private key authentication

Private key authentication (PKA) allows you to connect to your Trading Partner's remote server without exchanging your password over the Internet. PKA uses two keys: a private key that only you have, and a public key placed on the accessing server, usually by your Trading Partner's system administrator when the account is set up. In the Cleo Harmony application, the private key portion is maintained securely in a User Certificate protected with the **Certificate Password**. The **Certificate Alias** specifies the desired User Certificate to use for PKA.

Note: You must provide your Trading Partner with the corresponding SSH Public Key using the Certificate Manager. Using options **Export >OpenPGP** or **SSH FTP Keys** select either the **OpenSSH FTP Public Key** or **SSH FTP Public Key** (IETF) format. Do not select and send the **SSH FTP Private Key** format to your Trading Partner.

Alternatively, you can use an existing private key file. This file should be stored in a secure place and protected with a password. This feature is applicable only if you have an existing SSH private key for authentication with your Trading Partner and you are using JRE1.3. SSH private keys have no standard format. OpenSSH, SSH FTP Public Key (IETF), PuTTY, and ssh.com all have different proprietary formats. A private key generated with one cannot immediately be used with another. The Cleo Harmony application supports both OpenSSH and SSH FTP Public Key (IETF) private key file formats. If the private key is in a format not supported by the Cleo Harmony application, you should export if from the application that created it in an OpenSSH format. To determine the format of your key you can simply open it using a text editor and compare it to the partial example formats listed below.

Table 14: Supported Private Key Formats

Type	Partial Example

IEFT (DSA)	`---- BEGIN SSHTOOLS ENCRYPTED PRIVATE KEY ----`
	`Comment: 1024-bit DSA`
	`Subject: John Doe`
	`AAAACDNERVMtQ0JD3yrqcRRh1OwAAAFQof0uP52Ya5iOnuVr`
	`+o9TpQwXrOQfjPp0w8+GQ9uJ7`

IETF (RSA)	`---- BEGIN SSHTOOLS ENCRYPTED PRIVATE KEY ----`
	`Comment: 1024-bit RSS`
	`Subject: Jonh Doe`
	`AAAACDNERVMtQ0JDEOMMw0wR0TwAAAEoUYoVJjvLn7lEnvus`

OpenSSH (RSA)	`-----BEGIN RSA PRIVATE KEY-----` `MIICWwIBAAKBgQDzl7h/4lkzqSPR5GhpwYr5MmUL6IeiY9TA`

OpenSSH (DSA)	`-----BEGIN DSA PRIVATE KEY-----`
	`MIIBuwIBAAKBgQD42waNRIv7eJQoTR1PSQt`
	`+A2o8F9P1pGKLaLyw/rAg8N4FEHIN`

Table 15: Unsupported Private Key Formats

Type	Partial Example

PuTTY	`PuTTY-User-Key-File-2: ssh-rsa`
	`Encryption: none`
	`Comment: rsa-key-20070808`
	`Public-Lines: 4`
	`AAAAB3NzaC1yc2EAAAABJQAAAIBw8VeSCq0goiOwWqrlMu7F`
	`+N1QXAcBPdmvYttw`

SSH.COM	`---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----`
	`Comment: "rsa-key-20070808"`
	`P2/56wAAAiwAAAA3aWYtbW9kbntzaWdue3JzYS1wa2NzMS1z`

SSH FTP Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information about payload file packaging.

SSH FTP Action

An action's parameters capture a repeatable transaction for your mailbox on the host system.

You create actions under a mailbox.

SSH FTP Action: Action Tab

See Composing an action on page 89 and SSH FTP Command Reference on page 276.

SSH FTP Command Reference

CD

Changes the current working directory on the host.

```
CD "directory"
```

"*directory*"

The new working directory.

CHECK

See CHECK Command for information about this command.

CHGRP

Changes the group ID of the file or directory on the host.

```
QUOTE CHGRP group "path"
```

group

The numeric group id for the new group.

"*path*"

The path to the remote file/directory. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

CHMOD

Changes the access permissions or modes of the file or directory on the host.

```
QUOTE CHMOD permissions "path"
```

permissions

The absolute mode of the file/directory. Absolute modes are octal numbers specifying the complete list of attributes for the files; you specify attributes by OR'ing together these bits.

- `0400` - Individual read
- `0200` - Individual write
- `0100` - Individual execute (or list directory)
- `0040` - Group read
- `0020` - Group write
- `0010` - Group execute
- `0004` - Other read
- `0002` - Other write
- `0001` - Other execute

"path"

The path to the remote file/directory. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

CHOWN

Changes the user ID of the file or directory on the host.

```
QUOTE CHOWN owner "path"
```

owner

The numeric user id for the new owner.

"path"

The path to the remote file/directory. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

Comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

DIR

Get a directory listing of available files from the host.

```
DIR "source"
```

"source"

Remote source directory path. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

GET

Receive one or more files from the host

```
GET -REC -DEL -UNI|-APE "source" "destination"
```

-REC

Recursively retrieve nested subdirectories.

- Nested server directory structure retained locally.
- If used in conjunction with `-DEL`, the retrieved files, but not subdirectories, are deleted on the server.

-DEL

If the command is successful, delete the remote file.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

"*source*"

Remote source path. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Local destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).

- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

PUT

Send one or more files to the host.

```
PUT -DEL -APE "source" "destination" name=value,...
```

–DEL

If the `PUT` command is successful, delete local file(s).

-APE

Append copied file to existing destination file.

"*source*"

Local source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default outbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Remote destination path.

- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

MKDIR

Creates a new directory on the host.

```
QUOTE MKDIR "directory"
```

"*directory*"

The name of the new directory. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

MKDIRS

Creates a new directory on the host.

```
QUOTE MKDIRS "path"
```

"*path*"

The path of directories to create. Subdirectories are created using the / delimiter. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

PWD

Returns the name of the current working directory on the host.

```
QUOTE PWD
```

RENAME

Renames a file or directory on the host.

```
QUOTE RENAME "source" "destination"
```

"source"

The source file/directory to rename. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"destination"

- The destination file/directory name. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

RM

Removes a file on the host.

```
QUOTE RM "path"
```

"path"

The path of the file to remove. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

RMDIR

Removes a directory on the host.

```
QUOTE RMDIR "path"
```

"path"

The path of the directory to remove. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

SCRIPT

See SCRIPT command on page 951 for information about this command.

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

or

```
SET property=
```

- To clear a string property, use the `CLEAR` command

STAT

Returns the attributes of the file or directory on the host.

```
QUOTE STAT "path"
```

"*path*"

The path of the file/directory. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

SYMLINK

Creates a symbolic link on the host to a file or directory.

```
QUOTE SYMLINK "path" "link"
```

"*path*"

The target path of the file/directory for the symbolic link. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*link*"

The name for the new symbolic link. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"*path*"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

TOUCH

Sets the remote file access and modified times to the current time.

```
QUOTE TOUCH "path"
```

"*path*"

The path of the file/directory. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

OFTP Hosts

Odette FTP (OFTP) is a state-driven, point-to-point file transfer protocol.

- The initiator of the connection is the speaker, but speaker and listener roles can be reversed at anytime during the session.
- All four OFTP file formats are supported –Text, Unstructured, Fixed, and Variable.
- VersaLex OFTP can be used to perform EBCDIC-to-ASCII and ASCII-to-EBCDIC translations during the OFTP transfer.
- OFTP sessions can be over ISDN (Windows users only) or TCP/IP. ISDN equipment must support the Common ISDN API (CAPI) interface, version 2.0.
- Support for OFTP receipts (End-to-End Responses) is included.
- VersaLex is compatible with Odette FTP versions 1.2, 1.3, 1.4, and 2.0.
- VersaLex supports the OFTP2 specification, including secure transport over TLS, session authentication, encryption, compression, and document signing.
- VersaLex does not support forwarding OFTP messages – VersaLex must be an endpoint.
- VersaLex OFTP can receive files, both solicited via an OFTP receive action or unsolicited via the Local Listener Odette FTP service.
- VersaLex OFTP can send files only via an OFTP send action; files cannot be sent by the Local Listener Odette FTP service.

The following action commands are available on VersaLex:

	Command	Purpose	Possible underlying OFTP commands
Host commands	PUT	Send one or more files to the host	SFID (Start File Identification) DATA (Data exchange buffer) EFID (End of File Identification) CD (Change Direction) RTR (Ready to Receive) EERP (End to End Response) NERP (Negative End Response)

	Command	Purpose	Possible underlying OFTP commands
	GET	Receive one or more files and receipts from the host	CD (Change Direction) SFPA (Start File Positive Answer) SFNA (Start File Negative Answer) CDT (Set Credit) EFPA (End File Positive Answer) EFNA (End File Negative Answer) EERP (End to End Response) NERP (Negative End Response)
Local commands	SYSTEM	Execute a local system command	-
	WAIT	Pause	-
	SET	Sets a property	
	CLEAR	Clears a string property	
	LCOPY	Copy one or more local files	-
	LDELETE	Delete one or more local files	-
	LREPLACE	Replace bytes in one or more local files	-
	CHECK	Check for a transfer, file, or directory (VLTrader and Harmony only)	-
	SCRIPT	Execute a JavaScript File (VLTrader and Harmony only)	-

OFTP Configuration

Configure an Odette FTP (OFTP) host starting with the generic OFTP pre-configured host.

Only use this host if Cleo does not have a pre-configured host for the connecting trading partner. Visit https://www.cleo.com/trading-partner-network for a list of available pre-configured hosts.

As part of the configuration process, you must also configure your Local Listener to receive OFTP messages. See Configuring a Local Listener for OFTP on page 755 and Configuring OFTP Service on page 777 for detailed information about configuring your local host for OFTP.

First activate either a trading partner specific host or the generic OFTP pre-configured host.

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.
4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See OFTP Host on page 287.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See OFTP Mailbox on page 306.
   c) Click **Apply** to save your work.
6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See OFTP Action on page 313 .
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the product to prompt to you click **Apply** if you try to leave the page. However, in the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

OFTP Host

A host's parameters specify its location and how it is reached.

OFTP Host: General Tab

Use the **General** tab to configure three different types of connections: ISDN, TCP/IP, and Server Only

ISDN connection

ISDN equipment must already be installed and must support the Common ISDN API (CAPI) interface, version 2.0.

OFTP ISDN Addresses

A list of ISDN numbers the product will use to attempt to connect to the trading partner. The product will try each number until a successful conneciton is made. For each ISDN address, specify values for the following fields.

ISDN Phone Number

Your partner's ISDN phone number. If you are making an international call and are unsure of how to specify the number, www.countrycallingcodes.com can be used to determine your international dialing code and your trading partner's country code.

ISDN Subaddress

X.25 Network User Address

X.25 Network User Identification

Optional attributes that your trading partner might use.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For VLTrader and Harmony, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and/or Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send action are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive action are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

TCP/IP connection

Server Address

Either a fully qualified name (recommended) or an IP address.

Port

The OFTP port. You can specify either a specific port number or `-1` to indicate the default port (3305). Note that for secure connections using TLS, the default port is `6619`.

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` - Use either a direct connection to the internet or a VPN.

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For VLTrader and Harmony, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and/or Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send action are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive action are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Server-only connection

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For VLTrader and Harmony, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and/or Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send action are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive action are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

OFTP Host: OFTP Tab

Buffer Size

Can be between 128 and 99999 bytes.

Buffer Credits

This is the number of data exchange buffers that can be sent consecutively by the speaker without listener acknowledgment.

can be between 1 and 999.

Compress Content

Indicates whether the OFTP data compression algorithm should be invoked. This applies to buffer-level compression. OFTP2 utilizes better compression algorithms, which can be specified on the mailbox's V2 tab.

Allow Restart

Maximum Record Size

Indicates the maximum length of any single record when transferring a file. Maximum Record Size applies to the OFTP Text, Fixed, and Variable file formats; it does not apply to the OFTP Unstructured file format. In the case of the OFTP Fixed file format, Maximum Record Size specifies the fixed record length.

Incoming

Optional. Only specify an Incoming filter if you need to override the default inbox/filename or if EBCDIC translation or special end-of-record processing is required.

To add an **Incoming** destination or parameter, click **New**. See Adding an incoming destination or parameter on page 290

Adding an incoming destination or parameter

Add incoming destination information when you need to override the default inbox/filename or if EBCDIC translation or when special end-of-record processing is required.

1. On the **OFTP** tab in the **Incoming** section, click **New** to display the **OFTP Incoming Filter** dialog box.
2. Identify incoming files.

- If different incoming files are destined for different directories/filenames or require different parameters, uniquely identify the incoming file by specifying either a **Virtual Filename**, **Originator**, **Destination**, **Description** or **File Format**. Additionally, the Virtual Filename, Originator, Destination, and Description can contain wildcards or regular expressions if partial or global matching is needed on these fields. See Using wildcards and regular expressions on page 69. If the **File Identification** is left entirely blank, then the **File Destination** and/or **Parameters** specified below apply to all incoming files for which the originator and destination match the mailbox's trading partner ID and your ID respectively. If incoming originator and/or destination values differ from the mailbox login IDs, then the originator and/or destination values in the incoming filter must be set to match (either exactly or via wildcarding or regular expression) in order for the filter to be applied.
- If globally allowing incoming originator and/or destination values to differ from mailbox IDs in the Odette FTP Service, then the filter is optional. See Local Listener Odette FTP Service on page 777.
- Otherwise, if not globally allowing differing originator/destination, then an incoming filter with originator/destination filled in is required in order to accept the incoming file.

3. Specify a destination.
   - If the **Directory** is left blank, the host Inbox directory under the **OFTP Host: General Tab** is used. See OFTP Host on page 287. The host Inbox directory can be further subfoldered by enabling **Add Mailbox Alias Directory to Inbox** under the **OFTP Host: Advanced Tab**. See OFTP Host: Advanced Tab on page 292.
   - If the **Filename** is left blank, the Virtual Filename is used. If the filename already exists, a number is appended to the filename to ensure uniqueness. This field can also include any of the supported macros allowing for the inclusion of a date-time stamp in the name of an incoming file, for example, as shown in the diagram above. See Using macro variables on page 59 (Destination File context) for information about all applicable macros.
4. Optional. Specify destination parameters.
   - **Translate from EBCDIC** indicates that incoming characters should be translated from EBCDIC to ASCII. **EBCDIC Encoding** under the **OFTP Host: Advanced Tab** specifies the encoding character set. See OFTP Host on page 287.
   - **Trim Characters at End-Of-Record** applies to the OFTP Fixed file format only. The character or set of characters will be trimmed from the end of each incoming record, when present. Use a 0x prefix to specify hexadecimal character values.
   - **Insert End-Of-Record Delimiter** applies to the OFTP Fixed or Variable file format only. The character or set of characters should be inserted at the end of each incoming record. Use a 0x prefix to specify hexadecimal character values.

OFTP Host: V2 Tab

Starting with OFTP2, transport layer security (TLS) is an option for secure communications. When downgrading the OFTP version (see Advanced Tab below), non-secure communications are used regardless of any values you set on this page.

Partner Is ACE-Capable

Indicates whether the trading partner is capable of sending and receiving certificates through Automatic Certificate Exchange (ACE), and enables the **ACE** subtab in the **OFTP Mailbox: Security** tab. See OFTP Mailbox: Security Tab on page 308.

Possible values:

- `True` - Indicates your partner's OFTP2 product is capable of processing ACE messages, but no messages have been sent with the appropriate virtual filename
- `False` - Indicates your partner's product is not capable of processing ACE messages. However, when messages with the appropriate virtual filename (SFIDDSN) are received from a trading partner, this field is automatically changed to `True`.

- `False and Ignore Further Detection` - Indicates your partner's product is not capable of processing ACE messages and this field will not be updated automatically even if messages with the appropriate virtual filename (SFIDDSN) are received from a trading partner.

Default value: `False`

Outbound

The **Outbound** group settings are enabled for TCP/IP connections. See OFTP Host: General Tab on page 287.

TCP/IP

Select this option to use non-secure TCP/IP for outbound connections

Secure TCP/IP

Select this option to require TLS for outbound connections.

Check certificate server name

See OFTP Host: General Tab on page 287.

Inbound

The **Inbound** group is enabled for either Server Only or TCP/IP connections.

Secure TCP/IP only

Select this option to require your trading partner to use TLS for inbound file transfers. See OFTP Host: General Tab on page 287.

OFTP Host: Advanced Tab

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for OFTP include:

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Allow Duplicate SFIDs

Allows files with duplicate SFIDs to be accepted and simply logs a message if a duplicate is received.

Possible values: `On` or `Off`

Default value: `Off`

Always Change Direction After Sending

Indicates that a CD should always be sent after finished sending a set of files, giving the trading partner the opportunity to provide pending EERPs.

Possible values: `On` or `Off`

Default value: `Off`

Always Disconnect ISDN After End Of Session

Disable this setting if, for incoming ISDN calls, host should wait for trading partner to issue disconnect.

Possible values: `On` or `Off`

Default value: `On`

Always Include EERP Hash

Indicates whether to include a hash (EERPHSH) value in returned EERPs even if a signature (EERPSIG) is not included. The property defaults to off, and is included for backward compatibility.

Possible values: `On` or `Off`

Default value: `Off`

Application Layer Receipts

Note: This applies only to the Cleo Harmony and Cleo VLTrader applications.

Allows an EERP to not be returned until a received file has been processed by a backend application. Pending .eerp properties files can be stored in the configured inbox or the EERP storage folder or not at all.

For OFTP2 relationships, if processing should fail, the pending EERP can be changed to a NERP by adding a NERPREAS= property. (The SSIDLEV= property value for an OFTP2 relationship will be >= 5.) Valid application layer NERPREAS values are:

- 34 - File processing failed
- 35 - Not delivered to recipient
- 36 - Not acknowledged by recipient
- 99 - Unspecified reason

See section 5.3.14 in http://tools.ietf.org/html/rfc5024 for the full list of reason codes. An optional NERPREAST= property, which gives an additional description of the problem, can also be included.

The `PUT -RET` option must be used when the pending return receipt is being sent back.

Possible values:

- `Off`

- `Place pending EERP in inbox`
- `Place pending EERP in EERP storage subfolder`
- `On but do not generate a pending EERP` - This value can only be used when the API ILexiComIncoming interface or Cleo VLTrader or Cleo Harmony database payload is also being used; otherwise, the needed EERP property values will not be known. This setting also requires that the backend application generate a base64-encoded SHA-1 hash value for OFTP2 relationships. To know for sure what EERP properties are required, first use one of the **Place pending EERP…** settings and interrogate the generated .eerp file.

  If using the API **ILexiComIncoming** interface, the **EERP.pending** property in the `open()` method parameters object points to the location of the saved `.eerp` properties file or simply has a value of **True**. If using database payload, this property value is stored in the `VLIncomingProperties` table.

Default value: `Off`

Async EERP Resends

Specifies the number of attempts that will be made to resend an asynchronous transaction not completed within the specified timeout period. If you specify a value of `-1` (which is the default), the value specified for this parameter at the Local Listener level is used. If you change the value in this field from this default, that value overrides the one specified for the Local Listener.

Default value: `-1`

Async EERP Timeout (minutes)

The maximum time (in minutes) that the Local Listener will wait for an asynchronous response before either resending the transaction (if **AsyncResends** > 0) or logging an error. If you specify a value of `-1` (which is the default), the value specified for this parameter at the Local Listener level is used. If you change the value in this field from this default, that value overrides the one specified for the Local Listener.

Default value: `-1`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0` - `n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Delete Zero Length Files

Indicates whether files received that are zero-length (<= 5 bytes) should be deleted rather than processed.

Possible values: `On` or `Off`

Default value: `Off`

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Downgrade OFTP Version

Use may be necessary if the trading partner OFTP software does not on its own properly downgrade from Cleo Harmony, Cleo VLTrader, or Cleo LexiCom OFTP version 2.0.

Possible values:

- `1.2`, `1.3`, or `1.4` to force downgrade only when initiator of session
- `-1.2`, `-1.3`, or `-1.4` to force downgrade whether initiator of session or not

EBCDIC Encoding

When translating to and from EBCDIC, indicates the specific EBCDIC character encoding.

Possible values: `Cp037` - `Cp1149`

Default value: `Cp500` - EBCDIC International

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert

continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Repetitive Listener Failures

When "Email On Fail" is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, an email alert will be sent when the failure is resolved. Failure resolution email alerts will not be sent for general Listener failures since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Repetitive Listener Failures

When `Execute On Fail` is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, the `Execute On Fail` command will be executed again when the failure is resolved. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure. Executions of the "Execute On Fail" command for resolution of general Listener failures will not be done since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0` - `n`

Default value: `0`

Fixed Record Length From OFTP

Causes EOL characters to be inserted while receiving a file based on the SFIDLRECL value.

Note: For this property to be effective, Fixed Record EOL Characters must be specified, Fixed Record Incoming Insert EOL must be enabled, and a fixed SFIDFMT format with a positive SFIDLRECL value must be requested by the OFTP trading partner.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
```

SHA-384
SHA-512

Default value: System Default

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: On or Off

Default value: On

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: On or Off

Default value: On

PGP V3 Signature

Processing Disconnect Timeout (seconds)

When sending multiple large files within a put action, pre-processing (encryption, compression, signing) of files can take a while. This option will disconnect the connection if the processing time between files exceeds the timeout. The connection is re-established when file being processed is complete

Possible values: 0 - 99999

Default value: 20

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the PMode.ReceptionAwareness.Retry.Period setting.

Possible values: Any value greater than zero.

Default value: 60 seconds

Reuse SSL Sessions Across Actions

If selected, and if no forward proxy is being used for this host, SSL sessions from previous connections to the same destination (address and port number) may be resumed to avoid costly negotiation. If unselected, only SSL sessions used in the current action to the same destination may be resumed. When unselected, a new SSL session is created for the initial command port connection.

Possible values: On or Off

Default value: On

SSL Allow Legacy Renegotiation

When selected, legacy renegotiation is allowed. If this property is not selected, the extension described in RFC5746 is used for renegotiation and the server must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Possible values: On or Off

Default value: On

SSL Cipher

Indicates a specific cipher, or an ordered list of ciphers, to be used with the server for SSL key exchange, encryption, and hashing.

If not set (that is, left blank), the list of default ciphers (all standard ciphers, excluding anonymous and non-encrypting) is presented to the server and the server picks one. If a regular expression (enclosed in brackets) or a wildcard expression is specified, a list of implemented ciphers (all standard ciphers, including anonymous and non-encrypting) is presented to the server, based on the conditions of the pattern. For example, if a regular expression of `[.*ECDH.*]` is specified, then the list is a subset of all implemented ciphers that belong to the Elliptical-curve Diffie-Hellman group (for example, `ECDH` is in included in their string). In all cases, whenever a list is presented, it is always ordered by cryptographic strength, with the strongest listed first.

Based on the expression you type, the **List** button shows the resulting set of ciphers in the **SSL Cipher List** dialog box. Within this dialog box, you can view the list or select a specific cipher. If you select a cipher, then its value is displayed in this field.

Possible values:

Blank
a specific cipher picked from the SSL Cipher List dialog box
a regular/wildcard expression

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed. By default, this field is blank, designating that Cleo Harmony, Cleo VLTrader, or Cleo LexiCom will select the most recent version (currently TLS 1.3).

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed when selecting an SSL cipher. To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128`, or `256` (depending on the requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed. SSL 3.0 is the default value for compatibility with servers that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

Default value: `SSL 3.0`

SSL Reject Expired Certificates

When set, if an expired server certificate is received during SSL negotiations, the certificate will be rejected and the SSL handshake will be terminated.

Possible values: `On` or `Off`

Default value: `Off`

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Store Raw Sent Message

When this property is enabled, a copy of the outbound message is stored in the OFTP/sent directory.

Possible values: `On` or `Off`

Default value: `Off`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Uppercase Outbound DSN

Use an uppercase Dataset Name (DSN) identifier for outbound transfers.

By default, VersaLex sends the DSN using the same case as the filename. If the receiving system converts it to uppercase before returning it, enable this property to ensure consistent treatment of the DSN.

Validate String Characters For Inbound Message Fields

Validates that the incoming values for SSID and SFID string fields only contain characters from the following set:

- Numbers: 0-9
- Upper Case Letters: A-Z
- Special Characters: / - . & ( )

The fields validated are: SSIDCODE, SSIDPSWD, SSIDUSER, SFIDORIG, SFIDDEST, and SFIDDSN.

Possible values: `On` or `Off`

Default value: `Off`

Verify Calling Party ISDN Address

When receiving an incoming call for this ISDN host, indicates whether the call's source phone number must be one of the configured outgoing phone numbers.

Possible values: `On` or `Off`

Default value: `Off`

Wait For Disconnect After Sending End Of Session

Indicates that if the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application initiates end-of-session, it should wait for a disconnect request from the connected trading partner rather than immediately disconnecting.

Possible values: `On` or `Off`

Default value: `Off`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

`System Default`
`TripleDES`
`AES-128`
`AES-192`
`AES-256`

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`

`1`

`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

OFTP Mailbox

A mailbox's parameters allow access to the host system.

Create a new mailbox under the host.

OFTP Mailbox: OFTP Tab

User ID (SSIDCODE)

Password (SSIDPASWD)

Credentials that identify your trading partner.

Outgoing

Default Virtual Filename (SFIDDSN)

Optionally, enter an outgoing **Default Virtual Filename**. An action's `PUT` command destination, if specified, will override this value. If a `PUT` command does not specify a destination and a Default Virtual Filename is also not specified, then the source filename is used.

Originator

A user ID identifying the sender. Select the check box and provide a value to override the default. You can also use the `SET` command in an action to override these values.

Default value: your User ID.

Destination

A user ID identifying the receiver. Select the check box and provide a value to override the default. You can also use the `SET` command in an action to override these values.

Default value: your trading partner's User ID.

Send files when partner initiates connection

Enables the **Send Action** field.

Note: Available in the Cleo Harmony and Cleo VLTrader applications only.

Send Action

The action to be run whenever a trading partner-initiated connection makes the Cleo Harmony or Cleo VLTrader application the speaker. This allows the Cleo Harmony or Cleo VLTrader OFTP to act as the server in a traditional client-server model, where trading partner clients are both pushing and pulling files. If the **General** tab (see OFTP Host: General Tab on page 287) is set to **Server Only** and outgoing database payload is being used (see Transfers on page 895), any unsent database payload for the mailbox is also sent using the configured send action commands when the partner-initiated connection makes the Cleo Harmony or Cleo VLTrader application the speaker.

My Identification

User ID

Password

Override your default credentials.

Substation Mailbox

Enables a drop down menu where you select a substation mailbox. The mailbox uses the same user ID (SSIDCODE) and password (SSIDPASWD) as the managing mailbox, but has a different originator (SFIDORIG)/destination (SFIDDEST) pair (so these two override flags are automatically set). For OFTP2, a substation mailbox can have different signing, encryption, and/or EERP certificates.

OFTP Mailbox: V2 Tab

The following settings pertain only to OFTP2 sessions or later.

Session

Cipher Suite

Used for encryption, signing, and generating hash values.

Choose either `3DES-RSA-SHA` or `AES256-RSA-SHA`.

Secure Authentication

Indicates whether OFTP secure authentication should be used in exchanges with your trading partner (i.e., SSIDAUTH=Y/N). This setting controls what is placed in the SSIDAUTH field (Y/N) when sending and responding. It also is used by the responder to enforce compliance with RFC 5024, which states the secure authentication must be set to the same value for both the initiator and responder. The certificates used for session authentication are specified on the **Session** sub-tab of the **Mailbox Security** tab.

Signing Algorithm

The signing algorithm assigned to the mailbox for both inbound and outbound communications.

Choose from `SHA1`, `SHA256`, or `SHA512`.

Request

Encrypted Content

Select to encrypt outgoing files. Certificates used for encryption are specified on the **Mailbox Certificates** tab.

Signed Content

Select to sign outgoing files. Certificates used for signing are specified on the **Mailbox Certificates** tab.

Signed Receipt (EERPs/NERPs)

Select to sign outgoing EERPs and NERPs. Certificates used to sign EERPs/NERPs are specified on the **EERP** sub-tab of the **Mailbox Security** tab.

CMS Compression

Select to compress the file using CMS compression before sending. This is generally more effective than the legacy buffer compression used prior to OFTP2.

Inbound Message Security

Force Encryption

Select to only accept encrypted files from your trading partner that can be decrypted using a specified certificate.

Force Signed Content

Select to only accept signed files from your trading partner.

OFTP Mailbox: Certificates Tab

The following settings pertain only to OFTP2 sessions or later.

You must acquire your trading partner's signing and encryption certificates and provide yours to your trading partner. See Acquiring your trading partner's signing and encryption certificates on page 86 and Creating and providing your signing/encryption certificates on page 86.

Trading Partner's Certificates

Signing Certificate

The certificate used to verify a signature from an incoming file that is signed. This certificate is only required if **Secure Authentication** is selected in the **mailbox V2** tab.

Specify a value or click **Browse** to navigate to the file you want to select.

Encryption Certificate

The certificate used to encrypt outgoing files if **Encrypted Content** is selected on the mailbox **V2** tab.

Specify a value or click **Browse** to navigate to the file you want to select.

Use encryption certificate

Indicates that your trading partner uses the same certificate for signing and encryption, which is the general practice among most trading partners. When you select this check box, the **Signing Certificate** field is populated with the same certificate you selected in the **Encryption Certificate** field.

My Certificates

Override Local Listener Certificates

Enables fields where you specify signing and encryption certificates to use with this particular partner instead of the certificates you configured for the Local Listener. See Configuring certificates for Local Listener on page 758.

If you override the default certificates, you must also exchange the certificates you specify here with your partner.

Exchange Certificates

Displays the Certificate Exchange dialog box, which allows you to send your user and SSL certificates to your trading partner. See Exchanging certificates with your trading partner on page 672.

Signing Certificate Alias

The **Signing Certificate Alias** refers to the certificate used to sign outgoing files

Click **Browse** to navigate to and select a certificate. Enter the **Password** for your signing certificate's private key.

Encryption Certificate Alias

The **Encryption Certificate Alias** is for decrypting incoming encrypted files.

Click **Browse** to navigate to and select a certificate. Enter the **Password** for your encryption certificate.

Use signing certificate

Select this check box to use the same certificate for signing and decrypting your trading partner's messages. The **Encryption Certificate Alias** and **Password** are populated to match the **Signing Certificate Alias** and disabled.

OFTP Mailbox: Security Tab

The **Security** tab is divided into five sub-tabs: **TCP**, **Session**, **EERP**, **CLID**, and **ACE**.

Note: The settings in this tab pertain only to OFTP2 sessions or later.

OFTP Mailbox Security: TCP Tab

Use the **TCP** tab to specify an optional client certificate. This certificate is not applicable to ISDN connections and only needs to be specified for those servers that require a client certificate be specified.

Certificate Alias

The certificate to use for TLS over secure TCP/IP. This certificate is optional.

Specify a value or click **Browse** to navigate to the file you want to select.

Password

The password for the certificate you specify.

Exchange Certificates

Displays the Certificate Exchange dialog box, which allows you to send your user and SSL certificates to your trading partner. See Exchanging certificates with your trading partner on page 672.

OTFP Mailbox Security: Session Tab

Trading Partner's Certificates

Authentication Certificate

The certificate to use for authenticating your trading partner's OFTP2 session.

Specify a value or click **Browse** to navigate to the file you want to select.

If you do not specify a value, the incoming content's signature is compared to all valid certificates in the local certificate store.

Use encryption certificate

Indicates that your trading partner uses the same certificate for authentication as specified for encryption. When you select this check box, the **Authentication Certificate** field is populated with the same certificate you selected in the **Encryption Certificate** field on the **Certificates** tab (see OFTP Mailbox: Certificates Tab on page 308).

My Certificate

Authentication Certificate

The certificate to use for authenticating your OFTP2 session.

Specify a value or click **Browse** to navigate to the file you want to select.

Password

The password for the certificate you specify.

Use encryption certificate

Indicates that you want to use same certificate for authentication as specified for encryption. When you select this check box, the **Authentication Certificate** field is populated with the same certificate you selected in the **Encryption Certificate** field on the **Certificates** tab (see OFTP Mailbox: Certificates Tab on page 308).

Exchange Certificates

Displays the Certificate Exchange dialog box, which allows you to send your user and SSL certificates to your trading partner. See Exchanging certificates with your trading partner on page 672.

OFTP Mailbox Security: EERP Tab

The **EERP** tab is used to specify a certificate for EERP and NERP packet signing. The trading partner's signing certificate is used to validate an incoming signed EERP/NERP. Note that this certificate is optional. If it is not specified, the incoming signed EERP/NERP's signature is compared to all valid certificates in the local certificate store. **My Certificate** signing certificate is used to sign outgoing EERP/NERPs.

Trading Partner's Certificates

Signing Certificate

The certificate to use to validate an incoming signed EERP/NERPs.

Specify a value or click **Browse** to navigate to the file you want to select.

If you do not specify a value, the incoming EERP/NERP's signature is compared to all valid certificates in the local certificate store.

Use signing certificate

Indicates that your trading partner uses the same certificate as specified for signing in the **Signing Certificate** field on the **Certificates** tab (see OFTP Mailbox: Certificates Tab on page 308).

My Certificate

Signing Certificate

The certificate to use to sign outgoing EERP/NERPs.

Specify a value or click **Browse** to navigate to the file you want to select.

Password

The password for the certificate you specify.

Use encryption certificate

Indicates that you want to use the same certificate as specified for signing in the **Signing Certificate** field on the **Certificates** tab (see OFTP Mailbox: Certificates Tab on page 308).

Exchange Certificates

Displays the Certificate Exchange dialog box, which allows you to send your user and SSL certificates to your trading partner. See Exchanging certificates with your trading partner on page 672.

OFTP Mailbox Security: CLID Tab

Use the **CLID** tab to specify the Certificate Logical Identification Data (CLID) for your trading partner's certificates. If your trading partner provides their CLID, it allows for validation that the supplied certificates match, whether the certificate is provided automatically through ACE or imported and configured manually. Depending on which security features are used in the trading relationship and whether separate certificates are used for each feature, between one and five CLIDs are specified for signing, encryption, EERP, session, and TLS use.

A CLID consists of:

- The certificate’s subject and issuer in the form `EMAIL=xxx,CN=xxx,OU=xxx,O=xxx,L=xxx,ST=xxx,C=xxx` (the fields present and the order of the fields are dictated by the trading partner).
- Existence of `digitalSignature`, `keyEncipherment`, `clientAuth`, and/or `serverAuth` key usage flags.

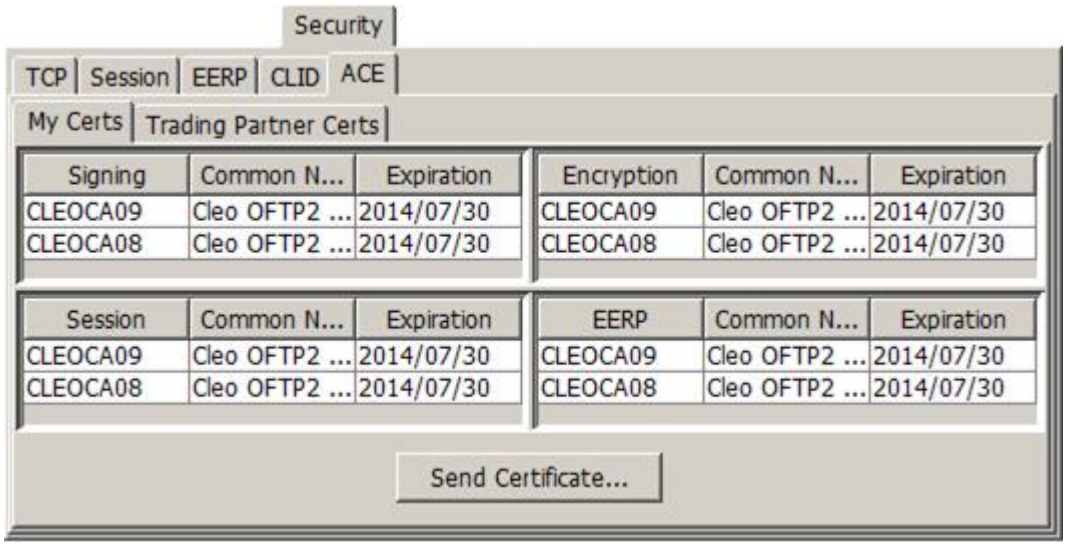
If a configured certificate does not match its CLID, the mailbox is not considered ready. A certificate received through ACE that does not have a matching CLID is rejected.

OFTP Mailbox Security: ACE Tab

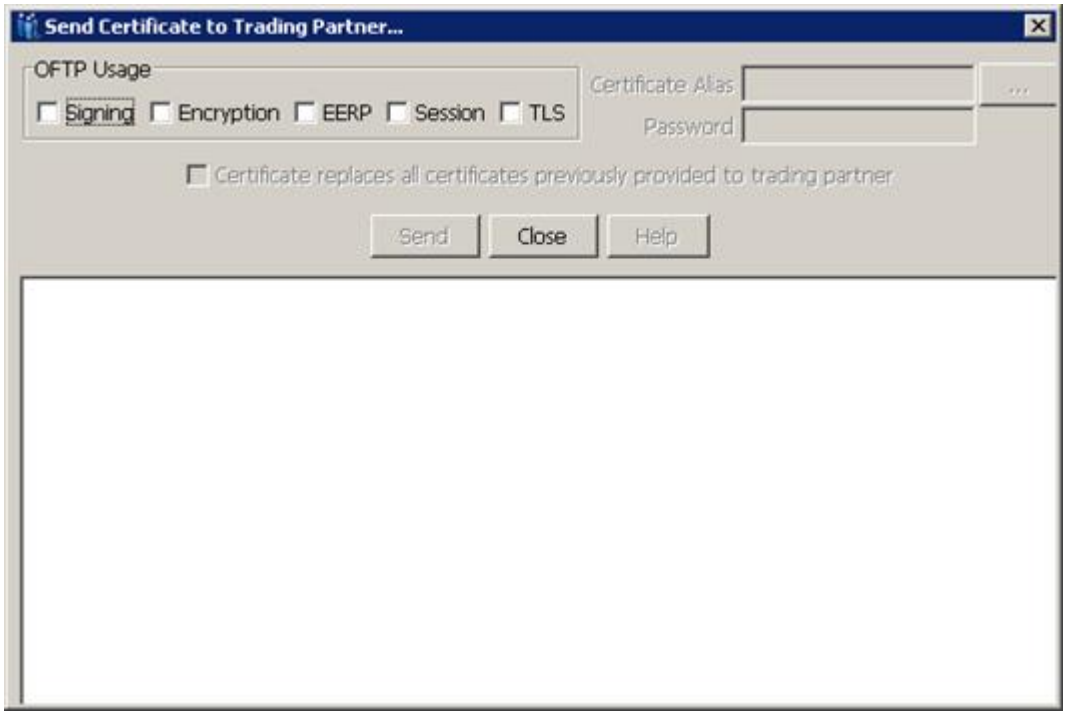
Use the **ACE** (Automatic Certificate Exchange) tab to trade certificates with your partner through the same OFTP channel used to trade payload. ACE exchanges do not themselves use channel security features, which allows for exchange of initial certificates as well as replacement certificates. ACE is an extension to the OFTP2 specification. Check with your trading partner that their OFTP2 product supports ACE before attempting to use this tab. Your trading partner can also require that you provide your Certificate Logical Identification Data (CLID) values before using ACE.

The ACE tab shows certificates for both sides of the relationship – **My Certs** and **Trading Partner Certs** – and four different uses – **Signing**, **Encryption**, **Session**, and **EERP**. The currently active certificate is always listed first, followed by the other certificates that have been delivered through ACE. These certificates can also be used as long as they are valid and will automatically replace any currently installed expired certificates designated for the same usage.

Although they can also be exchanged through ACE, TLS certificates are not shown because in general all trusted certificates are accepted for TLS rather than a specific list. If the mailbox is a substation mailbox, session certificates are also not shown because the session certificate is only applicable to the main station mailbox.



Click **Send Certificate** to display the **Send Certificate to Trading Partner** dialog box.



Select the intended usages and then fill in the user certificate alias and password. Click **Send** to initiate an ACE `ODETTE_CERTIFICATE_DELIVER` message. If your trading partner responds with an EERP, the certificate becomes the active certificate for the selected usages and what was the active certificate is dropped down in the list.

- For signing and EERP, the active certificate is in effect the only certificate used (to sign).
- For encryption and session, the active certificate is the first certificate used (to decrypt), but if decryption fails, the other valid certificates in the list are tried one-by-one.
- Only valid and non-expired certificates can be exchanged through ACE.
- Whenever an installed local or partner certificate is expired and there is a valid secondary certificate available that had previously been exchanged through ACE, the next secondary certificate for the specified usage(s) will be rolled over as the installed certificate before an OFTP message is either sent or received. In synced environments, certificates will be updated only on the node where the rollover has occurred to avoid syncing collisions. Each node will subsequently be updated during its own OFTP data exchange.

If **Certificate replaces all certificates previously provided to trading partner** is selected first, then clicking **Send** initiates an ACE `ODETTE_CERTIFICATE_REPLACE` message. When a new user certificate is sent through ACE in either a replacement or rollover scenario, attributes of the currently installed certificate are now included in the SFIDDESC field of the SFID message. These attributes may then be used by the receiver to implicitly trust the new certificate based on the trust of the currently installed certificate. If your trading partner responds with an EERP, the certificate becomes the active certificate for the selected usages, and all of the user certificates previously listed are automatically cleared. After an OFTP Trading Partner certificate is replaced, the replaced certificate is archived (in the certs/archive directory) and removed from the trusted store as long as it is no longer in-use in any other trading relationship.

To manually remove a certificate in the list (other than the active certificate), right-click on the certificate and select **Remove**.

The following dialog is shown when **Request Certificate(s)** is clicked:

Click **Request** to initiate an ACE , and if acceptable, queue your trading partner to send one or more ACE `ODETTE_CERTIFICATE_DELIVER` messages back. An `ODETTE_CERTIFICATE_DELIVER` message can also be received unsolicited. Based on your configured CLID, the usage for the certificate within the DELIVER is determined, the certificate becomes the active certificate for its usages, and what was the active certificate is dropped down in the list.

- For signing and EERP, the active certificate is the first certificate used (to verify a signature), but if verification fails, the other valid certificates in the list are tried one-by-one.
- For encryption and session, the active certificate is in effect the only certificate used (to encrypt).
- Only valid and non-expired certificates can be exchanged through ACE. Received ACE messages with expired certificates will be rejected.
- Whenever an installed local or partner certificate is expired and there is a valid secondary certificate available that had previously been exchanged through ACE, the next secondary certificate for the specified usage(s) will be rolled over as the installed certificate before an OFTP message is either sent or received. In synced environments, certificates will be updated only on the node where the rollover has occurred to avoid syncing collisions. Each node will subsequently be updated during its own OFTP data exchange.

To manually remove a certificate in the list (other than the active certificate), right-click on the certificate and select **Remove**.

OFTP Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information regarding payload file packaging.

OFTP Action

An action's parameters capture a repeatable transaction for your mailbox on the host system. Create a new action under the mailbox.

OFTP Action: Action Tab

Use the **Action** tab to configure commands within an action.

See Composing an action on page 89. Also see OFTP Command Reference on page 314.

OFTP Command Reference

Information about commands available to OFTP hosts and mailboxes

PUT

Send one or more files to the host

```
PUT –TEX|-UNS|-FIX|-VAR|-RET –DEL "source" "destination"
 RecordDelimiter=0x.. StripDelimiter=True|False PadCharacter=0x..
 TranslateToEBCDIC=True|False FileDescription=...
```

–TEX

Transfer file in OFTP text format:

There are several other parameters available for this format:

- `TranslateToEBCDIC=` - Optional
- `FileDescription=` - Optional

See Additional PUT parameters on page 315 for more information.

-UNS

Transfer file in OFTP unstructured format:

There are several other parameters available for this format:

- `TranslateToEBCDIC=` - Optional
- `FileDescription=` - Optional

See Additional PUT parameters on page 315 for more information.

-FIX

Transfer file in OFTP fixed format.

There are several other parameters available for this format:

- `RecordDelimiter=` - Optional
- `StripDelimiter=` - Optional
- `PadCharacter=` - Optional
- `TranslateToEBCDIC=` - Optional
- `FileDescription=` - Optional

See Additional PUT parameters on page 315 for more information.

-VAR

Transfer file in OFTP variable format.

There are several other parameters available for this format:

- `RecordDelimiter=` - Required
- `StripDelimiter=` - Optional
- `TranslateToEBCDIC=` - Optional
- `FileDescription=` - Optional

See Additional PUT parameters on page 315 for more information.

-RET

Transfer return receipt. See OFTP Configuration on page 286.

-DEL

If `PUT` is successful, delete the local file.

"*source*"

Source path

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default outbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

The file's Virtual Filename (SFIDDSN)

- Use of macro variables is supported. See Using macro variables on page 59 (Destination File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").
- If no destination is specified, the command uses Default Virtual Filename under the **OFTP Mailbox > OFTP Tab**. If the Default Virtual Filename also not specified, the command uses the source filename.

Additional PUT parameters

RecordDelimiter=

The character or set of characters that logically separate *records*. Use a `0x` prefix to specify hexadecimal character values.

StripDelimiter=

When a `RecordDelimiter` is specified, indicates whether the delimiters should be excluded from the file transfer. Defaults to False.

PadCharacter=

The character or set of characters to be used when necessary to pad a record to the needed fixed length. Use a 0x prefix to specify hexadecimal character values.

TranslateToEBCDIC=

Indicates that outgoing characters should be translated from ASCII to EBCDIC. The "EBCDIC Encoding" property under the **OFTP Host > Advanced Tab** specifies the encoding character set. Defaults to False. See OFTP Host on page 287

FileDescription=

Specify an optional description. This is set to the SFIDDESC field when sending a file. This field only pertains to OFTP2.

Note: During OFTP2 transfers where the file is encrypted, compressed, or signed, the file type is forced to unstructured (-UNS) regardless of the settings specified.

GET

Receive one or more files or receipts from the host

```
GET
```

The GET command has no options for two reasons:

- Whether files or receipts (EERP) are received cannot be controlled
- In OFTP, files and receipts can be received either solicited or unsolicited

You can use the **Incoming** options under **OFTP Host > OFTP Tab** can be used to configure the special destination and parameters for all received files, both solicited and unsolicited. See OFTP Host on page 287

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"path"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

You can also use the `SET` command to override any property in the **OFTP Host > Advanced Tab** (see OFTP Host on page 287) at action runtime. There are also a number of OFTP parameters in the **OFTP Host > OFTP Tab** and **OFTP Mailbox > OFTP Tab** that you can override at runtime, including:

- mailbox.SSIDSDEB
- mailbox.SSIDCRED
- mailbox.SSIDCMPR
- mailbox.SFIDLRECL

- mailbox.SFIDDSN
- mailbox.SFIDORIG
- mailbox.SFIDDEST

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).

- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

CHECK

See CHECK Command for information about this command.

SCRIPT

See SCRIPT command on page 951 for information about this command.

Comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

MQ Hosts

IBM MQSeries (also known as WebSphere MQ or IBM MQ) is a widely used means of guaranteed message delivery.

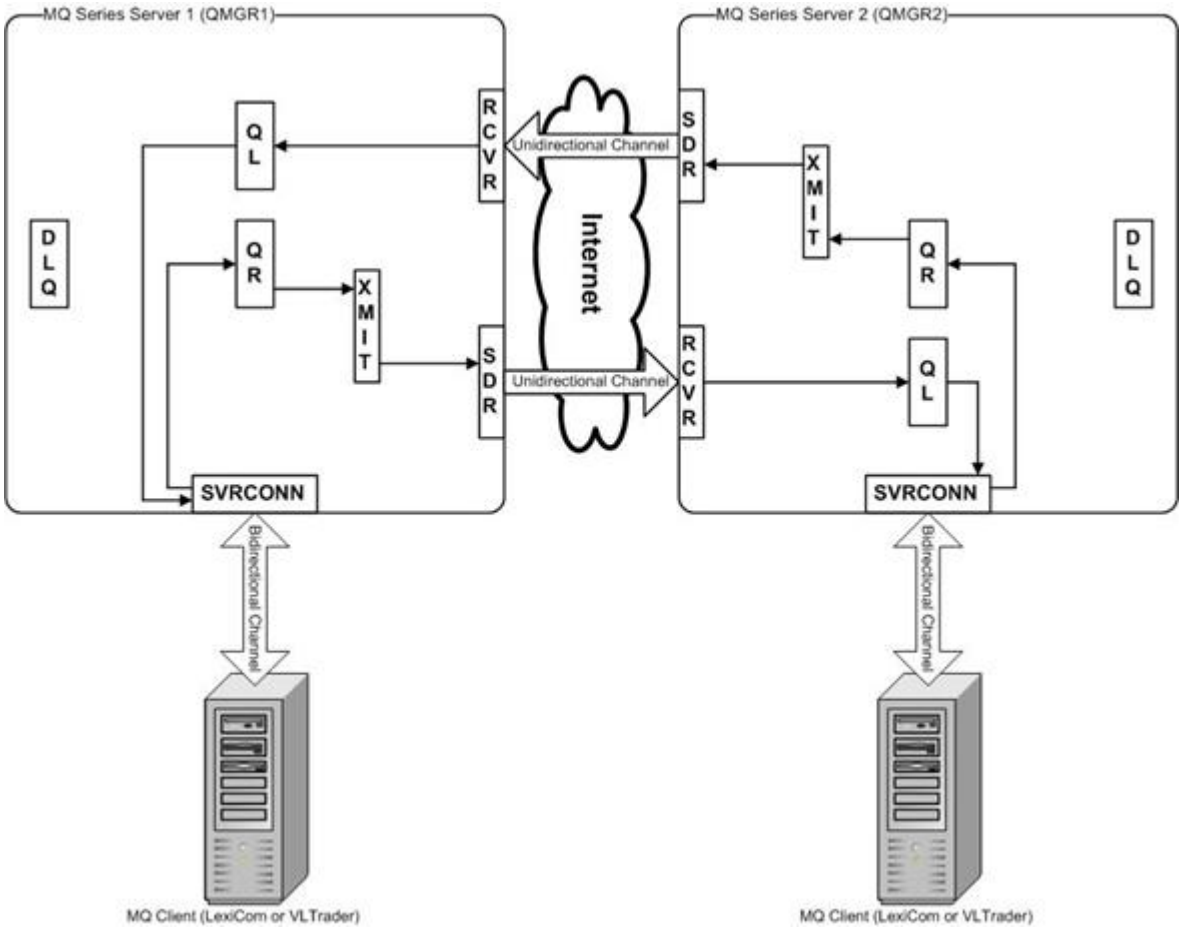
It uses Queue Managers containing local (and sometimes remote) message queues to send and receive message data. MQSeries uses a store-and-forward mechanism to transport the message data. If the remote Queue Manager is not available, the local Queue Manager retains the message until the remote Queue Manager is ready to receive it. Messages that cannot be delivered can eventually be stored in a dead letter queue.

Messages are put on queues and are generally retrieved on a First-In-First-Out (FIFO) basis. MQSeries also allows the use of a message-priority field (per-message) to put higher-priority messages at the front of the queue. User authentication and message security can also be applied to the sending and receiving channels.

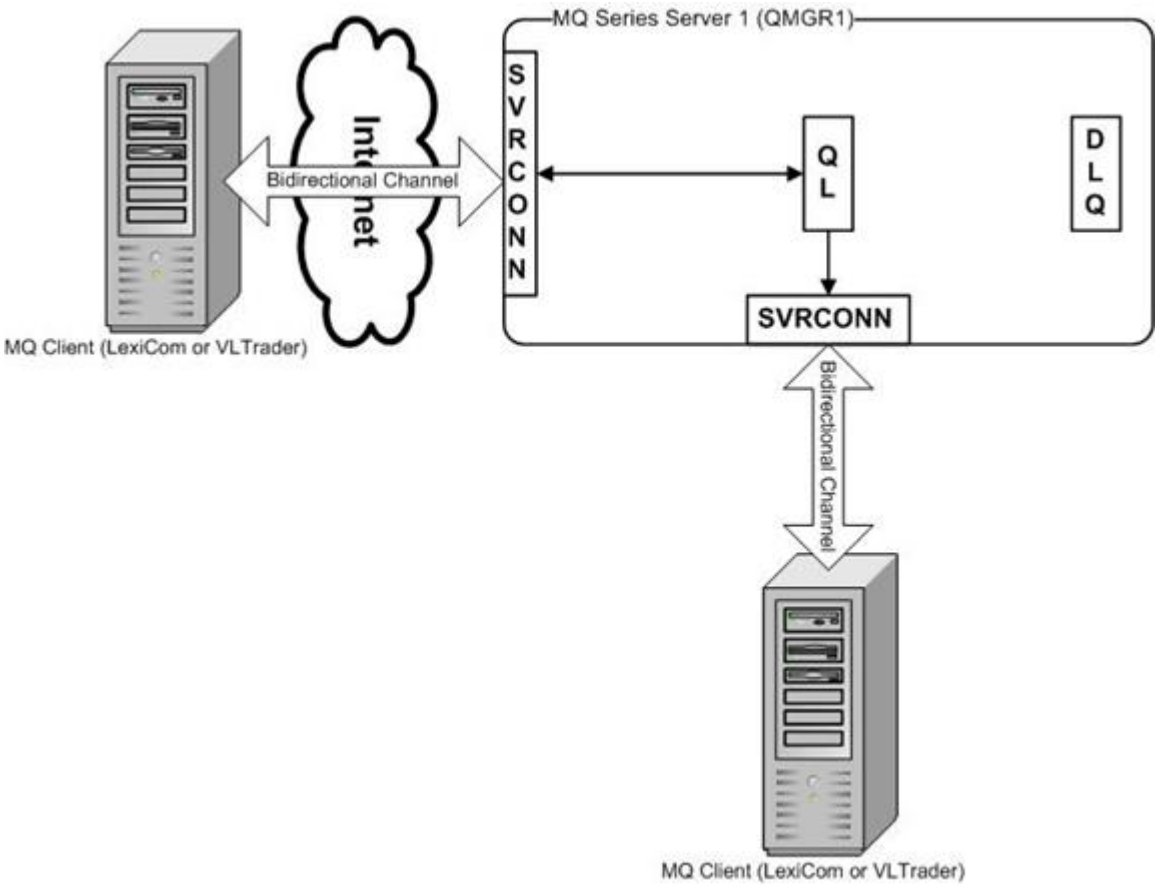
IBM MQSeries includes a Java client API that allows an application (such as the Cleo Harmony application) to programamtically connect to a Queue Manager using server-connection channels to PUT, GET and LIST messages on queues from either a local or remote Queue Manager. These Java client API files are included as part of the Cleo Harmony installation.

There are two ways to access a partner's queues:

1. **Queue Manager to Queue Manager**: Messages are written to a remote queue (QR) on the user's local Queue Manager (QMGR1) that maps to a local queue (QL) on the remote Queue Manager (QMGR2). Messages are transported over the internet via uni-directional sender (SDR) and receiver (RCVR) channels. If required, MQSeries automatically converts the data to the target queue manager's understood data format. If the remote queue manager (QMGR2) is unavailable, the sender channel is not running, or the message cannot be delivered for any other reason, the message is retained in either the transmission queue (XMIT) or the dead-letter queue (DLQ) on the local Queue Manager (QMGR1). The user must implement additional monitoring to periodically check the depth of these queues and take the appropriate action.



2. **Direct Connection to the Queue Manager**: Messages are sent to and received from local queues (QL) on a Queue Manager (QMGR1) using bi-directional server-connection channels (SVRCONN). User authentication and message encryption security (SSL) can be applied to server-connection channels, if desired. This access method does not take advantage of the store-and-forward mechanism; however, if the Queue Manager is not available, an error will occur in the client and the message transport will be re-tried at a later time. Additionally, if required, the Java MQ client API allows for automatic conversion of the data to the target Queue Manager's understood data format.



Either of these methods can be used with VersaLex. Using this section, decide which method fits your requirements and configure your Queue Manager(s) and MQ Host appropriately.

MQ Configuration

Configure an MQ host starting with the generic OFTP pre-configured host.

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.

4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See MQ Host on page 324.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See MQ Mailbox on page 335.

> **Note:** By default, the MQ host mailbox is configured to use the same Security settings for **Sender** and **Receiver**. To use different settings for **Receiver**, clear the **Use Same Channel for Sender and Receiver** check box on the **Mailbox > MQSeries** tab, and clear the **Use Sender's Security Definition** check box on the **Mailbox > Security > Receiver** tab. This enables the fields on the **Mailbox > Security > Receiver**. See MQ Mailbox: MQSeries Tab on page 335 and MQ Mailbox: Security Tab on page 336.

c) Click **Apply** to save your work.

6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See MQ Action on page 337 .
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Configure the host tree, starting with the host, then a mailbox, and finally an action. See MQ Host on page 324, MQ Mailbox on page 335, and MQ Action on page 337.

MQ Host

A host's parameters specify its location and how it is reached.

MQ Host: General Tab

Server Address

Either a fully qualified name (recommended) or an IP address.

This is the address of the server where the MQSeries Queue Manager is installed and running.

Port

The port on the server where your trading partner will receive your messages. If no port number is included in your trading partner's URL, default values are assumed.

Possible values: Either a specific port number or `-1` to indicate the default port for the MQSeries Queue Manager (`1414`)

Default value: `1414`

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` - Use either a direct connection to the internet or a VPN.

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For the Cleo VLTrader and Cleo Harmony applications, see URI File System interface overview on page 955 for

information about you can use a Cleo-provided or custom URI for the Inbox and Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Note: If the host is has an external association, the default directories might be managed outside of the Cleo Harmony application and not shown here.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

MQ Host: MQSeries Tab

Queue Manager

The name of the MQSeries Queue Manager to which you are connecting. This name is case-sensitive and must be entered exactly as it was defined.

MQ Host: Advanced Tab

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for MQSeries include:

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0` - `n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Delete Zero Length Files

Indicates whether files received that are zero-length (<= 5 bytes) should be deleted rather than processed.

Possible values: `On` or `Off`

Default value: `Off`

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0` - `n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

MQ Client CCSID

The CCSID (Coded Character Set Identifier) defines the character set of the data written to and read from the MQSeries queues. When the default CCSID of the environment differs from the Queue Manager's native CCSID (for example, when sending from the iSeries IFS where the native CCSID is `37`), this setting can be used to convert to and from the desired character formats.

Errors or unexpected results could occur if this value is not set correctly.

Possible values: Any valid CCSID that allows for the correct character encoding of the sent or received message.

The Queue Manager must have a valid conversion table installed to allow encoding to the CCSID.

When set to either `0` or `-1`, the native CCSID of the local environment is used.

Default value: `819`

Only Retrieve Next Available Message

Indicates a `GET *` should only retrieve the next available message from the queue.

Possible values: `On` or `Off`

Default value: `Off`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
```

```
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512
```

Default value: `System Default`

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: `On` or `Off`

Default value: `On`

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: `On` or `Off`

Default value: `On`

PGP V3 Signature

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

Save MQ Trace Info

Specifies that an MQ Series Trace file (`logs\MQTrace.dbg`) should be generated with each connection to the Queue Manager. This can be useful for debugging purposes.

Possible values: `On` or `Off`

Default value: `Off`

Set Identity Context on Put

Specifies whether the Identity Context should be set for an MQ PUT command. This setting is required for the file name associated with the message to be set in the message's **Application identity data** field.

Possible values: `On` or `Off`

Default value: `On`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-CHECK commands: When Terminate On Fail is on, if a command fails, Email On Fail and Execute On Fail, if set, are processed, and then the action stops. When Terminate On Fail is off, if a command fails, Email On Fail and Execute On Fail, if set, are processed, and the action continues.

Regarding CHECK commands: Terminate On Fail is only honored if the ConditionsMet parameter is set and the result of the CHECK is classified as Error. The CHECK command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: On or Off

Default value: On

Queue Access On Get

Indicates whether multiple actions are allowed to access entries on the queue at the same time or should be blocked from simultaneously accessing the queue.

Possible values: Exclusive or Shared

Default value: Exclusive

Unzip Use Path

Indicates whether or not zip entry paths should be used for LCOPY -UNZIP operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: On or Off

Default value: On

Wait For Execute On

Indicates whether execution should wait for processing to complete within an Execute On Fail, Execute On Successful Copy, Execute On Successful Receive, or Execute On Successful Send command. Note that this option does not apply to native AS400 execution.

Possible values: On or Off

Default value: On

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If System Default is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
AES-128
AES-192
AES-256
```

Default value: System Default

Zip Comment

Specifies the comment to be added to the zip archive file in LCOPY -ZIP operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for LCOPY -ZIP operations. If System Default is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

MQ Mailbox

A mailbox's parameters allow you access to the host system. Create a new mailbox under the host.

1. Right-click the MQ host in the active tree pane.
2. Select **New Mailbox** to create a new lower branch.
3. Optionally, type a new alias in the content pane panel.
4. Click **Apply**.

MQ Mailbox: MQSeries Tab

Use Same Channel for Sender and Receiver

Select the check box to indicate the same Server-Connection channel is being used for sending and receiving messages from queues on the Queue Manager.

Force Upper Case on Queues and Channels

Select the check box to automatically convert all queue and channel names to upper case. Queue and channel names are case-sensitive and must be entered exactly as they have been defined in the Queue Manager.

Sender

Queue

The name of the queue from which you will send messages.

Channel

The name of the channel used to connect to the Queue Manager. This channel must be a *Server-Connection* channel in order to successfully connect to the Queue Manager from the Cleo Harmony application. If you selected **Use Same Channel for Sender and Receiver**, the same channel name is used for both sending and receiving.

User Name

Password

Optional. These values can be provided to you by the administrator of MQSeries Queue Manager.

Receiver

Queue

The name of the queue where you will receive messages.

Channel

The name of the channel used to connect to the Queue Manager. This channel must be a *Server-Connection* channel in order to successfully connect to the Queue Manager from the Cleo Harmony application. If you selected **Use Same Channel for Sender and Receiver**, the same channel name is used for both sending and receiving.

Message Priority

The message priority to be applied when you `PUT` a message on a queue. By default, the message priority is `0` and all messages are written to the queue in a first in first out (FIFO) order. However, messages with a higher priority are placed ahead of lower priority messages in the queue.

Populate ReplyToQ Field

Select the check box to set the specified queue name (either the **Receiver Queue** name or any other queue name) in the **ReplyToQ** field of the message descriptor of messages sent by the Cleo Harmony application. Since the application only sends datagram messages, typically this field is used to notify your trading partner of your configured **Receiver Queue** and is not intended for receipt of report messages. The application does not monitor this field and will not issue report or reply messages.

Note: The Cleo Harmony application always leaves the **ReplyToQMgr** field in the message descriptor blank. When this occurs the queue manager will set the contents of the following fields in the message descriptor on the queue:

- **ReplyToQ** - If the queue is a local definition of a remote queue, the **ReplyToQ** field is set to the name of the remote queue; otherwise this field is not changed.
- **ReplyToQMgr** - If value in the **ReplyToQ** field is a local definition of a remote queue, the **ReplyToQMgr** field is set to the name of the queue manager that owns the remote queue; otherwise the **ReplyToQMgr** field is set to the name of the queue manager to which the Cleo Harmony application is connected.

MQ Mailbox: Security Tab

The Security tab contains two sub tabs: **Sender** and **Receiver**. While both tabs contain the same fields, the fields on the **Receiver** tab are not editable by default.

Use Sender's Security Definition

Note: This field is available only on the **Receiver** tab and is activated only when you clear the **Use Same Channel for Sender and Receiver** check box on the mailbox **MQSeries** panel .

Select the **Use Sender's Security Definition** check box to use the same settings as on the **Sender** tab. Clear the check box to enable the rest of the fields on the **Security > Receiver** tab, where you can specify security setting for the Receiver.

Enable Secure Connection

Enables the rest of the fields in the tab. Select the check box if the server-connection channel is using SSL message encryption. If you are provided with a server certificate for the MQSeries Queue Manager, copy it to the certs subdirectory of the Cleo Harmony product. If this is not provided, a dialog box is displayed when you connect to the Queue Manager to allow you to trust the server certificate provided by the Queue Manager per connection session or permanently.

MQ SSL Cipher Spec

Select the spec provided to you by the MQSeries Queue Manager administrator. The list of available cipher specs supported by the Cleo Harmony application requires that the Queue Manager be running with the latest IBM PTF. It is not guaranteed, however, that all cipher specs in the list will be supported by the version of the Queue Manager to which you are connecting.

Authenticate Client

Enables the **Client Certificate** fields. Select the check box if the server-connection channel used to transport your messages requires client authentication. In this case, you must also provide a client certificate that will be installed in the Queue Manager's key repository to authenticate your connection.

Certificate Alias

Password

Alias and password for the certificate you created for this server-connection channel. See Certificate management on page 661 for more information on creating a client certificate.

MQ Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information about payload file packaging.

MQ Action

An action's parameters capture a repeatable transaction for your mailbox on the host system. Create a new action under the mailbox.

MQ Action: Action Tab

Use the **Action** tab to configure commands within an action.

See Composing an action on page 89. Also see MQ Command Reference on page 337.

MQ Command Reference

CHECK

See CHECK Command for information about this command.

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

Comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

DIR

Get a directory listing of available files from the host.

```
DIR "source" "destination"
```

"*source*"

Identifies the queue from which the messages are to be listed.

- This queue must be "GET-enabled" on the target Queue Manager and can only be used to list the contents of queues that are defined as "Local" queues.
- "Remote" queues cannot be used to obtain directory listings.
- If not specified, the default receiver queue applies but may be overridden with the SET command. (Use a * as a place-holder when specifying the default queue and a "destination".)

"*destination*"

Optional path where the listing of the queue is to be written.

- If no destination is specified, the listing is logged rather than saved to a file.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

GET

Receive one or more files from the host.

```
GET -DEL –UNI|-APE "source" "destination"
```

-DEL

If the command is successful, delete host files. If the DELETE command is not supported on the server, the argument is not applicable and cannot be used. See HTTP Configuration on page 121

-UNI

Ensure the copied filename is unique.

-APE

If local filename exists, append copied file to existing file.

"*source*"

Remote source path

- You can specify `*` to receive all the messages currently on the queue.
- You can specify a particular message ID (in hexadecimal form), displayed in the directory listing (with a msgId= tag) to receive a specific message from the queue.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

Note: The `source` always applies to the receiver queue if not overridden by the `SET` command.

"*destination*"

Local destination path.

- Path can be to a filename (unless the `-DIR` option is used) or to a directory.
- If you specify no path or a relative path, the command uses the default inbox.

- You can use macro variables. See Using macro variables on page 59 (Destination File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use * and ?, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

PUT

Send one or more files to the host.

```
PUT -DEL "source"
```

DEL

If `PUT` is successful, delete local file.

`-DEL` option is not applicable to queue-based `PUT` commands. If specified for a queue-based `PUT`, it is ignored.

source

Source path

- `source` parameter is not applicable to queue-based `PUT` commands. If specified for a queue-based `PUT`, it is ignored.
- Path can be to a filename or to a directory.
- You can use * and ?, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default outbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

Note:

The default sender queue is the destination but can be overridden with a `SET` command.

All messages are `PUT` on queues with a persistence of Persistent even if the sender queue was created as Not Persistent.

SCRIPT

See SCRIPT command on page 951 for information about this command.

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

SMTP and SMTP/s Hosts

The generic SMTP and SMTP/s hosts allow you to specify a client email interface to an SMTP server.

Not all SMTP servers will support or require the full set of host options allowed by VersaLex. The following action commands are available on VersaLex:

	Command	Purpose	Underlying SMTP method
Host commands	PUT	Send one or more files to the server	MAIL FROM: RCPT TO: DATA or BDAT
	QUOTE *command*	Send a raw command to the server	command
Local commands	SYSTEM	Execute a local system command	-
	WAIT	Pause	-
	SET	Set a property	
	CLEAR	Clear a string property	
	LCOPY	Copy one or more local files	-
	LDELETE	Delete one or more local files	-
	LREPLACE	Replace bytes in one or more local files	-
	CHECK	Check for a transfer, file, or directory (VLTrader and Harmony only)	-
	SCRIPT	Execute a JavaScript File (VLTrader and Harmony only)	-

SMTP Configuration

The generic SMTP host provides an interface over non-secure SMTP. If interfacing to a server that requires use of the Secure Socket Layer (SSL) SMTP, then the generic SMTP/s host must be used.

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

Note: The original pre-configured host remains in the pre-configured tree.

4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See SMTP Host on page 344.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See SMTP Mailbox on page 357.
   c) Click **Apply** to save your work.
6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See SMTP Action on page 360 .
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the product to prompt to you click **Apply** if you try to leave the page. However, in the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

SMTP Host

A host's parameters specify its location and how it is reached.

SMTP Host: General Tab

Server Address

The address of the server where the SMTP server is running.

Specify either a fully qualified name (recommended) or an IP address. If you specify an IP address, it must be enclosed in square brackets.

You can specify a special open-ended SMTP host by using an asterisk (*) in the **Server Address** field. One open-ended SMTP host can be used to send to different SMTP servers at run-time; see SMTP Mailbox: SMTP Tab on page 357. Open-ended SMTP hosts are limited to sending; they cannot request DSNs to be returned and they cannot receive incoming payload emails.

Port

The SMTP command port.

Possible values: Either a specific port number or `-1` to indicate the default port.

Default value: SMTP - `25` or SMTP/s - **465**.

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` - Use either a direct connection to the internet or a VPN.

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Specifying default host directories on page 700 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For the Cleo VLTrader and Cleo Harmony applications, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Note: If the host is has an external association, the default directories might be managed outside of the Cleo Harmony application and not shown here.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

SMTP Host: SMTP Tab

Store raw sent

Save the contents of the raw MIME payload messages sent to the remote host. The files are stored in the `SMTP \sent` directory under the Cleo Harmony root path. These files can be useful in diagnosing problems, but should be disabled if disk space needs to be conserved.

Security Modes

If the SMTP server requires use of the Secure Socket Layer (SSL), select one of two different **Security Modes**.

Possible values:

- `None` - Indicates non-secure transfers; commands and data are clear-text.
- `SSL Implicit` - For servers that support only SSL connections.

- `SSL STARTTLS` - For servers that support SSL through the use of either the `STARTTLS` command.

Acceptable additional incoming sender subdomains

Subdomains from within the **Server Address** on the **General** tab from which incoming messages are acceptable. A subdomain can be wildcarded with asterisks (*) or question marks (?) (for example `*.cleo.com`) and multiple subdomains can be separated by semi-colons (;) or commas (,) or entered on separate lines (for example, `mailsvr01.lan.cleo.com;mailsvr02.lan.cleo.com`). Cleo VLTrader and Cleo Harmony applications only.

SMTP Host: Advanced Tab

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for SMTP or SMTP/s include:

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Always Send Multipart Messages

Indicates to always send a multipart MIME message to the trading partner, even when there is only one attachment in the message.

Possible values: `On` or `Off`

Default value: `On`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0` - `n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Convert Incoming Inline Charset

When there is an inline part in an incoming SMTP multipart message, this property indicates whether the original character set should be retained or converted during the transfer.

Data Termination Timeout

The amount of time allowed for reply from server after sending `DATA` or last `BDAT` command.

Possible values: `-1` - `600` seconds

`-1` indicates use of **Connection Timeout** value

`0` indicates no timeout

Default value: `-1`

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *`n`* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0 - n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

`Incoming`
`Outgoing`
`Both`

Ignore Exception After Quit

Indicates to ignore any I/O errors that occur when attempting to read the SMTP server response after issuing a `QUIT` command.

Possible values: `On` or `Off`

Default value: `Off`

Include Date In Duplicate Message ID Check

Some email clients do not generate a unique Message-ID in the email content. Including the message Date in the duplicate checker helps to avoid accidentally discarding messages that are not duplicates. **(Cleo Harmony and Cleo VLTrader applications only)**

Possible values: `On` or `Off`

Default value: `On`

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

Keep All Mutlipart Alternative Parts

When there is a multipart/alternative part in an incoming SMTP multipart message, this property indicates whether all of the parts should be kept rather than only attachments or text/plain content. Specify `True` to keep all parts.

Possible values: `True` or `False`

Default value: `False`

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0` - `n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0` - `n`

Default value: `0`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512
```

Default value: `System Default`

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: `On` or `Off`

Default value: `On`

PGP V3 Signature

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

SSL Allow Legacy Renegotiation

When selected, legacy renegotiation is allowed. If this property is not selected, the extension described in RFC5746 is used for renegotiation and the server must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Possible values: `On` or `Off`

Default value: `On`

SSL Cipher

Indicates a specific cipher, or an ordered list of ciphers, to be used with the server for SSL key exchange, encryption, and hashing.

If not set (that is, left blank), the list of default ciphers (all standard ciphers, excluding anonymous and non-encrypting) is presented to the server and the server picks one. If a regular expression (enclosed in brackets) or a wildcard expression is specified, a list of implemented ciphers (all standard ciphers, including anonymous and non-encrypting) is presented to the server, based on the conditions of the pattern. For example, if a regular expression of `[.*ECDH.*]` is specified, then the list is a subset of all implemented ciphers that belong to the Elliptical-curve Diffie-Hellman group (for example, `ECDH` is in included in their string). In all cases, whenever a list is presented, it is always ordered by cryptographic strength, with the strongest listed first.

Based on the expression you type, the **List** button shows the resulting set of ciphers in the **SSL Cipher List** dialog box. Within this dialog box, you can view the list or select a specific cipher. If you select a cipher, then its value is displayed in this field.

Possible values:

Blank
a specific cipher picked from the SSL Cipher List dialog box
a regular/wildcard expression

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed. By default, this field is blank, designating that Cleo Harmony, Cleo VLTrader, or Cleo LexiCom will select the most recent version (currently TLS 1.3).

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed when selecting an SSL cipher. To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128`, or `256` (depending on the

requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed. SSL 3.0 is the default value for compatibility with servers that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

Default value: `SSL 3.0`

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Use Put From As SMTP Mail From

Indicates that you should use the generated email's MIME From: value as the `SMTP MAIL` command's From: value also (instead of the configured SMTP service username and domain). This can be necessary when the recipient's mail server expects the two to match. If the From: value is not where bounced messages should be returned, then a Return-Path: should also be specified.

Possible values: `On` or `Off`

Default value: `Off`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

`System Default`
`TripleDES`
`AES-128`
`AES-192`
`AES-256`

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

SMTP Mailbox

A mailbox's parameters allow you access to the host system.

SMTP Mailbox: SMTP Tab

Provide **Default Values** for the headers for mailbox-level actions. Unless you specify an overriding value in a command in an action, these default values are used.

To

Cc

Bcc

You can enter multiple usernames in each of these fields. Use semi-colons (;) or commas (,) to separate them.

If this is an open-ended SMTP host (see SMTP Host: General Tab on page 344), each username specified must include the `@domain` portion of the email address.

Subject

Optional.

From

Optional. The value you specify (`user@domain`) will override the Cleo Harmony application's email address specified in the Local Listener SMTP service.

Return-Path

Optional. The value you specify here (user@domain) will override the Cleo Harmony application's return-path address specified in the Local Listener SMTP service.

Inline

Optional. The inline (non-attachment) portion of the message. You can enter text directly in this field or select a file.

Content-Type

The default content-type of the payload. Select a value from pull down menu or enter a value.

If **Content-Type** is not specified or if multiple payloads are attached in the message, the **Content-Type** is detected based first on file content and then on file extension. Detectable types include:

- `application/edifact`
- `application/edi-x12`
- `application/edi-tradacoms`
- `application/xml (text/xml)`
- `application/pdf`
- `application/msword`
- `application/x-msexcel`
- `application/rtf`
- `application/zip`
- `0`
- `image/gif`
- `image/tiff`
- `image/jpeg`
- `text/plain`
- `text/html`

- `video/mpg`

Content-Transfer-Encoding

Select a default value from the following:

- `7bit`
- `8bit`
- `quoted-printable`
- `base64`
- `uuencode`
- `binary`

If you do not select a value, the following values are assumed:

- `7bit` for `text/*` content-types
- `base64` for `binary` content-types if the server does not support the chunking extension
- `binary` for `binary` content-types if the server supports the chunking extension

Acceptable additional incoming sender usernames

Usernames (other than values above) from which incoming emails from this trading partner are accepted. come from usernames other than the To username(s) specified above. You can add multiple additional incoming sender usernames separated by semi-colons (;) or commas (,) or entered on separate lines. (VLTrader and Harmony only)

SMTP Mailbox: DSN Tab

Possible received Delivery Status Notification action (status) values:

- **delivered**: message delivery has succeeded. No further DSNs are expected.
- **failed**: message delivery has failed. No further DSNs are expected.
- **relayed**: message has been relayed or gatewayed into an environment that does not support DSNs. No further DSNs are expected.
- **delayed**: message delivery is delayed. Further DSNs are expected.
- **expanded**: message delivery has expanded to multiple recipient addresses. Further DSNs are expected.

Requested DSNs are returned back to the Cleo Harmony application in a separate SMTP session. When a DSN has been requested as part of a sent message, the Cleo Harmony application retains the original message and tracks message delivery based on the SMTP properties specified. See Specifying Local Listener advanced properties on page 759.

Message delivery status and received DSNs can be viewed in the Local Listener SMTP Server DSNs tab. See Working with DSNs on page 780.

Please note that not all SMTP servers support or honor DSN requests. DSNs are not non-reputable because they are not signed. The return of the entire original message in the DSN is meant to happen only upon failure, and only when requested. Some SMTP servers always return the entire original message in the DSN regardless of failure status and regardless of whether only message headers were requested.

If the entire original message is included in a DSN received by the Cleo Harmony application, it will strip the payload out of the DSN while saving the DSN to the received/ folder. (The Cleo Harmony sentbox can instead be used to permanently save sent payload.)

Since the Cleo Harmony SMTP server only acts as a mail endpoint, it only generates 'delivered' DSNs.

Return a DSN on success or failure

Request a Delivery Status Notification for each **To** recipient of a message (Cc and Bcc recipients are not included) and enable other fields on the tab.

Return message headers only

Return entire message

Indicate whether the returned DSN should include just the original message's outer headers or the entire original message.

Also return a DSN on delay

Requests that an intermediate DSN also be returned when a message's delivery has been delayed for an unusually long period of time.

SMTP Mailbox: Content Tab

Override SMTP Service

Enable the fields on this tab to override the default media types specified in the Local Listener **SMTP Service: Content** tab. See Configuring inbound and outbound media types on page 780.

Acceptable inbound media types

Acceptable outbound media types

Specify the media types acceptable for inbound and outbound messages.

You can use asterisks (*) or question marks (?) as wildards. Multiple media types can be separated by semi-colons (;) or commas (,) or entered on separate lines. Example values include:

- `*` - any payload media types acceptable
- `*/xml` - all payload media types with subtype 'xml' acceptable
- `text/*;image/*` - all payload media types with content-type 'text' or 'image' acceptable
- `application/edi*` - all payload media types with content-type 'application' and subtype starting with 'edi' acceptable

Specify separate values for outbound and inbound by clearing **Same as inbound**.

Same as inbound

Select the check box to use the same values specified as acceptable inbound media

SMTP Mailbox: Authenticate Tab

If the target server requires `SMTP AUTH` authentication, select the appropriate type and provide a **username** and **password** as necessary.

SMTP Mailbox: Security Tab

Note: This tab applies only to SMTPs hosts.

Security Mode

Possible values:

- `None` - For non-secure transfers, and commands and data are clear-text.
- `SSL Implicit` - For servers that support only SSL connections.
- `SSL STARTTLS` - For servers that support SSL by using either the `SSL STARTTLS` or `AUTH TLS` command.

Client Certificate

If you select `SSL STARTTLS` or `SSL Implicit` in the **SMPTs FTP** tab, the target server can issue client certificates. In this case, import the client certificate (see Certificate management on page 661) and then use the **Certificate Alias** and **Password** fields to specify or browse for the imported certificate.

SMTP Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information about payload file packaging.

SMTP Action

An action's parameters capture a repeatable transaction for your mailbox on the host system. Create a new action under the mailbox.

1. Right-click the mailbox under the host in the active tree pane.
2. Select **New Action** to create a new lower branch. Then, if desired, type a new alias in the content pane panel and click **Apply**.

SMTP Action: Action Tab

Use the **Action** tab to configure commands within an action.

See Composing an action on page 89 and SMTP Command Reference on page 360.

SMTP Command Reference

PUT

Send one or more files to the host.

```
PUT -MUL -DEL "source" "destination" name=value,...
```

-MUL

Multiple file payload (attachments).

-DEL

If the `PUT` command is successful, delete local file(s).

"source"

Local source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default outbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"destination"

Remote destination path.

- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

name=value

SMTP header=value pairs

To, Cc, Bcc, Subject, From, Return-Path, Inline, .InlineFile, Content-Type, and/or Content-Transfer-Encoding can be specified if you need to override the mailbox setting.

QUOTE

```
QUOTE "command"
```

"*command*"

Command to be sent to the server. (Example: `VRFY`, `EXPN`) See the SMTP RFC 2821 for more details on specific SMTP commands.

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"*path*"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).

- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.

- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

CHECK

See CHECK Command for information about this command.

SCRIPT

See SCRIPT command on page 951 for information about this command.

Comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

MLLP Hosts

The MLLP (Minimal Lower Layer Protocol) provides a minimalistic OSI session-layer framing protocol.

Note: All queue-based operations discussed in this section are supported only for the Cleo VLTrader and Cleo Harmony applications.

The MLLP (Minimal Lower Layer Protocol) provides a minimalistic OSI session-layer framing protocol. It is commonly used within the HL7 (Health Level Seven) community for transferring HL7 messages and acknowledgments. MLLP is defined under two releases: Release 1, which does not provide built-in reliable delivery assurance; and Release 2, which provides delivery assurance through the use of commit acknowledgments. Release 1 is most commonly used with HL7 Version 2.x, while Release 2 is typically used with HL7 Version 3. If security is required, additional protocols or packaging can be layered on top of MLLP to achieve these goals.

Within the MLLP protocol, it is important to understand senders and receivers.

- A sender is defined by an action that contains either one `PUT` command (queue-based) or one-to-many `PUT` commands (file-based). The sender, depending upon its configuration, will maintain a persistent or a transient connection with the receiver. If the send action is associated with queuing, the connection will be persistent; the connection will be opened when the action is started (either automatically at startup or manually by the user) and continue indefinitely until the action is stopped by the user. If the send action is not associated with queuing, the connection will be transient; the connection will be opened at the beginning of the action and closed at the end of the action.
- A receiver is defined by an action containing a singular `GET` command. The receiver, once its action is started (either automatically at startup or manually by the user), will enter a listening state, waiting for a sender to connect to it. Once connected, the receiver will keep the connection open, processing incoming messages, until the sender disconnects. After the connection is closed, the receiver will return to a listening state. Only one sender can be connected to a receiver at a time. The receiver, once successfully started, can only be stopped by the user.

The operation of an MLLP host is very similar to other hosts (for example, AS2, ebXML) within the Cleo Harmony application. For example, the concepts of host, mailbox, and actions still exist. However, since MLLP supports only direct connections between a sender and a receiver, and there is no authentication process, only one mailbox is allowed per host.

An MLLP host, in its strictest sense, does not need to be tied to an HL7 application or HL7 payload; however, in practice, it most likely will be. Therefore, all discussions within this section relate MLLP and HL7 together.

The following action commands are available with the Cleo Harmony application:

	Command	Purpose
Host commands	`PUT`	Send one or more messages to the host
	`GET`	Receive one or more messages from the host
Local commands	`SYSTEM`	Execute a local system command
	`WAIT`	Pause
	`SET`	Set a property
	`CLEAR`	Clear a string property
	`LCOPY`	Copy one or more local files
	`LDELETE`	Delete one or more local files

	Command	Purpose
	LREPLACE	Replace bytes in one or more local files
	CHECK	Check for a transfer, file, or directory (Cleo VLTrader and Cleo Harmony applications only)
	SCRIPT	Execute a JavaScript File (VLTrader and Harmony only)

MLLP Overview

Note: All queue-based operations discussed in this section are supported only for the Cleo VLTrader and Cleo Harmony applications.

The MLLP (Minimal Lower Layer Protocol) provides a minimalistic OSI session-layer framing protocol. It is commonly used within the HL7 (Health Level Seven) community for transferring HL7 messages and acknowledgments. MLLP is defined under two releases: Release 1, which does not provide built-in reliable delivery assurance; and Release 2, which provides delivery assurance through the use of commit acknowledgments. Release 1 is most commonly used with HL7 Version 2.x, while Release 2 is typically used with HL7 Version 3. If security is required, additional protocols or packaging can be layered on top of MLLP to achieve these goals.

Within the MLLP protocol, it is important to understand senders and receivers.

- A sender is defined by an action that contains either one PUT command (queue-based) or one-to-many PUT commands (file-based). The sender, depending upon its configuration, will maintain a persistent or a transient connection with the receiver. If the send action is associated with queuing, the connection will be persistent; the connection will be opened when the action is started (either automatically at startup or manually by the user) and continue indefinitely until the action is stopped by the user. If the send action is not associated with queuing, the connection will be transient; the connection will be opened at the beginning of the action and closed at the end of the action.
- A receiver is defined by an action containing a singular GET command. The receiver, once its action is started (either automatically at startup or manually by the user), will enter a listening state, waiting for a sender to connect to it. Once connected, the receiver will keep the connection open, processing incoming messages, until the sender disconnects. After the connection is closed, the receiver will return to a listening state. Only one sender can be connected to a receiver at a time. The receiver, once successfully started, can only be stopped by the user.

The operation of an MLLP host is very similar to other hosts (for example, AS2, ebXML) within the Cleo Harmony application. For example, the concepts of host, mailbox, and actions still exist. However, since MLLP supports only direct connections between a sender and a receiver, and there is no authentication process, only one mailbox is allowed per host.

An MLLP host, in its strictest sense, does not need to be tied to an HL7 application or HL7 payload; however, in practice, it most likely will be. Therefore, all discussions within this section relate MLLP and HL7 together.

The following action commands are available with the Cleo Harmony application:

	Command	Purpose
Host commands	PUT	Send one or more messages to the host
	GET	Receive one or more messages from the host

	Command	Purpose
Local commands	SYSTEM	Execute a local system command
	WAIT	Pause
	SET	Set a property
	CLEAR	Clear a string property
	LCOPY	Copy one or more local files
	LDELETE	Delete one or more local files
	LREPLACE	Replace bytes in one or more local files
	CHECK	Check for a transfer, file, or directory (Cleo VLTrader and Cleo Harmony applications only)
	SCRIPT	Execute a JavaScript File (VLTrader and Harmony only)

MLLP Configuration

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.
4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See MLLP Host on page 368.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See MLLP Mailbox on page 378.
   c) Click **Apply** to save your work.
6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See MLLP Action on page 379 .
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the product to prompt to you click **Apply** if you try to leave the page. However, in the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

MLLP Host

A host's parameters specify its location and how it is reached.

MLLP Host: General Tab

Outbound

Server Address

Either a fully qualified name (recommended) or an IP address for the MLLP host.

Port

The connection to the MLLP receiver. You can specify either a specific port number or `-1` to indicate the default port for MLLP/HL7 (`2575`).

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` -

Default value: `System Default`

Enabled

Select the check box to enable sender actions. Clear the check box to disable sender actions.

Inbound

Enabled

Select the check box to enable receiver actions. Clear the check box to disable receiver actions.

Port

The port on which the receiver action will listen. You can specify either a specific port number or `-1` to indicate the default port for MLLP/HL7 (`2575`).

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For the Cleo VLTrader and Cleo Harmony applications, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and/or Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Note: If the host has an external association, the default directories might be managed outside of VersaLex applications and not shown here.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

MLLP Host: MLLP Tab

Acknowledgment Mode

Select the mode for sending and receiving acknowledgments. Choose from the following options:

- **HL7 Original Acknowledgments**: when in this mode MSH-15 and MSH-16 must both be null.
- **HL7 Enhanced Acknowledgments**: when in this mode MSH-15 and MSH-16 must not be null, nor can they be set to "NE".
- **MLLP Release 2 Acknowledgments**: when in this mode only MLLP Release 2 acknowledgments are accepted.

Default File Name

The destination file name for incoming file-based messages or the destination message name for incoming queue-based messages. You can use any of the supported macros in this field, allowing for the incoming messages to be named, for example, with a date-time stamp. See Using macro variables on page 59 (Destination File context) information about all applicable macros.

MLLP Host: Advanced Tab

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for MLLP include:

Add Mailbox Alias Directory to Inbox

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0` - `n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0 - n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

`Incoming`
`Outgoing`

`Both`

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0` - `n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0` - `n`

Default value: `0`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
```

AES-256
Twofish

Default value: System Default

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If System Default is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512

Default value: System Default

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: On or Off

Default value: On

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: On or Off

Default value: On

PGP V3 Signature

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the PMode.ReceptionAwareness.Retry.Period setting.

Possible values: Any value greater than zero.

Default value: 60 seconds

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-CHECK commands: When Terminate On Fail is on, if a command fails, Email On Fail and Execute On Fail, if set, are processed, and then the action stops. When Terminate On Fail is off, if a command fails, Email On Fail and Execute On Fail, if set, are processed, and the action continues.

Regarding CHECK commands: Terminate On Fail is only honored if the ConditionsMet parameter is set and the result of the CHECK is classified as Error. The CHECK command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: On or Off

Default value: On

Unzip Use Path

Indicates whether or not zip entry paths should be used for LCOPY -UNZIP operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: On or Off

Default value: On

Wait For Execute On

Indicates whether execution should wait for processing to complete within an Execute On Fail, Execute On Successful Copy, Execute On Successful Receive, or Execute On Successful Send command. Note that this option does not apply to native AS400 execution.

Possible values: On or Off

Default value: On

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If System Default is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

System Default
TripleDES
AES-128
AES-192
AES-256

Default value: System Default

Zip Comment

Specifies the comment to be added to the zip archive file in LCOPY -ZIP operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for LCOPY -ZIP operations. If System Default is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

System Default
9 - (Best Compression)
8
7
6
5
4
3
2

`1`

`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

MLLP Mailbox

MLLP supports only direct connections between a sender and a receiver, and there is no authentication process, so only one mailbox is allowed per host.

MLLP Mailbox: MLLP Tab

Inbound Action

The default inbound action for the receiver. The drop down list contains all actions available for the mailbox.

Automatically run at startup

Select **Automatically run at startup** to have the **Inbound Action** automatically start each time the Cleo Harmony application is launched.

Note: If your **Inbound Action** is queue-based, and you have selected **Automatically run at startup**, you might encounter a condition where the action begins before the MSMQ service is up and running. In this case you will receive an error that states, `Cannot open queue. (hr=MQ_ERROR_SERVICE_NOT_AVAILABLE)`. If this occurs, you should set MSMQ as a dependency within the Cleo Harmony service. After setting this dependency, ensure that MSMQ will be started before the Cleo Harmony application. Likewise, if you shut down MSMQ, Cleo Harmony will also be shut down. Visit http://support.microsoft.com/kb/193888 for information regarding setting a dependency.

MLLP Mailbox: Queuing Tab

The **Queuing** tab allows you to establish inbound and outbound queues if messages are to be routed to and from queues rather than the file system.

Outbound

Use queue

Enables outbound queuing.

Queue Type

The only value available is **MSMQ**. MSMQ versions 2.0 through 5.0 are supported.

Queue Name

The name of the outbound queue. Only queues that are prefixed with "DIRECT=OS:" are supported. Both local and remote queues are supported.

Create queue

Indicates if the outbound queue should be created when not present. When selected, the queue specified in **Queue Name** field is created if not present. When not selected, ensure that the queue is present and properly configured. The outbound queue must be a transactional queue.

Outbound Action

Select the **Outbound Action** for the queue-based sender. The drop-down list contains all actions under the mailbox.

Automatically run at startup

Select **Automatically run at startup** to have the **Outbound Action** automatically start each time the Cleo Harmony application is launched.

Note: If you have selected **Automatically run at startup** for your **Outbound Action**, a condition can occur in which the action begins before the MSMQ service is up and running. In this case, receive an error that states, *Cannot open queue. (hr=MQ_ERROR_SERVICE_NOT_AVAILABLE)*. If this occurs, you should set MSMQ as a dependency within the Cleo Harmony service. Setting this dependency ensures that MSMQ starts before the Cleo Harmony application. Likewise, if you shut down MSMQ, the Cleo Harmony application will also be shut down. Visit http://support.microsoft.com/kb/193888 for information about setting a dependency.

Sender Restart

Specify the **Sender Restart** value. This setting determines the number of minutes before the **Outbound Action** is restarted after a connection failure or interruption.

Inbound

Use queue

Enables inbound queuing.

Queue Type

The only value available is **MSMQ**. MSMQ versions 2.0 through 5.0 are supported.

Queue Name

The name of the inbound queue. Only queues that are prefixed with "DIRECT=OS:" are supported. Both local and remote queues are supported.

Create queue

Indicates if the inbound queues should be created when not present. When selected, both the primary queue (specified in the **Queue Name** field) and an MSMQ administrative queue are created if not present. The MSMQ administrative queue is used to store MSMQ send acknowledgments. When MSMQ successfully completes a send operation on the primary queue, an acknowledgment is placed on the administrative queue. The Cleo Harmony application monitors the administrative queue to ensure guaranteed message delivery.

When the check box is cleared, ensure that the required queues are present and properly configured. The primary queue must be a transactional queue. The administrative queue must be a non-transactional queue, and its path must be that of the **Queue Name** field, suffixed with the string specified in the **MSMQ Administrative Queue Suffix** property. See Other system options on page 729

MLLP Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information about payload files and message packaging.

MLLP Action

An action's parameters capture a repeatable transaction for your mailbox on the host system. Create a new action under the mailbox.

MLLP Action: Action Tab

Use the **Action** tab to configure commands within an action.

See Composing an action on page 89 and MLLP Command Reference on page 380 below.

MLLP Command Reference

PUT

Send one or more files to the host.

```
PUT -DEL "source"
```

DEL

If `PUT` is successful, delete local file.

`-DEL` option is not applicable to queue-based `PUT` commands. If specified for a queue-based `PUT`, it is ignored.

source

Source path

- `source` parameter is not applicable to queue-based `PUT` commands. If specified for a queue-based `PUT`, it is ignored.
- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default outbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

GET

Listens for incoming connections and then receives one or more messages from the sender

```
GET
```

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"path"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.

- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place.

This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.

- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

CHECK

See CHECK Command for information about this command.

SCRIPT

See SCRIPT command on page 951 for information about this command.

Comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

WS Hosts

The Cleo Harmony Web Service (WS) protocol is used to connect to and transfer files to and from web services.

VersaLex uses Apache Axis2 (version 1.5.1) for SOAP communication and Apache Rampart (version 1.5) for WS-Security. The Cleo Harmony application does not, however, support all features contained within Axis2 and Rampart.

- The Cleo Harmony application will read and parse WSDL 1.1, 1.2 or 2.0 from a URI or local file.
- Supports HTTP and HTTP/s transports.
- Injects custom SOAP headers.
- The Cleo Harmony application can send and receive both text and binary files.
- Supports WS-Security profiles.

The Cleo Harmony Web Service protocol does NOT support:

- SOAP Encoding (as specified in SOAP 1.1)
- RESTful web services

The following action commands are available in the Cleo Harmony application:

	Command	Purpose
Host commands	CONNECT	Initializes new connection to host if necessary.
	PUT	Send one or more files to the host.
	PUT+GET	Send a SOAP document and retrieve/save the SOAP response.
	GET	Receive one or more files from the host.
	DIR	Retrieve a directory listing; can be used in conjunction with GET to retrieve multiple files.
	CONFIRM	Confirm a transfer; can be used in conjunction with GET to confirm transfer after successful retrieval.
	DELETE	Delete a remote file; can be used in conjunction with GET to delete file after successful retrieval.
	DISCONNECT	Shuts down connection to host if necessary.
Local commands	SYSTEM	Execute a local system command
	WAIT	Pause
	SET	Sets a property
	CLEAR	Clears a string property
	LCOPY	Copy one or more local files

	Command	Purpose
	LDELETE	Delete one or more local files
	LREPLACE	Replace bytes in one or more local files
	CHECK	Check for a transfer, file, or directory (VLTrader and Harmony only)
	SCRIPT	Execute a JavaScript File (VLTrader and Harmony only)

WS Configuration

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.
4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See WS Host on page 386.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See WS Mailbox on page 401.
   c) Click **Apply** to save your work.
6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See WS Action on page 402 .
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the product to prompt to you click **Apply** if you try to leave the page. However, in the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

WS Host

A host's parameters specify its location and how it is reached.

WS Host: General Tab

Server Address

Either a fully qualified name (recommended) or an IP address.

This field is automatically filled in when WSDL is selected on the WS Host: Web Service Tab on page 388 tab. You can modify this field to override the value supplied by the WSDL.

Port

You can specify either a specific port number or `-1` -1 to indicate the default port specified in the WSDL (usually `80` for HTTP or `443` for HTTP/s).

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See Specifying default host directories on page 700 for information about setting the system default.
- `Direct Internet Access or VPN` -

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For the Cleo VLTrader and Cleo Harmony application, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and/or Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Note: If the host has an external association, the default directories might be managed outside of the VersaLex application and not shown here.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

WS Host: Web Service Tab

Transport

The section is used to specify the transport protocol for connecting to the web service.

HTTP

Indicates your web service does not support HTTPs connections.

The appropriate value is automatically extracted from the WSDL. Use this option to override the WSDL setting.

HTTP/s

Indicates your web service supports secure HTTPs connections.

The appropriate value is automatically extracted from the WSDL. Use this option to override the WSDL setting.

Resource Path

The appropriate value is automatically extracted from the WSDL. Use this option to override the WSDL setting.

WSDL Location File/URL

The location for the Web Service Description Language (WSDL). Specify a URI to the WSDL or a local file containing the WSDL. The WSDL is a standard XML description of the entry points for your web service. If your service does not have a WSDL, you must create one. Refer to WSDL specification at http://www.w3.org/TR/wsdl.

Specify a URI to the WSDL or a local file containing the WSDL in the space provided. Click **Reload** to load and cache a local copy of the WSDL.

WS Host: Commands Tab

The **Commands** tab displays a list of available commands. Each command must be mapped to one or more actual web service method calls. Double-click a command or right-click the row and select **Edit** from the menu to display the **Methods** dialog box.

Using the Methods dialog box

Use the **Methods** dialog box to add, edit, and order method calls to the web service.

- Click **Add** to display the **Edit Method** dialog box, where you add a new web service call.
- For existing calls, highlight the entry and click **Edit** or double-click on the entry to display the **Edit Method** dialog box, where edit the web service call.
- Highlight and click **Delete** to remove the method call from the list for the command.
- Use **Move Up** and **Move Down** to move the highlighted method up and down in the list, respectively.

Adding or editing methods

Adding or editing the method will display the **Edit Method** dialog box. Provide information about the method you selected in the fields in the Edit Method dialog box.

Method

Choose the method you want to map from the drop-down menu. The menu is populate from methods defined in the WSDL.

Return Variable

This field is enabled if the method selected returns a value. Use this field to define a variable to store the result of the method call. Variable names must start and end with `%`. The type of the return data is displayed in parentheses following the Return Variable label. This variable can be used as a parameter input to a subsequent method call.

Success Expression

An optional expression that, if specified and true, will deem the method call successful. If the expression is false, the call is considered an error and subsequent calls are aborted. See WS Expressions on page 407 for information about specifying an expression.

Parameters

A table that contains the parameters for the selected method as defined by the WSDL. Each line in the table represents one parameter and contains the parameter's name and type, indicates whether the parameter is part of a choice, whether the parameter is required, whether the parameter field is a password field, and the parameter value.

If the WSDL specifies that the parameter part of a choice, no more than one of the choices can be used. If the WSDL has a choice of three items, the **Choice** column will display `1/3`, `2/3`, and `3/3` to indicate each item of the group. If the WSDL specifies that the parameter is required, the **Reqd** field will be selected and disabled. Otherwise, you can check the **Reqd** field to ensure that the parameter is defined before the method is called. In the value field you can enter a legal value or previously defined variable. Selecting that cell will provide a drop-down with system-recognized variables that match the parameter type.

If the parameter is a complex type or array type, a button is displayed and can be used to invoke another dialog to enter the values for the complex type or array values respectively. See WS Variables on page 402 for more information about variables. If the field is left blank, then a value can be entered for it at the mailbox and/or action levels. If the field is selected as required then a value must be entered at the mailbox or action levels.

Incoming File

The Incoming File section of the dialog box is displayed when the methods are being defined for the `GET` command. The **File Name** is used to define the resulting filename for the file to get. This can be an actual file name value or a variable that stores the file name result. The **File Data Variable** should specify the resulting variable that holds the data to get. System-recognized values will appear in a drop-down box when selecting that field. See WS Variables on page 402 for more information on specifying variable values. The **Continue Expression** is an expression which, if specified and true, determines whether to continue making calls for the same file or for subsequent files. If **Get File In Blocks** is selected on the **Advanced** tab, then this condition determines whether to continue calling the same method to continue getting blocks for the same file. If **Get File In Blocks** is cleared, then this condition determines whether there are more files to get and will repeat calling the same method until the condition returns false.

Incoming Directory

The Incoming Directory field is displayed when the methods are being defined for the `DIR` command. The **%directoryfiles%** is used to define the location of the directory file array when the array is not returned at the top-most level. If the array is at the top-most level, **%directoryfiles%** is defined in the **Return Variable** and this field will not be used.

WS Host: Advanced Tab

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for WS include:

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0` - `n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Delete Zero Length Files

Indicates whether files received that are zero-length (<= 5 bytes) should be deleted rather than processed.

Possible values: `On` or `Off`

Default value: `Off`

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0 - n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Get File In Blocks

Enable this setting if the file is transferred in multiple blocks by calling the same method repeatedly during a `GET` operation. Disable if the entire file is transferred during a single method call.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
```

MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512

Default value: System Default

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: On or Off

Default value: On

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: On or Off

Default value: On

PGP V3 Signature

Put File Block Size (bytes)

When **Put File In Blocks** is enabled, this specifies the maximum size of the data blocks for each method call.

Possible values: Any number

Default value: 4096

Put File In Blocks

Enable this setting if the file is transferred in multiple blocks by calling the same method repeatedly during a PUT operation. Disable if the entire file is transferred during a single method call.

Possible values: On or Off

Default value: Off

Reset Connection After Timeout On Response

When enabled will cause an immediate reset on the socket (instead of a graceful close) when a SocketTimeoutException occurs.

Possible values: On or Off

Default value: Off

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the PMode.ReceptionAwareness.Retry.Period setting.

Possible values: Any value greater than zero.

Default value: 60 seconds

Reuse SSL Sessions Across Actions

If selected, and if no forward proxy is being used for this host, SSL sessions from previous connections to the same destination (address and port number) may be resumed to avoid costly negotiation. If unselected, only SSL

sessions used in the current action to the same destination may be resumed. When unselected, a new SSL session is created for the initial command port connection.

Possible values: `On` or `Off`

Default value: `On`

SSL Allow Legacy Renegotiation

When selected, legacy renegotiation is allowed. If this property is not selected, the extension described in RFC5746 is used for renegotiation and the server must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Possible values: `On` or `Off`

Default value: `On`

SSL Cipher

Indicates a specific cipher, or an ordered list of ciphers, to be used with the server for SSL key exchange, encryption, and hashing.

If not set (that is, left blank), the list of default ciphers (all standard ciphers, excluding anonymous and non-encrypting) is presented to the server and the server picks one. If a regular expression (enclosed in brackets) or a wildcard expression is specified, a list of implemented ciphers (all standard ciphers, including anonymous and non-encrypting) is presented to the server, based on the conditions of the pattern. For example, if a regular expression of `[.*ECDH.*]` is specified, then the list is a subset of all implemented ciphers that belong to the Elliptical-curve Diffie-Hellman group (for example, `ECDH` is in included in their string). In all cases, whenever a list is presented, it is always ordered by cryptographic strength, with the strongest listed first.

Based on the expression you type, the **List** button shows the resulting set of ciphers in the **SSL Cipher List** dialog box. Within this dialog box, you can view the list or select a specific cipher. If you select a cipher, then its value is displayed in this field.

Possible values:

Blank
a specific cipher picked from the SSL Cipher List dialog box
a regular/wildcard expression

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed. By default, this field is blank, designating that Cleo Harmony, Cleo VLTrader, or Cleo LexiCom will select the most recent version (currently TLS 1.3).

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed when selecting an SSL cipher. To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128`, or `256` (depending on the requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed. SSL 3.0 is the default value for compatibility with servers that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

Default value: `SSL 3.0`

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Store Raw Received Message

When this property is enabled, a copy of the response message is stored in the WS/received directory.

Possible values: `On` or `Off`

Default value: `Off`

Store Raw Sent Message

When this property is enabled, a copy of the outbound message is stored in the OFTP/sent directory.

Possible values: `On` or `Off`

Default value: `Off`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

`System Default`
`TripleDES`
`AES-128`
`AES-192`
`AES-256`

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

WS Mailbox

A mailbox's parameters allow you access to the host system. Create a new mailbox under the host.

WS Mailbox: Web Service Tab

The following describes configuration of the mailbox **Web Service** tab.

You use the WS Mailbox **Web Service** tab to define parameters, both optional and required, that have not been defined on the **Web Service Host Commands** tab. See WS Command Reference on page 408. The parameters are displayed in a tree format, using indentation to show child parameters.

- For each parameter, you can enter a literal value or variable. Valid known variables of the same parameter type are displayed in the drop-down when editing the field.
- Parameters enclosed in square brackets (`[ ]`) are optional. Parameters that are not enclosed in square brackets are required and must be specified on this tab or in the command action.
- Parameter names that start with an asterisk (`*`) are password fields and the value displayed will be encoded with asterisks.
- Parameter names that start with `$` are attributes to their parent parameter.

WS Mailbox: Headers Tab

Use the mailbox **Headers** tab to specify any additional custom SOAP headers.

Double-click on an empty line (or right-click and select **Edit**) to add a new custom SOAP header.

Enter the custom SOAP header in the editor provided. The SOAP header must be valid XML, inserted into the SOAP request as part of every method call.

WS Mailbox: Security Tab

Web Services Security (WS-Security) is a flexible and feature-rich extension to SOAP to apply security to Web services. The protocol specifies how integrity and confidentiality can be enforced on messages and allows communication of various security token formats. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security. Visit http://www.oasis-open.org/specs/index.php#wssv1.0 for more information.

Use the mailbox **Security** tab to specify SSL (**TCP** sub-tab) and WS-Security options (**Request** and **Certificates** sub-tabs).

TCP

Use the TCP tab to specify an optional client certificate for TLS over secure TCP/IP. This certificate only needs to be specified for those servers that require that a client certificate be presented during SSL negotiations.

Request

WS-Security options are specified using an XML policy file. Use of a WS-Security policy file allows a wide variety of security options. The most common options have been incorporated into VersaLex as the default policy. The security elements that you are required to provide are most often dictated by the service being connected to. Check with an administrator for required security elements.

If you have your own policy file to use, you can clear **Use default policy** and enter the location of your policy file in the **Custom Policy** field. Otherwise, select **Use default policy**.

The custom policy is loaded into VersaLex when the settings are saved. To force VersaLex to reload the policy (for example, if changes to the policy have been made), click **Reload**.

Note: If you are supplying your own policy but still want to use VersaLex as your certificate store and supplier of passwords, select **Use VersaLex certs and passwords in custom policy**. VersaLex will automatically replace entries in your custom policy to utilize VersaLex resources.

- The timestamp token includes a timestamp for the time the request is created and expires. To include this token in the request, select **Send timestamp with requests**.
- The username token includes a username and non-encrypted password. To include a username token with the request, enter a username in the **username** field. A password must also be specified if a username is specified.

Certificates

The **Certificates** tab is for specifying the signing and encryption certificates. If a signing certificate is specified, then the request is signed. If an encryption certificate is specified, then the request is encrypted. In the VersaLex implementation, if the request is encrypted, it must also be signed.

The **Trading Partner's Certificates** are those provided by the trading partner.

- The **Signing Certificate** is used to verify a signature from a request's signed response.
- The **Encryption Certificate** is used to encrypt the outgoing request. If the encryption certificate is the same as the signing certificate, select **Use signing certificate**.
- Clicking **Browse** next to the field will bring up the **Select Certificate** dialog box. In this dialog box, you can locate the trading partner certificate from the local certificate store.

The **My Certificates** section is used for specifying your certificates.

- The **Signing Certificate Alias** refers to the certificate used to sign the outgoing request. You must also specify the password associated with this certificate.
- The **Encryption Certificate Alias** is used for decrypting the incoming encrypted request's response. If the encryption certificate is the same as the signing certificate, selecct **Use signing certificate**.

If you need more assistance with WS-Security, see the following resources:

http://www.ibm.com/developerworks/webservices/tutorials/ws-understand-web-services4/index.html

http://www.ibm.com/developerworks/java/library/j-jws4/

http://thilinamb.wordpress.com/2009/08/19/ws-security-policy-assymetric-binding-explained/

WS Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information about payload file packaging.

WS Action

An action's parameters capture a repeatable transaction for your mailbox on the host system.

WS Action: Action Tab

Use the **Action** tab to configure commands within an action.

See Composing an action on page 89 and WS Command Reference on page 408.

WS Variables

The Web Service protocol utilizes variables both as arguments to methods, and to store the results from method calls. The Cleo Harmony application also provides a series of predefined variables that can be used as arguments to methods. The predefined variables in the **all** section can also be used in the **Custom XML Soap Headers** field. SeeWS Mailbox: Headers Tab on page 401.

Predefined Variables

The following predefined standard and web service specific variables are available:

Command	Variable	Type*	Description
(all)	%inbox%	token	This is the path specified in the **Inbox** field on the host **General** tab.
	%outbox%	token	This is the path specified in the **Outbox** field on the host **General** tab.
	%datetime%	dateTime	The date and time that the session started.
	%date%	date	The date that the session started on.
	%time%	time	The time that the session started at.
	%host%	token	Name of the current host.
	%mailbox%	token	Name of the current mailbox.
	%index%	Int	Specifies the usage of a daily host index value. Each host's index is reset to 1 at the beginning of each day. It is incremented by one every time %index% is referenced. The minimum number of digits in the index string is determined by the **Minimum Number Of Macro Index Digits** setting on the **Options > Other** tab. See Other system options on page 729
PUT	%sourcefile%	token	Source file name.
	%sourcepath%	token	Path of the source file name.
	%sourcefilebase%	token	The base portion of the filename (minus the extension) for the source file.

Command	Variable	Type*	Description
	%sourcefileext%	token	Just the extension portion of the filename for the source file.
	%sourcefilelength%	long	The length of the file that is being sent. This is -1 for streams and files where the length cannot be determined.
	%destination%	token	The value in the destination field for the PUT action command.
	%filedata%	base64Binary	This is the file data to send. The data will be Base64 encoded. If the file is being sent in blocks (using the **Put File In Blocks** advanced option), then this holds just a block of data. Otherwise, it holds the entire file or streams worth of data.
	%filecdata%	string	This is the file data to send as a string. If this variable is specified, file data is converted to a string prior to the method call. This will be encapsulated in the request in <![CDATA[…]]> unless the file already contains CDATA, in which case it will behave like %filedatastring%.
	%filedatastring%	string	This is the file data to send as a string. If this variable is specified, file data is converted to a string prior to the method call. If the file is sent in blocks, this contains a block of data.
	%blocksize%	int	This is the size of the block of data in %filedata %, %filecdata%, or %filedatastring% that is being sent.

Command	Variable	Type*	Description
PUT, GET	%blocknumber%	int	When file data is transferred in blocks, this is the current block number being sent or received. This value is zero based, so the first block being sent or received is 0.
PUT, GET	%filecount%	int	When transferring multiple files, this is the number of files being transferred. For a PUT command, this is the number of files specified in the source field. For a GET command (when used with the -DIR option), this is the number of files returned from the DIR command.
PUT, GET	%filenumber%	int	When transferring multiple files, this is the current file number of the transfer. This number is 1 based, so the first file transferred is 1.
GET, DELETE	%directoryfile%	?	When used with the -DIR option, the DIR command is expected to return an array of values stored in %directoryfiles%. This array is enumerated and each item is assigned to the %directoryfile % variable. The type of the %directoryfile% is the same type of the array returned into the %directoryfiles% variable.
(special)	%directoryfiles%		This variable is a special variable that is expected to be assigned as part of a result in the DIR command. If this variable is not assigned prior to a GET or DELETE with the -DIR option, an error will result.

* The type corresponds to an XML schema type.

When available, variables that match the type of a drop-down field will appear as options in the drop down.

Within a session, the return variable of a method can be used as the input to any other method. The return value is stored using the variable that is specified for the method definition. Since a return value can be of any time or an array, each value of the array and complex type is also stored.

Variable names begin and end with % (i.e. %result%).

Arrays

When the return value of a method call is an array, the array is stored in the specified variable. The array's size is stored in a special member "._count". The items in the array can be indexed using brackets.

For example, if the result of a call returns a string array (string[]) and %result% is specified as the variable to store the returned value, the following table illustrates the variable definitions:

Variable	Definition
%result%	Contains the array of values
%result%._count	An integer stating the number of items in the array.
%result%[0]	The first item in the array.
%result%[1]	The second item in the array; the bracketed number is n-1 of the defined item.

Complex Data Types

When the return value of a method call is an object with a complex data type, the object is stored in the variable; member values can be accessed using a period or full stop to separate the member value from the variable name.

For example, if the result of a call is a data structure similar to the following code structure:

```
public class FileInfo {
    public FileCreds fileCreds;
    public int fileSize;
    public String fileName;
    public String[] fileOwners;
    public byte[] fileData;
}

public class FileCreds {
    public String userId;
    public String password;
    public String location;
}
```

and the return variable name is `%result%`, the following table describes the variables contained in the array:

Variable	Definition
`%result%`	Contains the complex object
`%result%.fileName`	Access the fileName field of the object
`%result%.fileData`	Access the fileData field of the object
`%result%.fileCreds.userId`	Access the userId field of the object

For an array of complex objects, dereference the array before specifying the field name. For example, for an array of FileInfo structures: `%result%[0].fileName` would access the fileName field of the first item in the array.

Method Input Terms

For method parameters that take a string value, multiple variables and text can be combined to form a term.

For example:

%outbox%%result%.fileName	Combines the outbox path with the filename field of the %result% complex variable.
%filebase%.dat	Adds ".dat" to the contents of the %filebase% variable.
Session: %sessionid%	Specifies the session with the value in the %sessionid% variable.

Method Input Functions

Method input functions are evaluated after all method input terms are resolved.

Function	Description
`file( filename )`	The file function looks up the file name specified and replaces the method data with the contents of the file. If the method parameter is expecting an array of bytes (base64Binary), then the file is treated as a binary file. Otherwise, the file is treated as a text file. Example: `file(%outbox%test\test.edi)`

WS Expressions

Expressions are evaluated by comparing the rendering of each side of the expression using the specified operator.

The following operators are available:

Operator	Description
=	Performs an equality comparison of the string rendering of both sides of the expression. If both terms contain the same string, the expression evaluates to true.
!=	The inverse of the equality comparison. If both terms are different strings, the expression evaluates to true.
<	Compares two numeric terms. Both sides must resolve to a numeric value; the expression evaluates to true if the first term is less than the second term.
<=	Compares two numeric terms. Both sides must resolve to a numeric value; the expression evaluates to true if the first term is less than or equal to the second term.

Operator	Description
>	Compares two numeric terms. Both sides must resolve to a numeric value; the expression evaluates to true if the first term is greater than the second term.
>=	Compares two numeric terms. Both sides must resolve to a numeric value; the expression evaluates to true if the first term is greater than or equal to the second term.
HAS	The expression evaluates to true if the string in the first term is contained at all in the second term.
!HAS	The expression evaluates to true if the string in the first term is NOT contained in the second term.

null keyword

The special term `null` can be entered to compare the variable with the value `NULL`.

Binary Comparisons

For binary comparisons, variable values are rendered as hexadecimal strings. The operators that work with string values can be used for these comparisons.

For example, if the variable `%result%` contains two bytes with the value of 255 in each byte, the following expression would return true:

```
%result% = FFFF
```

Array Comparisons

An array is represented as a string in an expression in the following format:

```
{term1,term2,term3}
```

WS Command Reference

CONNECT

Initializes new connection to host, if necessary.

```
CONNECT name=value,...
```

name =value

WS method parameter=value pairs. The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See WS Host: Commands Tab on page 388. An optional parameter or header is enclosed in brackets ([...]).

PUT

Send one or more files to the host.

```
PUT -DEL "source" name=value,...
```

–DEL

If the PUT command is successful, delete local file(s).

"*source*"

Local source path

- Path can be to a filename or to a directory
- You can use * and ?, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default outbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

name=value

WS method parameter=value and header=value pairs

The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See WS Host: Commands Tab on page 388. An optional parameter or header is enclosed in brackets ([...]).

GET

Receive one or more files from the host

```
GET -DIR -CON -DEL –UNI|-APE "destination" name=value,...
```

-DIR

Receive one or more files from the host

If the DIR command is not supported on the server (see Configuration), the -DIR argument is not applicable and cannot be used.

-CON

If GET is successful, confirm on host that file received.

If the CONFIRM command is not supported on the server (see Configuration), the -CON argument is not applicable and cannot be used.

-DEL

If GET is successful, delete host files.

If the DELETE command is not supported on the server (see Configuration), the -DEL argument is not applicable and cannot be used.

–UNI

Ensure local filename unique

Cannot be used with the -APE option.

-APE

If local filename exists, append to file.

Cannot be used with the -UNI option.

"*destination*"

Destination path.

- Path can be to a filename (unless you use the -DIR option) or to a directory.
- You can use a single * within the destination path in conjunction with a canned prefix and/or suffix in the filename.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Destination File context) for a list of the applicable macros.
- You can use the %HTTP.header.XXXX% macro, where XXXX references an HTTP header name in the server's response and is replaced with the header's value.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

name=value

WS method parameter=value and header=value pairs

The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See WS Host: Commands Tab on page 388. An optional parameter or header is enclosed in brackets ([...]).

PUT+GET

Send one or more files to the host and receive one or more files from the host in return.

```
PUT+GET -DEL -UNI|-APE "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-UNI

Ensure the local filename is unique.

-APE

If local filename exists, append to existing file.

"source"

Local source path

- Path can be to a filename or to a directory
- You can use * and ?, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default outbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"destination"

Local destination path.

- Path can be to a filename or to a directory.
- If you specify no path or a relative path, the command uses the default inbox.
- One * is supported with canned prefix and/or suffix in filename.
- You can use macro variables. See Using macro variables on page 59 (Destination File context) for a list of the applicable macros.

- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

DIR

Get a directory listing of available files from the host.

```
DIR name=value,...
```

name =value,...

WS method parameter=value and header=value pairs

The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See WS Host: Commands Tab on page 388. An optional parameter or header is enclosed in brackets ([...]).

CONFIRM

Confirm the receipt of one or more files on the host.

```
CONFIRM -DIR name=value,...
```

-DIR

Confirm file(s) received using directory listing from the host.

If the DIR command is not supported on the server (refer to Configuration), the -DIR argument is not applicable and cannot be used.

name=value

WS method parameter=value and header=value pairs

The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See WS Host: Commands Tab on page 388. An optional parameter or header is enclosed in brackets ([...]).

DELETE

Delete one or more files on the host.

```
DELETE -DIR name=value,...
```

-DIR

Delete files using directory listing from the host.

If the DIR command is not supported on the server (see HTTP Configuration on page 121), the -DIR argument is not applicable and cannot be used.

name=value

WS method parameter=value and header=value pairs

The required and optional parameters and headers (and potential values) are identified in the syntax of the host commands for the server. See WS Host: Commands Tab on page 388. An optional parameter or header is enclosed in brackets ([...]).

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"path"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.

- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

CHECK

See CHECK Command for information about this command.

SCRIPT

See SCRIPT command on page 951 for information about this command.

Comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

RNIF Hosts

The RosettaNet Implementation Framework (RNIF) is the protocol for packaging, routing, and transferring RosettaNet XML documents.

Primarily targeting the supply chain area, manufacturing, product and material data and service processes are also addressed. Each interaction between two companies is defined by a Partner Interface Process (PIP) specification. A PIP is essentially the definition of an XML document to be exchanged with a partner and the rules of how the document is exchanged.

Cleo Harmony RNIF supports:

- Sending and receiving v1.1 and v2.0 RNIF messages
- HTTP and HTTPs transports
- Single-action and two-action PIPs
- Synchronous and asynchronous acknowledgments
- DTD or schema validation

Cleo Harmony RNIF does not support:

- Two-action synchronous responses
- Multi-hop/intermediaries

The following action commands are available with the Cleo Harmony application:

	Command	Purpose
Host commands	`PUT`	Send one or more files to the host
Local commands	`SYSTEM`	Execute a local system command
	`WAIT`	Pause
	`SET`	Set a property
	`CLEAR`	Clear a string property
	`LCOPY`	Copy one or more local files
	`LDELETE`	Delete one or more local files
	`LREPLACE`	Replace bytes in one or more local files
	`CHECK`	Check for a transfer, file, or directory (Cleo VLTrader and Cleo Harmony applications only)
	`SCRIPT`	Execute a JavaScript File (Cleo VLTrader and Cleo Harmony applications only)

Interfacing with Cleo Harmony RNIF

Since each PIP is, in essence, a different document channel, a PIP code must be identified with each document to be sent and/or received. If a mailbox uses only one PIP and it is a single-action PIP, then the PIP can be automatically identified; otherwise, a PIP code must be associated with a document either via the PUT command or by using the Cleo Harmony proprietary RosettaNet document wrapper as outlined below.

Outgoing Documents

Example wrapper for an outgoing request (single-action or two-action PIP):

```
<w:pip xmlns:w="http://www.cleo.com/protocols/RosettaNet/
wrapper/1.0" pipCode="3A1" pipVersion="*">
<w:serviceContent>
    ...
PIP XML service content request document goes here
    ...
</w:serviceContent>
</w:pip>
Example wrapper for an outgoing response (two-action PIPs only):

<w:pip xmlns:w="http://www.cleo.com/protocols/RosettaNet/
wrapper/1.0" pipCode="3A1" pipVersion="*"
              pipInstanceId="1234567" actionType="response">
<w:serviceContent>
    ...
    PIP XML service content response document goes here
    ...
  </w:serviceContent>
</w:pip>
```

Element	Description	Attribute	Description
<pip>	Required. Root element.	pipCode	Required. The code for a PIP specification. Incoming and outgoing PIPs that can be used with a trading partner are activated and configured in the mailbox **PIPs** tab. See RNIF Mailbox: PIPs Tab on page 435.
		pipVersion	Optional. The version that matches to a particular version of a PIP. If no version is specified or the version is set to "*", the first occurrence of a configured PIP is used.

Element	Description	Attribute	Description
		pipInstanceId	Optional. The PIP instance ID uniquely identifies each usage of a PIP when documents are sent and received. This is only necessary for two-action PIPs in order to associate a response document with the original request document. If a PIP instance ID is not specified, then VersaLex automatically generates one.
		actionType	Optional. Specifies the type of message being sent. Valid values are **request** and **response**. If not specified, the default is **request**. Specify **response** for the response of a two-action PIP.
<serviceContent>	Required. PIP XML service content (payload).		

Note: Do not forget the namespace definition on the root <pip> element of the wrapper.

The service content can be specified three ways: as an XML fragment, text as part of a CDATA section, or as Base64 encoded data.

Content as XML Fragment

If the content does not have a DOCTYPE declaration (either no validation or schema validation), it can be included as an inline XML fragment:

```
...
<w:serviceContent>
<Pip3A1QuoteRequest>
...
</Pip3A1QuoteRequest>
</w:serviceContent>
...
```

Content as CDATA Section

If the content has DOCTYPE declaration, it must be wrapped in a CDATA section or encoded as Base64. The following is an example of CDATA wrapped content:

```
...
<w:serviceContent>
  <![CDATA[
  <!DOCTYPE Pip3A1QuoteRequest SYSTEM "3A1_MS_V02_00_QuoteRequest.dtd">
  <Pip3A1QuoteRequest>
    ...
  </Pip3A1QuoteRequest>
  ]]>
</w:serviceContent>
...
```

Content as Base64 Encoded Data

The content data can be encoded as Base64 data. If encoded, the attribute `encoding="base64"` must be added to the <serviceContent> element.

```
...
<w:serviceContent encoding="base64">
  [base64 content goes here]
</w:serviceContent>
...
```

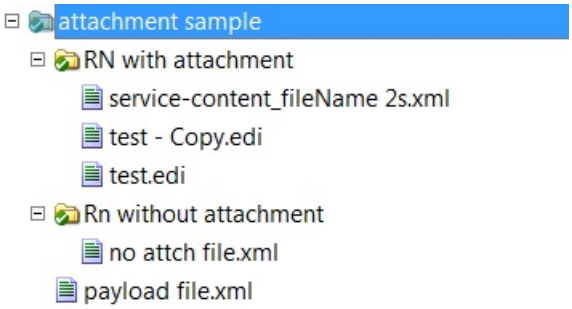
Outgoing Documents with attachments

RNIF messages with attachments can be sent using the `PUT` command with the `-MUL` option. See RNIF Command Reference on page 439 for details about using the `-MUL` option.

When you use the `-MUL` option:

- each subfolder within the outbox is sent as one RNIF message with attachments.
- the file that starts with the name `service-content_` is considered the payload. The rest of the files are attachments. If there is no file that stats with `service-content_`, no message is sent and an error is logged.
- if there is more than one file whose name starts with `service-content_`, an error is logged.
- in the generated MIME multipart message for the payload:
  - the file name used for the payload strips off the `service-content_` part of the name.
  - the Content-ID of the header is the name of the attachment.

For example, assume you want to send RNIF messages with attachments and the outbox contains three folders with the following structure:



Three RNIF messages would be sent as follows:

1. The `RN with attachment` folder contains three files: `service-content_fileName 2s.xml` is the payload. The other two files, `test.edi` and `test - Copy.edi`, are the attachments.

   When the RNIF MIME multipart message is constructed the `service-content_` part of the payload file name is stripped and `fileName 2s.xml` is used as the payload file name.

   Note: If there are multiple files in the folder, only one file name should start with `service-content_`.
2. The `RN without attachment` folder contains only one file, which is the payload. This payload is sent without attachments.
3. `payload file.xml` is directly under the source directory. This is sent as payload without attachments.

Incoming Documents

Incoming messages can be written in several formats. The raw content can be written as a stand-alone file or the content can be wrapped in XML as described in the previous section.

To control the format of the incoming message, use the **Incoming Content Format** menu and select **Two-action only** in the **RNIF Host: RosettaNet** tab. See RNIF Host: RosettaNet Tab on page 422. If **Two-action only** is selected, then all one-action PIPs will be written in the **Original** format and the two-action PIPs will follow the **Incoming Content Format** selection. If **Two-action only** is not selected, then both one-action and two-action PIPs follow the **Incoming Content Format** selection. If **Original** is selected in the **Incoming Content Format** pull-down menu, then the content is written in separate stand-alone files. If the pull-down selection is **Wrapped XML**, then the content is wrapped as specified in the previous section, with the content written as an inline XML fragment. If the selection is **Wrapped CDATA**, the content is saved as text within a CDATA section within the wrapper. If the selection is **Wrapped BASE64**, then the content is encoded as Base64 data. If the selection is MIME, the entire MIME payload is saved instead of the service content.

For a wrapped incoming message, the following attributes are added to the root <pip> element for your convenience:

Element	Description	Attribute	Description
<pip>	Required. Root element.	test	This attribute is set to **true** for a test message and **false** for a production message.
		host	The alias of the receiving VersaLex host.
		mailbox	The alias of the receiving VersaLex mailbox.

RNIF Configuration

Configure a RosettaNet host from scratch using the generic RNIF pre-configured host.

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.

4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See RNIF Host on page 421.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See RNIF Mailbox on page 434.
   c) Click **Apply** to save your work.
6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See RNIF Action on page 439 .
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the native UI to prompt to you click **Apply** when changes are made. See Other system options on page 729. However, in the web UI, this is not valid. In the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

RNIF Host

A host's parameters specify its location and how it is reached.

RNIF Host: General Tab

Server Address

Either a fully qualified name (recommended) or an IP address for the HTTP host.

Port

The HTTP command port. You can specify either a specific port number or `-1` to indicate the default port for HTTP (80) or HTTP/s (443).

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.

- `Direct Internet Access or VPN-`

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For the Cleo VLTrader and Cleo Harmony applications, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and/or Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Note: If the host has an external association, the default directories might be managed outside of the application and not shown here.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

RNIF Host: RosettaNet Tab

RNIF Version

Indicates the version of RosettaNet to use for communications. Select **v2.0** or **v1.1**.

If you select **v1.1**, you have the option to enable CIDX, an XML-based standard used in the chemical industry.

Outbound

Transmission protocol. Select **HTTP** to transmit over the standard HTTP protocol. Select **HTTP/s** to transmit using secure HTTPS protocol. If you select **HTTP/s**, you can select **Check certificate server name** to validate the name of the certificate as part of the secure transport.

Inbound

Indicates whether your trading partner is required to use **HTTP/s only** for inbound file transfers.

Resource Path

The address of the connecting RosettaNet server. If necessary, this value includes any URL parameters as well.

Overwrite duplicate file names

Allows for unique naming of stored files. Select the check box to overwrite any files that exist in the specified **Inbox**. Clear the check box to append incoming files with the same name as one as an existing. Filenames are appended with a unique number beginning with 1 and incremented each time a new file is saved.

Use default file name

Allows the incoming file to be given the name specified in its associated field. Use this option to override the file name specified by the sender. This feature is useful if the received file name must be something other than its original file name, and is common for iSeries (AS/400) platforms where the file name must be specified with a .mbr extension. You can use any of the supported macros, allowing for the incoming file to be named with a date-time stamp, for example. See Using macro variables on page 59 (Destination File context) for information about applicable macros.

Add PIP Directory to Inbox

Allows incoming messages to be sorted based on a PIP-code and PIP version number to a subdirectory (under the **Inbox** specified on the **General** tab). The subdirectory name is formatted as `PIPcode_PIPVersion` and is based on the incoming message.

Incoming Content Format

Indicates the format in which incoming documents are written. The options are **Original**, **Wrapped XML**, **Wrapped CDATA**, **Wrapped BASE64**, and **MIME**. See the **Incoming Documents** section in RNIF Overview.

Two-action only

Controls whether **Incoming Content Format** is used for two-action PIPs only or both one and two-action PIPs. See the **Incoming Documents** section in RNIF Overview.

RNIF Host: Advanced Tab

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for RNIF include:

Add Authenticated Signer Attributes

Indicates for RNIF 1.1 whether `ContentType`, `SigningTime`, and `MessageDigest` authenticated attributes are added to the signature.

Possible values: `On` or `Off`

Default value: `On`

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Allow Missing Message Digest

When this property is enabled, the RNIF message digest is not required.

Possible values: `On` or `Off`

Default value: `Off`

Base64 Encode Content

Base64 is the encoding format used by Multi-purpose Internet Mail Extension (MIME) for transmitting non-text material over text-only communications channels. Base64 is based on a 64-character subset of US-ASCII, enabling 6 bits to be represented per printable character.

Possible values: `On` or `Off`

Default value: `Off`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0` - `n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the

failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0 - n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Include Entire Certificate Chain in Signature

Indicates for RNIF 1.1 whether the entire certificate chain is sent in the signature.

Possible values: `On` or `Off`

Default value: `On`

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

Include XML Declaration In Wrapped Data

Indicates whether the optional XML Declaration is included when the incoming content is being wrapped.

Possible values: `On` or `Off`

Default value: `Off`

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0` - `n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0` - `n`

Default value: `0`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
```

SHA-1
SHA-256
SHA-384
SHA-512

Default value: System Default

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: On or Off

Default value: On

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: On or Off

Default value: On

PGP V3 Signature

Reset Connection After Timeout On Response

When enabled will cause an immediate reset on the socket (instead of a graceful close) when a SocketTimeoutException occurs.

Possible values: On or Off

Default value: Off

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the PMode.ReceptionAwareness.Retry.Period setting.

Possible values: Any value greater than zero.

Default value: 60 seconds

Reuse SSL Sessions Across Actions

If selected, and if no forward proxy is being used for this host, SSL sessions from previous connections to the same destination (address and port number) may be resumed to avoid costly negotiation. If unselected, only SSL sessions used in the current action to the same destination may be resumed. When unselected, a new SSL session is created for the initial command port connection.

Possible values: On or Off

Default value: On

Run In Test Mode

Used to enable test mode. If test mode is on, the Test setting is specified in the RosettaNet headers of outgoing messages.

Possible values: On or Off

Default value: Off

Save Received Ack As Payload

Enable this property to copy the Received Ack into the Inbox and Receivedbox.

SSL Allow Legacy Renegotiation

When selected, legacy renegotiation is allowed. If this property is not selected, the extension described in RFC5746 is used for renegotiation and the server must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Possible values: `On` or `Off`

Default value: `On`

SSL Cipher

Indicates a specific cipher, or an ordered list of ciphers, to be used with the server for SSL key exchange, encryption, and hashing.

If not set (that is, left blank), the list of default ciphers (all standard ciphers, excluding anonymous and non-encrypting) is presented to the server and the server picks one. If a regular expression (enclosed in brackets) or a wildcard expression is specified, a list of implemented ciphers (all standard ciphers, including anonymous and non-encrypting) is presented to the server, based on the conditions of the pattern. For example, if a regular expression of `[.*ECDH.*]` is specified, then the list is a subset of all implemented ciphers that belong to the Elliptical-curve Diffie-Hellman group (for example, `ECDH` is in included in their string). In all cases, whenever a list is presented, it is always ordered by cryptographic strength, with the strongest listed first.

Based on the expression you type, the **List** button shows the resulting set of ciphers in the **SSL Cipher List** dialog box. Within this dialog box, you can view the list or select a specific cipher. If you select a cipher, then its value is displayed in this field.

Possible values:

Blank
a specific cipher picked from the SSL Cipher List dialog box
a regular/wildcard expression

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed. By default, this field is blank, designating that Cleo Harmony, Cleo VLTrader, or Cleo LexiCom will select the most recent version (currently TLS 1.3).

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed when selecting an SSL cipher. To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128`, or `256` (depending on the requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed. SSL 3.0 is the default value for compatibility with servers that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

Default value: `SSL 3.0`

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Store Raw Sent Message

When this property is enabled, a copy of the outbound message is stored in the OFTP/sent directory.

Possible values: `On` or `Off`

Default value: `Off`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

`System Default`
`TripleDES`
`AES-128`
`AES-192`
`AES-256`

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

RNIF Mailbox

A mailbox's parameters allow you access to the host system.

RNIF Mailbox: RosettaNet Tab

The mailbox **RosettaNet** tab provides the identification needed for interacting with your trading partner's RosettaNet service.

Trading Partner Identification

Identifies your trading partner.

Business Identifier

Your partner's DUNS number or the agreed upon identifier.

Location Identifier

The optional target location to be sent in RNIF headers.

My Identification

Allows you to override the default RosettaNet identifiers set in the Local Listener.

Override RosettaNet service

Enables the rest of the fields in the section.

Business Identifier

Your DUNS number or the agreed upon identifier.

Location Identifier

Your optional location to be sent in the RNIF headers

RNIF Mailbox: PIPs Tab

Use the mailbox **PIPs** tab to activate and configure the Partner Interface Processes (PIPs) allowed for incoming and outgoing messages.

The **Outgoing** subtab is for Cleo Harmony application-initiated PIPs and the **Incoming** subtab is for partner-initiated PIPs.

The **Partner Interface Processes (PIPs)** menu is populated with PIPs pre-defined for the system. The system can only send or receive those PIPs added to the **Outgoing** or **Incoming** lists, respectively.

- Click **Add** to add the selected PIP in the menu to the list. When a pre-defined PIP is added to the list, it is removed from the menu. Likewise, when a pre-defined PIP is removed from the main list, it is added back into the menu.
- Click **New** to define a new PIP, or one that is not in the list.
- The same PIP code with different versions is supported by the system. If a PIP of a specific version isn't specified, the first matching PIP is used. Right-click on the **PIP** list and select **Move Up** and **Move Down** to move the PIP up or down in the list respectively.
- Right click and select **Remove** to remove a PIP from the list.
- Right click and select **Copy To** to copy the PIP from outgoing to incoming or vice versa, or to another mailbox.
- Double-click the **PIP** entry in the list (or right-click and select **Edit**) to invoke the PIP Editor dialog box, where you can edit the rules governing a PIP. See PIP Editor on page 435.

PIP Editor

The **PIP Editor** is displayed when you double-click the **PIP** entry on the **RNIF Mailbox PIP** tab or right-click an entry and select **Edit**.

For pre-defined or newly-defined PIPs, any field can be updated. PIP specifications can be obtained from RosettaNet at http://www.rosettanet.org/Standards/RosettaNetStandards/PIPDirectory/tabid/476/Default.aspx . The values for the fields in these tabs can be obtained from these specifications.

The **PIP Editor** page contains five tabs: **General**, **Content**, **Request**, **Request Ack**, **Response** and **Response Ack**.

General tab

Use the **General** tab to specify general naming information for the PIP.

PIP Code

The code that uniquely defines the PIP.

PIP Version

The version of the PIP specification. Incoming and outgoing messages are mapped to the PIP code and version to determine the rules for processing the message.

PIP Description

A user-friendly description of the PIP. This description is displayed in the PIP drop-down on the PIPs form.

My Role

The initiator role. This value is found in the specification for the PIP.

My Service

The initiator role's service. This value is found in the specification for the PIP.

Partner Role

The message receiver's role. This value is found in the specification for the PIP.

Partner Service

The receiver role's service. This value is found in the specification for the PIP.

Time to Perform

The total time to perform a two-action PIP. This field is not used for single-action PIPs. The expected value is found in the specification for the PIP. This field should be of the format HH:MM:SS.

Content tab

Use the **Content** tab to specify information related to sending and receiving of general message parts.

Retries

Specify the number of times to attempt resending the request or response when sending a request or response (as applicable to two-action PIPs) results in an error or fails to receive an expected acknowledgment.

Encryption

Specify whether no encryption is used (**None**), whether the service content and service content header are encrypted (**Payload container**), or just the service content (**Payload only**) is encrypted.

For selections other than **None**, the encryption algorithm to be used is selected in the **Encryption Method** field. If an encryption option is selected for any of the PIPs, encryption certificates will need to be specified in the mailbox **Certificates** tab. See RNIF Mailbox: Certificates Tab on page 438.

Signing

Select this check box to digitally sign messages. If **Authorization Required** is selected on any of the other tabs, you must select this option and sign the message. If you enable signing, the **Signing Algorithm** to be used can be selected and you must also specify signing certificates in the mailbox **Certificates** tab. See RNIF Mailbox: Certificates Tab on page 438.

Synchronous Acks

Select this check box to receive synchronous rather than asynchronous acknowledgments to requests and responses.

Request tab

Use the **Request** tab to define the rules for an incoming or outgoing message request.

Activity Id

The business activity name for the request. This value is found in the specification for the PIP.

Service Action Identity

The action name for the request. This value is found in the specification for the PIP.

Content Validation

Specify whether outgoing content (in the case of an outgoing message) or incoming content (in the case of an incoming message) is validated. Options are **None**, **DTD**, and **Schema**. If **DTD** or **Schema** is selected, it is expected that the DTD or schema reference are specified in the message content. Click **Import** to import a PIP DTD or schema file into the Cleo Harmony application.

Authorization Required

Select this check box to compare the signing certificate for the incoming message against the signing certificate specified in the mailbox.

Non-repudiation Required

Select this check box to save the the original request message in the host **General** tab's **Sentbox** folder for outgoing and **Receivedbox** folder for incoming. See RNIF Host on page 421.

Has Response

Select this check box if the PIP is a two-action PIP and will send a response. Clear the check box for single-action PIPs.

Request Ack tab

Use the **Request Ack** tab to define the rules for a request acknowledgment.

Time to Acknowledge

The amount of time to wait for a request acknowledgment. If the time expires without an acknowledgment or exception, the original request is resent according to the retries rules.

Authorization Required

Select this check box to compare the signing certificate for the incoming message against the signing certificate specified in the mailbox.

Response tab

The **Response** tab defines the rules for a response message.

Activity Id

The business activity name for the request. This value is found in the specification for the PIP.

Service Action Identity

The action name for the request. This value is found in the specification for the PIP.

Content Validation

Specify whether outgoing content (in the case of an outgoing message) or incoming content (in the case of an incoming message) is validated. Options are **None**, **DTD**, and **Schema**. If **DTD** or **Schema** is selected, it is expected that the DTD or schema reference are specified in the message content. Click **Import** to import a PIP DTD or schema file into the Cleo Harmony application.

Authorization Required

Select this check box to compare the signing certificate for the incoming message against the signing certificate specified in the mailbox.

Non-repudiation Required

Select this check box to save the original response message in the host **General** tab's **Sentbox** folder for outgoing and **Receivedbox** folder for incoming. See RNIF Host on page 421.

Response Ack

Use the **Response Ack** tab to define the rules for response acknowledgment.

Time to Acknowledge

The amount of time to wait for a response acknowledgment. If the time expires without an acknowledgment or exception, the original response is resent according to the retries rules.

Include in Time to Perform

Select the check box if the time for the response acknowledgment is included in the **Time to Perform** specified on the **General** tab.

Authorization Required

Select this check box to compare the signing certificate for the incoming message against the signing certificate specified in the mailbox.

RNIF Mailbox: Certificates Tab

Use this tab to associate a trading partner's signing and encryption certificates with a mailbox and override your own Local Listener's signing and encryption certificates, if necessary.

Prior to completing the mailbox's **Certificates** tab, you must acquire your trading partner's signing/encryption certificate(s) and create and/or provide to your trading partner your signing/encryption certificate(s) (see Acquiring your trading partner's signing and encryption certificates on page 86 and Creating and providing your signing/encryption certificates on page 86.)

Trading Partner Certificates

Provided by the trading partner.

Signing Certificate

Used to verify a signature from an incoming message that is signed. This certificate is optional. If not specified, the incoming signed content's signature is compared to all valid certificates in the local certificate store.

Encryption Certificate

Used to encrypt outgoing messages sent to your trading partner.

My Certificates

By default, the certificates you configured on the **Certificates** tab of the Local Listener panel are the certificates used to sign messages sent to your trading partner and decrypt messages received from your trading partner. See Configuring certificates for Local Listener on page 758.

Override Local Listener Certificates

Enables fields where you specify signing and encryption certificates to use with this particular partner instead of the certificates you configured for the Local Listener. See Configuring certificates for Local Listener on page 758.

If you override the default certificates, you must also exchange the certificates you specify here with your partner.

Signing Certificate Alias

The name of the signing certificate registered with the Cleo Harmony application through the Certificate Manager. The certificate must be the same as the one exchanged with your remote trading partners, unless you want to override it at the Mailbox level. See Local HTTP Users Configuration on page 834.

Click **Browse** to view and select a certificate. Enter the **Password** for your signing certificate's private key.

Encryption Certificate Alias

The certificate for decrypting your trading partner's messages, if you have created or obtained a separate certificate.

Click **Browse** to view and select a certificate. Enter the **Password** for your encryption certificate.

Use signing certificate

Select this check box to use the same certificate for signing and decrypting your trading partner's messages. The **Encryption Certificate Alias** and **Password** are populated to match the **Signing Certificate Alias** and disabled.

Exchange Certificates

Invokes the **Certificate Exchange** dialog box. If you override the default the certificates, you must exchange these alternate certificates with your trading partner.

RNIF Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information about payload file packaging.

RNIF Action

An action's parameters capture a repeatable transaction for your mailbox on the host system.

RNIF Action: Action Tab

Use the **Action** tab to configure commands within an action.

See Composing an action on page 89. Also see RNIF Command Reference on page 439.

RNIF Command Reference

PUT

Send one or more files to the host.

```
PUT -DEL "source" "destination" [pipCode]= .. [pipVersion]= ..
  [pipInstanceId]= .. [actionType]=request|response
```

-DEL

If the `PUT` is successful, delete the local file.

"*source*"

Local source path.

- Path can be to a filename or to a directory.
- `*` and `?`, or a regular expression, are supported in filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, it uses default outbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Remote destination path

- If a destination is not specified, this command uses the source filename.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

pipCode

The code for a PIP specification. Not needed if only one outgoing PIP. Incoming and outgoing PIPs that can be used with a trading partner are activated and configured in the mailbox **PIPs** tab. See RNIF Mailbox on page 434.

pipVersion

Matches to a particular version of a PIP. Not needed if only one version of the PIP code is active. If no version is specified or the version is set to `*`, the first occurrence of a configured PIP is used.

pipInstanceId

The PIP instance ID uniquely identifies each use of a PIP when documents are sent and received. Not needed for a request. This is really only needed for two-action PIPs in order to associate a response document with the original request document. If a PIP instance ID is not specified, the Cleo Harmony application automatically generates one.

actionType

Specifies the type of message being sent. Valid values are `request` and `response`. The default value is `request`. Specify `response` for the response of a two-action PIP.

Note: The `PUT` command `pipCode`, `pipVersion`, `pipInstanceId`, and `actionType` parameters are not needed if an outgoing file wrapper is being used instead. See RNIF Overview.

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"path"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

You can use the `SET` command to override any property in the RNIF Configuration on page 421 at action runtime.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

```
SET property
```

or

```
SET property=
```

- To clear a string property, use the CLEAR command

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the CLEAR.

```
CLEAR property
```

property

Action property name with no embedded spaces.

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the -UNZ option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the LCOPY command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The LCOPY command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).

- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.
- You can use * and ?, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use * and ?, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

CHECK

See CHECK Command for information about this command.

SCRIPT

See SCRIPT command on page 951 for information about this command.

Comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

fasp Hosts

The **Fast and Secure Protocol** (**FASP**) is a network-optimized proprietary data transfer protocol.

FASP does not expect any feedback on every packet sent. The recipient only need request those packets marked as lost.

fasp Configuration

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.
4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See fasp Host on page 445.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See fasp Mailbox on page 454.
   c) Click **Apply** to save your work.
6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See fasp Action on page 457 .
   c) Click **Apply** to save your work.
7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the native UI to prompt to you click **Apply** when changes are made. See Other system options on page 729. However, in the web UI, this is not valid. In the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

fasp Host

A host's parameters specify its location and how it is reached.

fasp Host: General Tab

SSH Connection

Server Address

Either a fully qualified name (recommended) or an IP address for the host.

Port

The fasp command port. You can specify either a specific port number or `-1` to indicate the default port for fasp (22).

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` -

Default value: `System Default`

UDP Connection

Port

Specifies the fasp data port and can be either a specific port number or `-1` to indicate the default port for fasp (33001).

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For the Cleo VLTrader and Cleo Harmony applications, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and/or Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Note: If the host has an external association, the default directories might be managed outside of Cleo Harmony, Cleo VLTrader and Cleo LexiCom, and not shown here.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

fasp Host: Advanced Tab

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for fasp include:

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0` - `n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Create Target Path

Create a target directory if it does not already exist.

Possible values: `On` or `Off`

Default value: `Off`

Delete Zero Length Files

Indicates whether files received that are zero-length (<= 5 bytes) should be deleted rather than processed.

Possible values: `On` or `Off`

Default value: `Off`

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Minimum Rate (kilobits/s)

The minimum desired transfer rate in kilobits per second (kbps).

Possible values: `0 - n`

Default value: `0`

Only Retrieve First Available File

Indicates a `GET *` should only retrieve the first available file from the server.

Possible values: `On` or `Off`

Default value: `Off`

Only Retrieve Last Available File

Indicates a `GET *` should only retrieve the last available file from the server.

Possible values: `On` or `Off`

Default value: `Off`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

`System Default`
`Alphabetical`
`Date/Time Modified`

Default value: `System Default`

Overwrite

Policy used to overwrite existing files at the destination. See Overwrite and Resume Check properties on page 454 for more information.

Possible values:

`Always` - Always re-transfer the file.
`Different` - Overwrite only if the existing file is different.
`Different and Older` - Overwrite only if the existing file is both different and older.
`Never` - Do not overwrite - skip transferring the file.
`Older` - Overwrite only if the existing file is older.

Default value: `Always`

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

Policy

Transfer rate policy with respect to other simultaneous transfers.

Possible values:

`Adaptive` - Transfer using adaptive mode for being fair to other flows.
`Fixed` - Transfer using fixed mode for constant transfer at the specified rate.
`Trickle` - Transfer using trickle mode for utilizing unused bandwidth.

Default value: `Adaptive`

Post Get Command

Post Put Command

In an action, specify commands to be executed only after a successful `GET` or `PUT` as post-get or post-put commands, respectively. When using this property, use a `SET` command within the action **before the `GET` or `PUT` command** rather than the **Advanced** tab.

The Post Put Command can be set to `QUIT`, which allows a disconnect and reconnect between file uploads when necessary.

If multiple FTP commands are needed after the `GET` or `PUT`, set this property to **all** of the commands separated by semicolons (;). If a specific FTP command needs to contain a semicolon, enclose that specific FTP command in quotes ("). Use of macro variables is supported. Refer to Using macro variables on page 59 (Post/Pre Command context) for a list of the applicable macros.

Pre Get Command

Pre Put Command

In an action, specify commands to be executed before a `GET` or `PUT` as pre-get or pre-put commands, respectively. This has the benefit of keeping the log results relative to just `GET`s and `PUT`s (especially important for Cleo VLTrader and Cleo Harmony `GET` transfer logging). In addition, for the `PUT`, it avoids connecting and logging into the server when there are no files to send. When using this property, use a `SET` command within the action **before the `GET` or `PUT` command** rather than the **Advanced** tab.

If multiple FTP commands are needed prior to the GET or PUT, set this property to **all** of the commands separated by semicolons (;). If a specific FTP command needs to contain a semicolon, enclose that specific FTP command in quotes ("). Use of macro variables is supported. See Using macro variables on page 59 (Post/Pre Command context) for a list of the applicable macros.

Pre Put Command For First File Only

If a Pre Put Command is specified, indicates whether to execute them before each file being transferred by the `PUT` or only before the first file transfer.

Possible values: `On` or `Off`

Default value: `On`

Preserve Dates

Preserve file date attributes.

Possible values: `On` or `Off`

Default value: `Off`

Resume Check

Resume policy used for partially transferred files. See Overwrite and Resume Check properties on page 454 for more information.

Possible values:

`File Attributes`- If the sizes of both files match, do not re-transfer

`Full Checksum` - If the full checksums of both files match, do not re-transfer.

`Off` - Replace the file.

`Sparse Checksum` - If the sparse checksums of both files match, don't re-transfer.

Default value: `Off`

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

Target Rate (kilobits/s)

The target transfer rate in kilobits per second (kbps). A value of zero uses the default Aspera rate, typically 10000.

Possible values: `0 - n`

Default value: `0`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Transport Encryption

Specifies the encryption cipher to be used on the UDP transport.

Possible values:`None` or `AES128`

Default value: `None`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

Overwrite and Resume Check properties

The values of the `Overwrite` and `Resume Check` properties determine whether the destination file is overwritten. The influence of each property is shown in the following table.

Overwrite	**Resume Check**			
	Off	**File Attributes**	**Full Checksum**	**Sparse Checksum**
Always	Yes	Yes	Yes	Yes
Different	Yes	?	?	?
Different and Older	?	?	?	?
Never	No	No	No	No
Older	?	?	?	?

For combinations marked with '?', the destination file is overwritten if the destination file is not identical according to the criteria selected.

fasp Mailbox

A mailbox's parameters allow access to the host system.

fasp Mailbox: fasp Tab

You can configure the **fasp** mailbox using a Password and/or one of two Public Key Authentication (PKA) methods. Your Trading Partner should specify the required type(s) of authentication necessary to access your account.

To use PKA, you must create your authentication certificate (see Creating and providing your signing/encryption certificates on page 86) and then export an SSH FTP key to send to your trading partner in either OpenSSH FTP Public Key or SSH FTP Public Key (IETF) format. See Certificate management on page 661 and Exporting certificates on page 668. See also Private key authentication on page 274.

User Name

Password

Credentials for authentication to the remote server.

Use Public Key Authentication

Enables fields necessary to use public key authentication with a user certificate. See Private key authentication on page 274.

Certificate Alias

Certificate Password

Credentials used to access the user certificate for PKA.

Use Key From File

Enables fields necessary to use PKA with an existing SSH private key file. This option is only available when you select **Use Public Key Authentication**. See Private key authentication on page 274.

Private Key File

Private Key Password

Name of and the password protecting the SSH private key file to use for PKA.

Private key authentication

Private key authentication (PKA) allows you to connect to your Trading Partner's remote server without exchanging your password over the Internet. PKA uses two keys: a private key that only you have, and a public key placed on the accessing server, usually by your Trading Partner's system administrator when the account is set up. In the Cleo Harmony application, the private key portion is maintained securely in a User Certificate protected with the **Certificate Password**. The **Certificate Alias** specifies the desired User Certificate to use for PKA.

Note: You must provide your Trading Partner with the corresponding SSH Public Key using the Certificate Manager. Using options **Export >OpenPGP** or **SSH FTP Keys** select either the **OpenSSH FTP Public Key** or **SSH FTP Public Key** (IETF) format. Do not select and send the **SSH FTP Private Key** format to your Trading Partner.

Alternatively, you can use an existing private key file. This file should be stored in a secure place and protected with a password. This feature is applicable only if you have an existing SSH private key for authentication with your Trading Partner and you are using JRE1.3. SSH private keys have no standard format. OpenSSH, SSH FTP Public Key (IETF), PuTTY, and ssh.com all have different proprietary formats. A private key generated with one cannot immediately be used with another. The Cleo Harmony application supports both OpenSSH and SSH FTP Public Key (IETF) private key file formats. If the private key is in a format not supported by the Cleo Harmony application, you should export if from the application that created it in an OpenSSH format. To determine the format of your key you can simply open it using a text editor and compare it to the partial example formats listed below.

Table 16: Supported Private Key Formats

Type	Partial Example

IEFT (DSA)	`---- BEGIN SSHTOOLS ENCRYPTED PRIVATE KEY ----`
	`Comment: 1024-bit DSA`
	`Subject: John Doe`
	`AAAACDNERVMtQ0JD3yrqcRRh1OwAAAFQof0uP52Ya5iOnuVr`
	`+o9TpQwXrOQfjPp0w8+GQ9uJ7`

IETF (RSA)	`---- BEGIN SSHTOOLS ENCRYPTED PRIVATE KEY ----`
	`Comment: 1024-bit RSS`
	`Subject: Jonh Doe`
	`AAAACDNERVMtQ0JDEOMMw0wR0TwAAAEoUYoVJjvLn7lEnvus`

OpenSSH (RSA)	`-----BEGIN RSA PRIVATE KEY-----` `MIICWwIBAAKBgQDzl7h/4lkzqSPR5GhpwYr5MmUL6IeiY9TA`

OpenSSH (DSA)	`-----BEGIN DSA PRIVATE KEY-----`
	`MIIBuwIBAAKBgQD42waNRIv7eJQoTR1PSQt`
	`+A2o8F9P1pGKLaLyw/rAg8N4FEHIN`

Table 17: Unsupported Private Key Formats

Type	Partial Example

PuTTY	`PuTTY-User-Key-File-2: ssh-rsa`
	`Encryption: none`
	`Comment: rsa-key-20070808`
	`Public-Lines: 4`
	`AAAAB3NzaC1yc2EAAAABJQAAAIBw8VeSCq0goiOwWqrlMu7F`
	`+N1QXAcBPdmvYttw`

SSH.COM	`---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----`
	`Comment: "rsa-key-20070808"`
	`P2/56wAAAiwAAAA3aWYtbW9kbntzaWdue3JzYS1wa2NzMS1z`

fasp Mailbox: Packaging Tab

You can configure packaging when you want content protection (encryption at rest).

Encrypt Outbound

Encrypt the payload sent to your Trading Partner.

Decrypt Inbound

Decrypt the payload retrieved from your Trading Partner.

Password

The password required to encrypt or decrypt.

fasp Action

An action's parameters capture a repeatable transaction for your mailbox on the host system.

fasp Action: Action Tab

Use the **Action** tab to configure commands within an action.

See Composing an action on page 89 and fasp Command Reference on page 457.

fasp Command Reference

Note: Use of absolute remote paths is recommended and might be required. Relative remote paths might result in undesired operation unless the user configuration in your Trading Partner's Aspera has an absolute path defined (non-default value).

PUT

Send one or more files to the host.

```
PUT -DEL -APE "source" "destination"
```

-DEL

If the `PUT` is successful, delete the local file.

-APE

Append file to existing destination file.

"*source*"

Local source path.

- Path can be to a filename or to a directory.
- `*` and `?`, or a regular expression, are supported in filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, it uses default outbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Remote destination path

- You can use macro variables. See Using macro variables on page 59 (Destination File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

GET

Receive one or more files from the host

```
GET -DEL -UNI|-APE "source" "destination"
```

-DEL

If the GET is successful, delete the remote file.

-UNI

Ensure the local filename is unique.

-APE

Append to existing destination file.

"*source*"

Remote source path.

If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Local destination path

- Path can be to a filename or to a directory.
- If you specify a relative path, it uses default inbox.
- You can use macro variables. See Using macro variables on page 59 (Destination File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

DIR

Get a directory listing (including file size, permissions, etc.) of available files from the host.

```
DIR "source" ["destination"]
```

"*source*"

Remote source directory path. If not specified, the current working directory applies.

"*destination*"

If not specified, the directory listing is logged rather than saved to a file. If specified, use “.” to indicate the current working directory.

LS

Get a listing of available files and directory names from the host

```
LS "source" ["destination"]
```

"*source*"

Remote source directory path. If not specified, the current working directory applies.

"*destination*"

If not specified, the filename listing is logged rather than saved to a file. If specified, use “.” to indicate the current working directory.

CD

Changes the current working directory on the host.

```
CD "directory"
```

"*directory*"

The new working directory. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

PWD

Returns the name of the current working directory on the host.

```
PWD
```

MKDIR

Creates a new directory on the host.

```
QUOTE MKDIR "directory"
```

"*directory*"

The name of the new directory. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

MV

Renames a file or directory on the host.

```
QUOTE MV "source" "destination"
```

"*source*"

The source file/directory to rename. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

The destination file/directory name. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

RM

Removes a file on the host.

```
QUOTE RM "path"
```

"*path*"

The path of the file or directory to remove. If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"path"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.

- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

CHECK

See CHECK Command for information about this command.

SCRIPT

See SCRIPT command on page 951 for information about this command.

Comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

EBICS Hosts

Electronic Banking Internet Communication Standard (EBICS) uses the HTTPs protocol as its transport mechanism to send files over the Internet.

VersaLex uses the `PUT` and `GET` action commands, both using `HTTP POST`, to transport the secure data to the remote banking server. All EBICS messages are encapsulated within XML packaging. In addition to SSL/TLS-level encryption, the package content is also encrypted. Within EBICS, there is strong usage of signatures, both hand-written and electronic.

EBICS has a client-server architecture, where the bank is the **server** and the bank's customer (company or individual) is the **client**. Within EBICS, the client uploads so-called **orders** to the server and the server processes the orders. Order direction is classified as either an **upload order**, where the customer is sending payload to the server (e.g., order type IZV - upload of a domestic payment) or a **download order**, where the bank is sending data to its customer (e.g., order type STA - download SWIFT daily accounts). Whether the order is an upload or download order, the transaction is always initiated from the client.

The EBICS specification classifies orders as **bank-technical** or **system-related** (organizational or ancillary transfers). Bank-technical orders transfer specific data between the customer and bank (e.g., payments, statements, etc.). System-related orders are used for administrative details such key management or for bank-customer contractual information exchange. The EBICS specification defines many different order types that encompass both bank-technical and system-related orders. With the exception of a few system-related orders, the VersaLex EBICS client is not required to know or understand the content of the orders; it will simply transport the information without parsing the content. With VersaLex, all supported bank-technical orders are transmitted through the `GET` or `PUT` action commands, and all supported system-related orders are transmitted through functions on the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485.

While the EBICS specification calls for many different order types that can accommodate specific requests, the FUL and FDL orders are defined by the specification to support general uploads (FUL) and downloads (FDL). See the EBICS specification at www.ebics.org for details on order types.

Customers and Users

In the context of EBICS, a **customer** is defined as the organizational unit that concludes a contract with the bank, and a **user** is defined as a human or technical system that is assigned to a customer. Customers are often also referred to as **partner**, and users are often also referred to as **subscriber**. The customer/partner has a **Partner ID** to uniquely identify it, and the user/subscriber has a **User ID**. The customer-user combination is tied to a mailbox, and their associated IDs are specified on the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485. These IDs are sent with almost every initial request to the bank server.

Technical Subscribers

The EBICS specification explains the concept of **technical subscribers**. When requests are sent from a technical subscriber, the optional <SystemID> element is defined. Technical subscribers do not exist in the context of the VersaLex EBICS client, therefore, the <SystemID> element will never be specified.

Bank-Customers Contracts

Initially, a contract is established between a bank and a customer. The contract includes details such as the orders the customer can issue, which accounts are accessible, and signing permission level.. All contractual details are outside of the EBICS specification and are therefore outside the scope of the VersaLex EBICS client. The management of these contractual details are maintained somewhere within the environment of the financial institution, and not within the VersaLex environment. Therefore, it is the responsibility of the financial institution to guard against unauthorized transactions. For example, if a certain VersaLex user is not authorized to issue a particular order,

this transaction will ultimately be prevented when the bank server issues the appropriate return code (that is, `EBICS_INVALID_USER_STATE`) during the initialization phase of an order.

File-Based Transfers

All order data tranmissions are file-based. The VersaLex EBICS client, by default, ensures that all upload requests specify an HTTP header **Content-Type** `name` parameter corresponding to the original file name within the VersaLex file system. Conversely, it is anticipated that the bank server will provide a **Content-Type** "name" parameter or a **Content-Disposition** "filename" parameter within the returned HTTP headers for all download requests. While this is anticipated, it is not required for download orders. See Inbound File Names on page 466.

Data Segmentation and Checkpoint Restart

According to the EBICS specification, there is a one (1) MB limit on the size of the payload (i.e., the data encapsulated within the <OrderData> element). After the payload has been compressed, encrypted, and base64-encoded, if larger than 1 MB, it must be segmented into multiple transaction steps. The EBICS specification defines optional checkpoint restart rules at the segment breaks. The VersaLex EBICS client supports the checkpoint restart capability for both uploads and downloads.

Signatures

EBICS calls for multiple levels of signatures. Almost every message request and response carries a signature; this signature is wrapped within the <AuthSignature> element and it uses the XML Signature methodology. This is referred to as the **identification and authentication** signature, and it is required for almost every EBICS request and response. In addition to the identification and authentication signature, a so-called **electronic signature** (abbreviated as ES) can also be present on an EBICS upload request. This signature is embodied within the <UserSignatureData> element. The **ES** signs the payload and the **identification and authentication signature** signs overall EBICS packages.

Order Attributes

The EBICS specification requires the <OrderAttribute> element on most EBICS requests. See the table below. To learn more, see the EBICS specification at www.ebics.org .

The <OrderAttribute> element is 5-character field. The setting for each character is as follows:

Position	Meaning	Permitted Values
Position	Meaning	Permitted Values
1	Type of data transmitted	**O** = order data and ES **U** = ES only **D** = order data and transport ES (or no ES in the case of certain key management orders like HIA and INI)
2	Compression type	**Z** = ZIP compression
3	Encryption type for order data and/or ES	**N** = no encryption **H** = hybrid encryption AES/RSA

Position	Meaning	Permitted Values
4	Reserved	**N** = reserved setting
5	Reserved	**N** = reserved setting

Security Media For Private Keys

The EBICS specification defines the following codes for identification of the medium for storage of private keys.

Security Medium	Setting
Security Medium	Setting
No specification	0000
Diskette	01dd
Chipcard	02dd
Other removable storage medium	03dd
Non-removable storage medium	04dd

Note that "dd" represents any number combination that is configurable by the customer. This value is specified through the **EBICS Host: EBICS** tab. See EBICS Host on page 471.

Inbound File Names

Inbound files can be received via a `GET` command or via one of the ancillary orders executed through the **EBICS mailbox: EBICS** tab (using **Execute Ancillary Order** or **Download Bank Keys**). See EBICS Mailbox on page 485.

The general order of precedence is as follows:

1. If a "destination" name is specified on the `GET` command, it is used.
2. Otherwise, the **Default File Name** setting from the **EBICS Host: EBICS** tab is used. See EBICS Host on page 471

Within the destination string of a `GET` command or within the **Default File Name**, source file macros (e.g., %sourcefile%) can be used to build the final destination name. When a macro is used, if the **Content-Disposition** "filename" or the **Content-Type** "name" is specified on the inbound response from the bank server, then it is used to resolve the macro. If both parameters are specified, then **Content-Disposition** takes precedence. Conversely, if neither parameter is specified, then the generic string, "receive.file", is used for the macro substitution.

After the inbound file name is determined, the following will determine its final name. These steps are different for files associated with a `GET` command and for files associated with an ancillary or key download.

If a file is associated with a `GET` command:

- if -UNI is specified on the command, and the file already exists, the name will be made unique (e.g., changing `FDL.xml` to `FDL1.xml`) to avoid overwriting the file.
- if -APE is specified on the command, the file will be appended to if it already exists.
- if neither -UNI nor -APE are specified, and the file already exists, it will be overwritten.

If a file is associated with an ancillary or key download:

- if the file already exists, the name will be made unique (e.g., changing `HTD.xml` to `HTD1.xml`) to avoid overwriting the file.

Key Management

The EBICS specification defines several provisions and order types associated with the exchange of public keys. Three sets of public-private keys are defined for EBICS application-level encryption and signing. They are:

1. key pair for encryption
2. key pair for identification and authentication signature
3. key pair for electronic signature (ES)

According to the specification, key pairs 1 and 2 can be the same pair, but key pair 3 must be unique. The bank server will respond with appropriate error codes if this requirement is not met.

SSL/TLS Keys

In addition to the keys used at the application-level, there is a public-private key pair for TLS-level encryption. The EBICS specification makes no restrictions as to whether or not this key pair may coincide with one of the application-level keys.

Key Exchange

When a user is first created, the bank will classify the user as **New**. Prior to conducting transactions, the user must be classified as **Ready**. The **Ready** state means that the bank has all the information necessary for the user to start submission of orders, including bank's download keys. To achieve the **Ready** state, the bank requires the receipt of certain keys. Know the requirements of your banking partner in order to provide the necessary keys according to the prescribed methods.

The transfer of keys from the client to the server and from the server to the client is referred to as **key exchange** and is supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485. Under EBICS, provisions have been made for key exchange through certain order types defined within the specification. The key exchange order types implemented through the VersaLex EBICS client are:

Upload:

- **INI** - Upload ES key
- **HIA** - Upload signing and encryption keys
- **H3K** - Upload signing, encryption, and ES keys
- **PUB** - Update ES key
- **HCA** - Update signing and encryption keys
- **HCS** - Update signing, encryption, and ES keys

Download:

- **HPB** - Download signing and encryption keys

The EBICS specification also calls for hardcopy "initialisation letters" through which a secondary submission of key information is passed. The VersaLex EBICS client also provides functions to produce these letters.

EBICS Client Order Types

Below is a table summarizing the order types referenced in the EBICS specification at www.ebics.org . The source of the table originated from Appendix 13 of **Specification EBICS Version 2.5**. The last column of the table displays where the order type is supported within the framework of an EBICS host, mailbox, or action.

Order Type	Direction of Transfer	Text	Specification Status	Where Supported in VersaLex
FDL	D	Download file with any format	Optional	Supported through the `GET` command. See EBICS Command Reference on page 489
FUL	U	Upload file with any format	Optional	Supported through the `PUT` command. See EBICS Command Reference on page 489
HAA	D	Download retrievable order types	Optional	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
HAC	D	Download status information (XML Format)	Mandatory	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
HCA	U	Update signing and encryption keys	Mandatory	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
HCS	U	Update signing, encryption, and ES keys	Mandatory	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
HEV	D	Download supported versions	Mandatory	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
HIA	U	Upload signing and encryption keys	Mandatory	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
HKD	D	Download customer data for all users	Optional	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
HPB	D	Download signing and encryption keys	Mandatory	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485

Order Type	Direction of Transfer	Text	Specification Status	Where Supported in VersaLex
HPD	D	Download bank parameters	Mandatory	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
HSA	U	Upload subscriber keys for FTAM users	Optional	Not Planned [4]
HTD	D	Download customer data for this specific user	Optional	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
HVD	D	Retrieve VEU state	Conditional	
HVE	U	Add VEU state	Conditional	
HVS	U	VEU cancellation	Conditional	
HVT	D	Retrieve VEU cancellation details	Conditional	
HVU	D	Download VEU overview	Conditional	
HVZ	D	Download VEU overview with additional information	Conditional	
H3K	U	Upload signing, encryption, and ES keys	Optional	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
INI	U	Upload ES key	Optional	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
PTK	D	Download status information (German version only)	Optional	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485

Order Type	Direction of Transfer	Text	Specification Status	Where Supported in VersaLex
PUB	U	Update ES Key	Optional	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
SPR	U	Suspend user	Optional	Supported through the **EBICS mailbox: EBICS** tab. See EBICS Mailbox on page 485
AEA, AIA, etc. [5]	U/D	Variable	Variable	Upload commands supported through the `PUT` command . Download command supported through the `GET` command . See EBICS Command Reference on page 489

EBICS Configuration

The following sections explain how to configure an EBICS host from scratch using the generic EBICS preconfigured host.

1. Obtain the following parameters from your bank server:
   - URL, of the form *https://remote-host:port/resource-path?optional-parameters* .
   - The server's Host ID.
   - EBICS version supported (2.4 or 2.5).
   - ES (electronic signature) version supported (A005 or A006).
2. Provide the following parameters to your bank server:
   - Your Partner ID
   - Your User ID
3. Click the **Templates** tab in the tree pane.
4. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
5. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.
6. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See EBICS Host on page 471.
   c) Click **Apply** to save your work.
7. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.

b) Enter mailbox-level configuration information on the tabs in the content pane. See EBICS Mailbox on page 485.

c) Click **Apply** to save your work.

8. Enter action-level configuration information.

a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.

b) Edit action information on the tabs in the content pane. See EBICS Action on page 488 .

c) Click **Apply** to save your work.

9. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the native UI to prompt to you click **Apply** when changes are made. See Other system options on page 729. However, in the web UI, this is not valid. In the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

EBICS Host

The following describes configuration of the Generic EBICS preconfigured host.

To rename the host alias, right-click on the host and choose **Rename**. Alternatively, you can change the host alias by modifying the **Host** alias field in the content pane and clicking **Apply**.

EBICS Host: General Tab

Server Address

The address where your trading partner's server receives requests. Either a fully qualified name (recommended) or an IP address.

Port

The port where your trading partner's server receives requests. You can specify either a specific port number or `-1` to indicate the default port for HTTP (80) or HTTP/s (443).

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` - Use either a direct connection to the internet or a VPN.

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For VLTrader and Harmony, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and/or Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: No default value.

EBICS Host: EBICS Tab

To

Host ID

The bank server's identifier, up to 35 characters with pattern [a-zA-Z0-9,=]. The value you enter here is placed in the `<HostID>` element of requests.

Received Files

Default File Name

The filename to be used when an inbound file name is not otherwise specified. To understand the rules for naming inbound files, see EBICS Overview. This field can include any supported macros; see Using Macro Variables for information about applicable macros (Destination File context) and example usage. Also, note the EBICS-specific reserved macro variable, `%ebics.ordertype%`, which substitutes the three-character order type.

Ancillary Order Inbox

Specify the destination location for the ancillary download orders through the **Ancillary Order Inbox**. All ancillary order data downloaded through **Execute Ancillary Order** will be placed in this location, as well as the <HPBResponseOrderData> associated with **Download Bank Keys**. See EBICS Mailbox on page 485. Click **[...]** to change the ancillary order inbox location, or select "%inbox%" or a custom macro variable from the drop-down list. If this field is left blank, the default inbox location (as set on the host **General** tab) will be inserted automatically and used.

Initial Requests

Specify product information

Select **Specify product information** to specify the optional <Product> element on each initial EBICS request (that is, "initialisation" phase). When selected, the following element will be included in the XML: `<Product Language="en" InstituteID="Cleo Communications">`**`VersaLex`** `4.5</Product>`. Language (i.e., "en" for English) is in accordance with ISO 639-1. "VersaLex" will be replaced

by "LexiCom", "VLTrader", or "Harmony" as necessary, followed by the current version level of the software product.

Security Medium ID

Specify the **Security Medium ID**. This is the two-digit identifier that the EBICS specification requires as part of the <SecurityMedium> element. Since all Cleo Harmony private keys are stored on a non-removable medium, the following element will be included in the XML (given the example value of "00" as shown in the panel above): `<SecurityMedium>0400</ SecurityMedium>`.

EBICS Host: HTTP Tab

HTTP/HTTPs

Only **HTTP/s** is allowed for EBICS; therefore, it is pre-selected and cannot be changed. However, to verify that the server name in the received SSL server certificate matches the connected server name, select **Check certificate server name**.

Check certificate server name

Verifies that the server name in the received SSL server certificate matches the server name actually connected to.

Method

Use `POST` for both the `PUT` and `GET` commands since `POST` is used exclusively within the context of EBICS.

Path

The bank server's resource path. Given the URL provided by your banking partner in the form `https://remote-host:port/resource-path?optional-parameters`, the bolded portion in this field should be entered. Note that the beginning slash ("/") is required.

Parameters

Specify any optional URL parameters. By default, no parameters are specified for EBICS messages. If parameters are required, you must obtain them from your banking partner when the relationship is established. Given the URL provided by the banking partner in the form `https://remote-host:port/resource-path?optional-parameters` the bolded portion in this field should be entered.

For syntax and rules on specifying HTTP parameters, see HTTP Configuration on page 121 section. Note that you cannot specify a parameter that matches an EBICS `PUT`/`GET` reserved parameter (for example, `OrderType`).

Headers

Specify values to override any default headers or add new, custom headers. When overriding default headers, make sure they meet the requirements of the EBICS specification. The Cleo Harmony EBICS client will, by default, generate the following headers on all generated HTTP requests:

- `Host` header (for example, *Host: bank01.bank.com:443*)
- `Content-type` header, with the `name` parameter if applicable (for example, *Content-Type: text/xml; name=cust01.pain.001.001.02*)
- `Content-Length` header (for example, *Content-length:1000*)

The Cleo Harmony EBICS client will in turn honor the following headers on all generated HTTP responses:

- `Content-type` header, with the `name` parameter if applicable (for example, *Content-type: text/xml; name=cust01.camt.053.001.02*)
- `Content-Length` header (for example, *Content-length:1000*)
- `Content-Disposition` header, with the `filename` parameter if applicable (for example, *Content-disposition: inline; filename= cust01.camt.053.001.02*)

EBICS Host: Advanced Tab

The host's **Advanced** tab contains several property settings fields. These settings typically do not affect your ability to connect to a host. However, you may want to change some of these settings when configuring a runtime environment.

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for EBICS include:

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0` - `n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0` - `n` seconds

`0` indicates no timeout

Default value: `150` seconds

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

EBICS Version

Specifies the version of EBICS that should be used.

Possible values: `EBICS 2.4` or `EBICS 2.5`

Default value: `EBICS 2.4`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Encryption Algorithm

The method used to encrypt/decrypt payload.

Possible values:

- `AES/128`
- `AES/192`
- `AES/256`
- `SEED`
- `TripleDES`

Default value: `TripleDES`

ES Version

Specifies the version of ES that should be used.

Possible values:

- `A005`
- `A006`

Default value: `A005`

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0 - n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Ignore EOL Characters In ES Hash Calculation

If selected, all CR and LF characters that are in the payload will be ignored in the ES hash calculation.

Possible values: `On` or `Off`

Default value: `Off`

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

Include Line Separators In Base64 Content

If selected, indicates that CRLF should be used to break Base64 <OrderData> content into fixed-length blocks (generally 64 bytes). If false, Base64 <OrderData> will be output with no line breaks.

Possible values: `On` or `Off`

Default value: `Off`

Include X509 Data In Key Uploads

When this property is selected, the optional X509 certificate data is included in the XML document body for all key uploads that contain an element that extends `<PubKeyInfoType>`. This includes `INI`, `HIA`, `PUB`, `HCA`, and `HCS`. For the H3K transaction (version 2.5 only), X509 certificate data is always included, as it is not optional for H3K.

Possible values: `On` or `Off`

Default value: `Off`

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Omit Name Parameter From Content Type

When selected, the applicable file name is not included in the Content-Type header.

Possible values: `On` or `Off`

Default value: `Off`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512
```

Default value: `System Default`

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: `On` or `Off`

Default value: `On`

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: `On` or `Off`

Default value: `On`

PGP V3 Signature

Reset Connection After Timeout On Response

When enabled will cause an immediate reset on the socket (instead of a graceful close) when a `SocketTimeoutException` occurs.

Possible values: `On` or `Off`

Default value: `Off`

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

Reuse SSL Sessions Across Actions

If selected, and if no forward proxy is being used for this host, SSL sessions from previous connections to the same destination (address and port number) may be resumed to avoid costly negotiation. If unselected, only SSL sessions used in the current action to the same destination may be resumed. When unselected, a new SSL session is created for the initial command port connection.

Possible values: `On` or `Off`

Default value: `On`

SSL Allow Legacy Renegotiation

When selected, legacy renegotiation is allowed. If this property is not selected, the extension described in RFC5746 is used for renegotiation and the server must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Possible values: `On` or `Off`

Default value: `On`

SSL Cipher

Indicates a specific cipher, or an ordered list of ciphers, to be used with the server for SSL key exchange, encryption, and hashing.

If not set (that is, left blank), the list of default ciphers (all standard ciphers, excluding anonymous and non-encrypting) is presented to the server and the server picks one. If a regular expression (enclosed in brackets) or a wildcard expression is specified, a list of implemented ciphers (all standard ciphers, including anonymous and non-encrypting) is presented to the server, based on the conditions of the pattern. For example, if a regular expression of `[.*ECDH.*]` is specified, then the list is a subset of all implemented ciphers that belong to the Elliptical-curve Diffie-Hellman group (for example, `ECDH` is in included in their string). In all cases, whenever a list is presented, it is always ordered by cryptographic strength, with the strongest listed first.

Based on the expression you type, the **List** button shows the resulting set of ciphers in the **SSL Cipher List** dialog box. Within this dialog box, you can view the list or select a specific cipher. If you select a cipher, then its value is displayed in this field.

Possible values:

Blank
a specific cipher picked from the SSL Cipher List dialog box
a regular/wildcard expression

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed. By default, this field is blank, designating that Cleo Harmony, Cleo VLTrader, or Cleo LexiCom will select the most recent version (currently TLS 1.3).

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed when selecting an SSL cipher. To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128`, or `256` (depending on the requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed. SSL 3.0 is the default value for compatibility with servers that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

Default value: `SSL 3.0`

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Store Raw Sent And Received

Indicates whether copies of the "raw" outgoing requests and corresponding incoming responses are stored in the EBICS\sent+received folder. These files may be useful in diagnosing problems, however, generally this property should be 'off' to conserve disk space.

Possible values: `On` or `Off`

Default value: `Off`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When

`Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

`System Default`
`TripleDES`
`AES-128`
`AES-192`
`AES-256`

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`

4
3
2
1
0 - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

EBICS Mailbox

A mailbox's parameters allow access to the remote bank server and define the desired security level of the file being sent.

EBICS Mailbox: EBICS Tab

Set up your identification to the bank server, manage key exchange, and perform several ancillary functions.

From

While these fields are not required for all EBICS requests, they are required for most and therefore values must be specified.

My Partner ID

My User ID

Your identification. Up to 35 characters with pattern `[a-zA-Z0-9,=]` for each field..

Ancillary Orders

Execute Ancillary Order

Click **Execute Ancillary Order** to display the **Executing Ancillary Order** dialog box. See Executing an ancillary order on page 485 .

Key Management

Perform key management tasks. See Managing keys within EBICS on page 486.

Executing an ancillary order

1. Optional. Override the value in the **Ancillary Order Inbox** field.
2. Select an order from the **Order Type** menu.

   Choose from the following:

   - Download Retrievable Orders (HAA)
   - Download Customer Acknowledgment (HAC)
   - Download Supported Versions (HEV)
   - Download Customer Data (HKD)
   - Download Bank Parameters (HPD)
   - Download Subscriber Data (HTD)
   - Download Customer Protocol (PTK)
3. Depending upon the order type selected, the **Start Date** and **End Date** will be enabled. In this case, specify values. The date values must be in the form `YYYY-MM-DD`.

4. Click **Execute** to run the order.

   Messages are displayed as the transaction steps take place for execution of the order.
5. Optional. Click **Cancel** at any point to interrupt the execution.

Some of the ancillary orders might not be supported by the server, either because they are optional or because they are not supported under the particular EBICS version. When this occurs, it is possible to see the return code `EBICS_UNSUPPORTED_ORDER_TYPE` or `EBICS_INVALID_ORDER_TYPE`.

For all ancillary orders except HEV, the downloaded order data will be placed in ancillary order inbox (as seen in the FILE record shown in the dialog box above). Since the response data is very simple for HEV, it will be reported immediately through detail messages.

Managing keys within EBICS

The exchange of all keys takes place from the **Key Management** panel. To understand key-pair requirements and key exchange within the context of EBICS, see EBICS Overview.

Uploading your keys

1. On the EBICS mailbox EBICS tab, click **Upload My Keys**.

   The **Uploading My Keys** dialog box appears.
2. In the **Order Type** menu, select the upload order to execute.

   Choose from the following:

   - Upload ES Key (INI)
   - Upload Signing and Encryption Keys (HIA)
   - Upload Signing, Encryption, and ES Keys (H3K)
   - Update ES Key (PUB)
   - Update Signing and Encryption Keys (HCA)
   - Upload Signing, Encryption, and ES Keys (HCS)
3. Click **Execute** to begin the transaction for uploading. As the transaction takes place, the progress is shown through messages displayed within the dialog box.
4. Optional. Click **Cancel** at any point to interrupt the execution.

Downloading the bank keys

1. On the EBICS mailbox EBICS tab, click **Download Bank Keys**.

   The **Downloading Bank Keys** dialog box appears and the download begins.

   As the transaction takes place, the progress is shown through messages displayed within the dialog box.

   The <OrderData> of the HPB response (embodied in <ebicsKeyManagementResponse>) is decoded, decrypted, and decompressed, yielding an <HPBResponseOrderData> instance document. This document is stored in the ancillary order inbox location in a file name according to the **Inbound File Names**. See EBICS Overview. In addition, the pertinent key information contained within the <HPBResponseOrderData> is also stored in the host file associated with this mailbox.
2. Optional. Click **Cancel** at any point to interrupt the download.

Printing initialization letters

If you have uploaded your keys to the bank through the INI and HIA transactions, the EBICS specification calls for separate hard copy letters.

1. On the EBICS mailbox EBICS tab, click **Print Initialisation Letters**.

Separate confirmation dialog boxes appears for each type of transaction - INI and HIA.

2. Click **OK** for each confirmation.

   The system prints two letters containing the data according the EBICS specification. For more information, visit www.ebics.org.

Suspending your account

If your account or its associated keys have been compromised in some way, you can easily suspend your account.

- On the EBICS mailbox **EBICS** tab, click **Suspend My User Account**.

  The system executes the SPR order and displays a dialog box containing information about the order.

  The SPR order is a special upload transaction, transmitting only the ES of a dummy one-space payload. Since only the ES is sent, the <OrderAttributes> will be set to **UZHNN**. See EBICS Overview.

EBICS Mailbox: ES Tab

ES Certificate Alias

Password

Enter your **ES Certificate Alias**. This is the name of the ES certificate that is registered with the Cleo Harmony application through the Certificate Manager. Click **Browse** to view and select this certificate.

Enter the for your certificate's private key.

Signature Class

If you are transacting business with a bank that is EBICS T compliant, then **Signature Class** should be set to **Transport signature (type 'T')**. If you are transacting business with a bank that is EBICS TS compliant, then **Signature Class** should be set to **Single signature (type 'E')**. Note that the A and B signature classes, as defined in the EBICS specification, will not be supported until VEU is fully supported. See EBICS Overview.

Note:

Referring to the EBICS specification and the `ebics_signature.xsd` schema (found at www.ebics.org), it appears that the element <OrderSignatureData> is unbounded within the <UserSignatureData> element. At this time, the Cleo Harmony EBICS client supports only one instance of <OrderSignatureData>.

The bank server will maintain a record of your partner and user ID, along with your associated signature permission level. The mechanism the bank uses to obtain and initialize these records is outside the scope of the Cleo VerasLex EBICS client.

The EBICS specification requires that the certificate used for ES is different from the certificate used for identification and authentication and encryption. See EBICS Overview. See EBICS Mailbox: Certificates Tab on page 487 for information about defining identification and authentication certificate and the encryption certificate.

EBICS Mailbox: Certificates Tab

My Certificates

Override Local Listener Certificates

Enables fields where you specify signing and encryption certificates to use with this particular partner instead of the certificates you configured for the Local Listener. See Configuring certificates for Local Listener on page 758.

If you override the default certificates, you must also exchange the certificates you specify here with your partner.

Signing Certificate Alias

The name of the signing certificate registered with the Cleo Harmony application through the Certificate Manager. The certificate must be the same as the one exchanged with your remote trading partners, unless you want to override it at the Mailbox level. See Configuring certificates for Local Listener on page 758.

Click **Browse** to navigate to and select a certificate. Enter the **Password** for your signing certificate's private key.

Encryption Certificate Alias

The certificate for decrypting your trading partner's messages, if you have created or obtained a separate certificate.

Click **Browse** to navigate to and select a certificate. Enter the **Password** for your encryption certificate.

Use signing certificate

Select this check box to use the same certificate for signing and decrypting your trading partner's messages. The **Encryption Certificate Alias** and **Password** are populated to match the **Signing Certificate Alias** and disabled.

EBICS Mailbox: HTTP Tab

Use the mailbox **HTTP** tab to assign **Default Values** for headers for `GET` and `PUT`. For EBICS, the default value of the **Content-Type** header must always be `text/xml` or `application/xml`.

EBICS Mailbox: Authenticate Tab

If the target server requires WWW authentication, select the appropriate type and provide a **Username** and **Password** and, optionally, the **Realm**.

EBICS Mailbox: Security Tab

Since it is mandated for EBICS, HTTP/s is pre-selected on the **Security** tab. With HTTP/s, the target bank server can issue client certificates. If so, import the client certificate using Certificate management on page 661 and then specify (or browse to) the imported **Certificate Alias** and specify a **Password**.

EBICS Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information about payload files packaging.

EBICS Trading Partner

A trading partner's parameters define a unique identifier on the host system. By default, the **Trading Partner** branch is not created since it is unnecessary for EBICS transactions.

EBICS Action

An action's parameters capture a repeatable transaction for your mailbox on the host system. Create a new action under the mailbox.

EBICS Action: Action Tab

Use the **Action** tab to configure commands within an action.

The commands specified in the host **HTTP** tab (as well as the local commands) are available for use. See EBICS Host on page 471, Composing an action on page 89, and EBICS Command Reference on page 489.

Note: If a parameter or header value has an embedded space, you must use a `\s` to represent the space within the command. For example, `%OPQ\scompany` represents `%OPQ company`. This is done automatically in the dialog editor. If a space is left in the value, the command is not parsed correctly.

EBICS Command Reference

PUT

Send one or more files to the bank server.

```
PUT -DEL "source" OrderType=,
[StartDate]=, [EndDate]=,[FileFormat]=, [CountryCode]=,
[CustomParameters]=, name=value,...
```

-DEL

If `PUT` is successful, delete the local file.

"source"

Local source path

- Path can be to a filename or to a directory.
- `*` and `?`, or a regular expression, are supported in filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default outbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

OrderType=,

This required parameter specifies the three-character code defined by the EBICS specification. The acceptable order types include the generic FUL or any supported **upload** request listed in Section 1 of *Annex 2 to the Specification EBICS*.

[StartDate]=, [EndDate]=

These optional parameters specify the start and end date, both of the form `YYYY-MM-DD` according to ISO 8601. If a date range is specified, then both the StartDate and EndDate must be specified. If the order type is not FDL or FUL, you can only specify StartDate-EndDate if CustomParameters is not specified.

[FileFormat]=,

The file format must be of the form *<area>.<syntax_and_format>.<description>*. See Section 2 of the *Annex 2 to the Specification EBICS*. Note that, while this parameter is only applicable to certain order types, it is required for the FUL and FDL order types. Also, macros are allowed when FileFormat is used on the PUT command (Destination File context).

[CountryCode]=,

If you specify the FileFormat parameter, you can also specify an optional two-character country code. All country codes should comply with the ISO 3166-1 standard, including the "exceptional reservations" category (for example, "EU" indicates European Union).

[CustomParameters],

This optional parameter can contain one-to-many generic key-value pairs, each separated by a semi-colon. If the order type is not FDL or FUL, you can only specify CustomParameters if StartDate-EndDate are not specified.

name

HTTP parameter=value and header=value pairs

GET

Receive one file from the bank server.

```
GET -UNI|-APE "destination" OrderType=,
[StartDate]=,[EndDate]=, [FileFormat]=, [CountryCode]=,
[CustomParameters]=, name=value,...
```

-UNI

Ensure the local filename is unique.

–APE

If local filename exists, append the file.

"destination"

Local destination path

- Path can be to a filename or to a directory.
- `*` and `?`, or a regular expression, are supported in filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

OrderType=,

This required parameter specifies the three-character code defined by the EBICS specification. The acceptable order types include the generic FDL or any supported **download** request listed in Section 1 of *Annex 2 to the Specification EBICS*.

[StartDate]=, [EndDate]=

These optional parameters specify the start and end date, both of the form `YYYY-MM-DD` according to ISO 8601. If a date range is specified, then both the StartDate and EndDate must be specified. If the order type is not FDL or FUL, you can only specify StartDate-EndDate if CustomParameters is not specified.

[FileFormat]=,

The file format must be of the form *<area>.<syntax_and_format>.<description>*. See Section 2 of the *Annex 2 to the Specification EBICS*. Note that, while this parameter is only applicable to certain order types, it is required for the FUL and FDL order types. Also, macros are allowed when FileFormat is used on the PUT command (Destination File context).

[CountryCode]=,

If you specify the FileFormat parameter, you can also specify an optional two-character country code. All country codes should comply with the ISO 3166-1 standard, including the "exceptional reservations" category (for example, "EU" indicates European Union).

[CustomParameters],

This optional parameter can contain one-to-many generic key-value pairs, each separated by a semi-colon. If the order type is not FDL or FUL, you can only specify CustomParameters if StartDate-EndDate are not specified.

name

HTTP parameter=value and header=value pairs

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"path"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.

- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

CHECK

See CHECK command on page 943 for information about this advanced command.

SCRIPT

See to SCRIPT command on page 951 for information about this advanced command.

EBICS Comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

EBICS-Specific Directories

The following additional directories will be created either during the EBICS installation or as needed by the application.

Directory	Purpose
`EBICS\ack\sent\`	The `EBICS\ack\sent\` directory contains the sent application-level acknowledgments (those sent during the 'Receipt' step of an EBICS download transaction). Acknowledgments are only stored if 'Save Sent Receipt' is set on the Local Listener Advanced tab. Saved receipts are archived automatically according to the 'Archive ...' settings, also located on the Local Listener Advanced tab. See Specifying Local Listener advanced properties on page 759. Archive files are stored under `EBICS\ack\sent\`.

Directory	Purpose
`EBICS\schemas_2_4\`	The `EBICS\schemas_2_4\` directory contains XML schema (.xsd) files that describe the format of EBICS 2.4 documents.
`EBICS\schemas_2_5\`	The `EBICS\schemas_2_5\` directory contains XML schema (.xsd) files that describe the format of EBICS 2.5 documents.
`EBICS\sent+received\`	The `EBICS\sent+received\` directory contains copies of the raw outgoing requests and corresponding incoming responses. These files can be helpful in diagnosing problems. Old files should be deleted or archived by the user if necessary. Within `EBICS\sent+received\` , subdirectories further divide the data based on host ID, upload\nonce, download\nonce, or order type.
`EBICS\unsent\`	The `EBICS\unsent` directory contains transient copies of the raw XML associated with EBICS requests. Files in the folder are removed once a transaction is complete.

EBICS Quick-Start Steps

Below are the steps to get started with an EBICS host.

Before Starting

Before starting, you must obtain the following parameters from your bank server:

- URL, of the form `https://remote-host:port/resource-path?optional-parameters`
- **Host ID**
- EBICS version supported (2.4 or 2.5)
- ES (electronic signature) version supported (A005 or A006)

Before starting, you must provide the following parameters to your bank server:

- Your **Partner ID**
- Your **User ID**

Once you exchange the above information with your bank server, you can proceed to activate a generic EBICS host within VersaLex:

1. Click the **Templates** tab in the tree pane.
2. Right-click the **Generic EBICS** host under the **Generic** folder.
3. Select **Clone and Activate**.
4. If desired, type a new host alias in the content pane panel and click **Apply**.
5. From here, all changes will be made to the newly activated host.

Host Configuration

1. On the EBICS Host General tab (see EBICS Host: General Tab on page 471) do the follwing:
   a. In the **Server Address** field, provide the *remote-host* section of the server's URL.
   b. In the **Port #** field, provide the *port* section of the server's URL.
2. On the EBICS Host EBICS tab (see EBICS Host: EBICS Tab on page 472 do the following:
   a. In the **Host ID** field, provide the Host ID provided by your bank server. This identifier is case sensitive.

3. For the HTTP `GET` and `PUT` commands on the EBICS Host HTTP tab (see EBICS Host: HTTP Tab on page 473):
   a. Since EBICS allows only the POST method, the **Method** fields will be pre-configured.
   b. In the **Path** fields, provide the *resource-path* section of your bank server's URL.
   c. In the **Parameters** fields, provide the *optional-parameters* section of your bank server's URL.
   d. Since EBICS allows 'text/xml' and 'application/xml', the **Headers** fields will be preconfigured for you.
4. On the EBICS Host Advanced tab (see EBICS Host: Advanced Tab on page 474:
   a. Select the **EBICS Filter Group** to view the baseline configurable EBICS properties. The default properties related to SSL should be sufficient to begin. Note that the **EBICS Version** defaults to EBICS 2.4 and the **ES Version** defaults to A005. If the server requires a different setting, change these properties appropriately. For detailed information regarding EBICS-specific advanced properties, refer to the host Advanced tab.
   b. While performing initial tests, it can be useful to set the **Store Raw Sent And Received** property. When set, the outgoing requests and corresponding incoming responses will be stored in the **EBICS\sent+received** folder. These files can be useful in diagnosing problems. However, after initial tests are complete and everything is running smoothly, you can disable this property to conserve disk space.

Mailbox Configuration

1. On the mailbox **EBICS** tab:
   a) Fill in the **My Partner ID** field with the **Partner ID** provided to your bank server. This value is case-sensitive.
   b) Fill in the **My User ID** field with the **User ID** provided to your bank server. This value is case-sensitive.
2. On the mailbox **ES** tab, fill in the **ES Certificate Alias** and **Password** fields associated with your ES certificate. EBICS requires that your ES certificate be different from the certificate you use for basic signing and encryption (those configured under the mailbox **Certificates** tab).
3. On the mailbox **Certificates** tab:
   a) To override the baseline Local Listener certificates, select **Override Local Listener Certificates** and fill in the **Signing Certificate Alias** and **Password**, as well as the **Encryption Certificate Alias** and **Password** fields. Note that EBICS allows these certificates to be the same; however, they must be different from your ES certificate configured under the mailbox **ES** tab.

At this point, no other configuration should be necessary. Proceed to Key Exchange on page 496.

Key Exchange

1. Upload your ES key to the bank server.
   a) On the mailbox **EBICS** tab, click **Upload My Keys**.
   The **Uploading My Keys** dialog box appears.
   b) In the **Order Type** field, select **Upload ES Key (INI)**, and then click **Execute**.
   The message pane displays information regarding the INI transaction.
2. Upload your signing (X002) and encryption (E002) keys to the bank server.
   a) On the mailbox **EBICS** tab, click **Upload My Keys**.
   b) In the **Order Type** field, select **Upload Signing and Encryption Keys (HIA)**, and then click **Execute**.
   The message pane displays information regarding the HIA transaction.

   Note: Once the INI and HIA transactions have been successfully completed, the bank server should reject repeated attempts to transmit keys via INI and HIA. If you attempt this, you should receive `EBICS_INVALID_USER_OR_USER_STATE` from the server. To update your keys, use the PUB, HCA, and HCS orders through **Upload My Keys**.
3. Download the bank's keys for signing (X002) and encryption (E002).
   a) In the mailbox **EBICS** tab, click **Download Bank Keys**.

The message pane displays information about the HPB transaction.

Now you are ready to issue upload orders through the `PUT` command and download orders through the `GET` command. See EBICS Command Reference on page 489. You can also issue any of the ancillary orders through the mailbox **EBICS** tab **Execute Ancillary Order** function. For information about how to send and receive a test file, see Send and Receive a Test File on page 497.

Send and Receive a Test File

In the **Action** tab, run the <test> action. Executing the <test> action will send a sample file through an `FUL` order and then receive the same file through an `FDL` order type. See EBICS Action: Action Tab on page 488 for more information.

HSP Hosts

The generic HSP host is provided to allow a user to fully specify a client file transfer interface to an HSP server. If at all possible, use a pre-configured host specific to the target server; this will save the effort of having to research, specify, and then debug the interface.

The following action commands are available in the Cleo Harmony application:

	Command	Purpose	Underlying HSP method
Host commands	PUT	Send one or more files to the host	POST
Local commands	SET	Change an action property value	-
	CLEAR	Clears an action string property value	-
	SYSTEM	Execute a local system command	-
	WAIT	Pause	-
	LCOPY	Copy one or more local files	-
	LDELETE	Delete one or more local files	-
	LREPLACE	Replaces bytes in one or more local files	-
	CHECK	Check for a transfer, file, or directory (VLTrader and Harmony only)	-
	SCRIPT	Execute a JavaScript File (VLTrader and Harmony only)	-

HSP configuration tips

HSP transfer speeds are limited by certain configurations, including certain system settings, network card configuration and hardware (CPU, RAM, disk and network card). For Windows systems, transfer speeds are also influenced by whether Windows is running as a standalone instance or on a VM.

These tips can help you improve your system's transfer speeds.

Running in a VM

If you are running the Cleo Harmony or Cleo VLTrader application in a VM, use Linux for the HSP receiver where possible. If using Linux is not feasible, use the most recent version of Windows Server (with up-to-date drivers from the VM provider) for the HSP receiver.

Network card configuration

If running the Cleo Harmony or Cleo VLTrader application in either a VM or a native OS, ensure that your network cards support Receive Side Scaling and that Receive Side Scaling is enabled in the network card configuration. If

Receive Side Scaling is not enabled, individual HSP channels will not be able to scale, that is, increase the amount of data it is capable of receiving over time, which results in slow overall transfer speeds.

Windows-specific configuration

- Ensure that Windows has downloaded and applied the latest Windows updates
- Ensure the following network configuration parameters are set correctly.

  Note: You can view your current network configuration by opening a command prompt and running this command as administrator: `netsh int tcp show global`

  Receive Window Auto-Tuning Level

  Set the value of this parameter to `normal`.

  Open a command prompt and run this command as administrator:`netsh int tcp set global autotuninglevel=normal`

  Receive-Side Scaling State

  Set the value of this parameter to `enabled`.

  Open a command prompt and run this command as administrator:`netsh int tcp set global rss=enabled`

HSP Configuration

A host is configured using parameters that specify its location and how it is reached.

First activate either a trading partner-specific host or the generic HSP preconfigured host. The generic HSP host provides an interface over non-secure HSP or Secure Socket Layer (SSL) over HSP.

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including a mailbox and actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, you can append the new active host alias with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.

4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See HSP host configuration on page 500.
   c) Click **Apply** to save your work.
5. Enter mailbox-level configuration information.
   a) Click the mailbox under your host in the tree pane.
   b) Enter mailbox-level configuration information on the tabs in the content pane. See HSP mailbox configuration on page 510.
   c) Click **Apply** to save your work.
6. Enter action-level configuration information.
   a) Click an existing mailbox action to display its configuration tabs. Alternatively, right-click the mailbox and select **New Action**.
   b) Edit action information on the tabs in the content pane. See HSP Action on page 511.
   c) Click **Apply** to save your work.

7. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the native UI to prompt to you click **Apply** when changes are made. See Other system options on page 729. However, in the web UI, this is not valid. In the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

HSP host configuration

A host is configured using parameters that specify its location and how it is reached.

HSP Host: General Tab

Server Address

The address where your trading partner's server receives requests. Either a fully qualified name (recommended) or an IP address.

Port

The port where your trading partner's server receives requests. You can specify either a specific port number or `-1` to indicate the default port for HTTP (80) or HTTP/s (443).

Connection Type

The kind of connection you want to use for this host.

Possible values:

- `System Default` - See for information about setting the system default.
- `Direct Internet Access or VPN` - Use either a direct connection to the internet or a VPN.

Default value: `System Default`

Forward Proxy

The address of the forward proxy you want to use for this host.

Select the **System Default** check box to use the default proxy. See Configuring for a proxy on page 881 for information about specifying a default proxy.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For VLTrader and Harmony, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and/or Outbox. See Specifying default host directories on page 700and Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Note: Specifying a value in the **Sentbox** field could result in slower transfer times.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Note: Specifying a value in the **Receivedbox** field could result in slower transfer times.

Possible values: Any local or shared directory.

Default value: No default value.

HSP Host: HTTP Tab

Use the **HTTP** tab to provide information about how your HSP host uses HTTP and HTTP/s.

Outbound

HTTP

HTTP/s

If the HSP server requires use of the Secure Socket Layer (SSL), select **HTTP/s**. Otherwise, select **HTTP**.

Check certificate server name

Indicates the system should verify that the server name in the received SSL server certificate matches the server name connected to.

Inbound

HTTP/s only

Require your trading partner to use Secure Socket Layer (SSL) for inbound file transfers.

Command

The commands supported by the server. In this case, the `PUT` command.

Method

The methods unlying the the supported commands.

Path

The server **Path** for the `PUT` command. The **Path** depends on your trading partner's server **Resource Path** configuration defined in their HSP Service Panel. See Local Listener HSP Service on page 774.

Parameters

Headers

Add custom **Parameters** and additional **Headers** as needed. The values for these fields are available on the receiving side either through the properties passed to the `ILexiComIncoming` Java API OR by accessing `ISessionScript.getTrigger()` in a JavaScript action scheduled for a new file arrives event.

HSP Host: Advanced Tab

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Properties available for HSP include:

Add Mailbox Alias Directory to Inbox

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Receivedbox

Appends a subdirectory at the end of the host's configured receivedbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Sentbox

Appends a subdirectory at the end of the host's configured sentbox directory. This allows files that have been sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Buffer Size (kbytes)

The size of the data blocks (in kbytes) used to transfer the message over each channel.

Possible values: `1 - n`

Default value: `32`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0 - n`

Default value: `0`

Connection Timeout

The amount of time allowed for each read operation.

Possible values: `0 - n` seconds

`0` indicates no timeout

Default value: `150` seconds

Do Not Send Zero Length Files

Indicates whether zero length files to be sent to the server should be ignored rather than processed. If the `-DEL` option is being used, any zero length file ignored will also be deleted.

Possible values: `On` or `Off`

Default value: `Off`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the

failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

Integrity Algorithm

When `NONE` is not specified, the content of the message will be hashed using the desired algorithm when sending and will be verified by the HSP using the same algorithm to validate the content has not been changed while in-transit.

Possible values:

`NONE`
`MD5`
`SHA`
`SHA256`

Default value: `NONE`

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Minimum Size Per Channel (kbytes)

Reduces the number of requested channels depending on the overall size of the file. This helps balance the efficiency of the protocol for small files. If the file is smaller than the value you set, a single request is used to transfer the file.

Default value: `1024`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

`System Default`

`Alphabetical`
`Date/Time Modified`

Default value: `System Default`

Partner Email Address

The email address of the trading partner for this trading relationship. When set, this address is automatically used to send your local profile information and/or certificates to your trading partner. See Emailing a profile to your trading partner on page 87.

Possible values: Email address(es) separated by commas (,), semicolons (;) or colons (:).

Note: This is a Cleo LexiCom only option. For Cleo Harmony and Cleo VLTrader, this information is stored in the trading partner management table. See Managing Trading Partners on page 631.

Reset Connection After Timeout On Response

When enabled will cause an immediate reset on the socket (instead of a graceful close) when a `SocketTimeoutException` occurs.

Possible values: `On` or `Off`

Default value: `Off`

Resume Failed Transfers

When selected and a transfer fails (and Command Retries > 0), attempt to resume the transfer on a retry. If OpenPGP is enabled on the packaging tab (see Configuring mailbox packaging on page 79), the entire file is transferred instead of resuming with a partial file. The server must support the `FEAT`, `SIZE`, and `REST STREAM` extensions to FTP. For more information, visit http://tools.ietf.org/html/rfc3659.

Possible values: `On` or `Off`

Default value: `Off`

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

Reuse SSL Sessions Across Actions

If selected, and if no forward proxy is being used for this host, SSL sessions from previous connections to the same destination (address and port number) may be resumed to avoid costly negotiation. If unselected, only SSL sessions used in the current action to the same destination may be resumed. When unselected, a new SSL session is created for the initial command port connection.

Possible values: `On` or `Off`

Default value: `On`

SSL Allow Legacy Renegotiation

When selected, legacy renegotiation is allowed. If this property is not selected, the extension described in RFC5746 is used for renegotiation and the server must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Possible values: `On` or `Off`

Default value: `On`

SSL Cipher

Indicates a specific cipher, or an ordered list of ciphers, to be used with the server for SSL key exchange, encryption, and hashing.

If not set (that is, left blank), the list of default ciphers (all standard ciphers, excluding anonymous and non-encrypting) is presented to the server and the server picks one. If a regular expression (enclosed in brackets) or a wildcard expression is specified, a list of implemented ciphers (all standard ciphers, including anonymous and non-encrypting) is presented to the server, based on the conditions of the pattern. For example, if a regular expression of `[.*ECDH.*]` is specified, then the list is a subset of all implemented ciphers that belong to the Elliptical-curve Diffie-Hellman group (for example, `ECDH` is in included in their string). In all cases, whenever a list is presented, it is always ordered by cryptographic strength, with the strongest listed first.

Based on the expression you type, the **List** button shows the resulting set of ciphers in the **SSL Cipher List** dialog box. Within this dialog box, you can view the list or select a specific cipher. If you select a cipher, then its value is displayed in this field.

Possible values:

Blank
a specific cipher picked from the SSL Cipher List dialog box
a regular/wildcard expression

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed. By default, this field is blank, designating that Cleo Harmony, Cleo VLTrader, or Cleo LexiCom will select the most recent version (currently TLS 1.3).

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed when selecting an SSL cipher. To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128`, or `256` (depending on the requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed. SSL 3.0 is the default value for compatibility with servers that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

Possible values:

```
SSL 3.0
TLS 1.0 (SSL 3.1)
TLS 1.1 (SSL 3.2)
TLS 1.2 (SSL 3.3)
TLS 1.3
```

Default value: `SSL 3.0`

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`

4
3
2
1
0 - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

HSP mailbox configuration

Configure a mailbox using parameters that allow access to the host system.

HSP Mailbox: HTTP Tab

In the mailbox's **HTTP** tab, the parameters and headers listed are those identified in the host **HSP** tab that do not have static values or special `%file` and `%dir` associations.

Provide **Default Values** for any of the parameters and headers for which it makes sense at the mailbox level. Unless an overriding value is specified within the command in an action, the default value specified here is used.

HSP Mailbox: Certificates Tab

Unlike other protocols that use signing certificates, the HSP protocol requires that a unique partner signing certificate be defined for each trading relationship. If multiple mailboxes are created for the same trading partner, a different partner signing certificate must be assigned to each mailbox.

The **Certificates** tab allows you to associate a trading partner's signing certificate with this mailbox and override your own Local Listener's signing certificate as necessary.

Prior to completing this tab for HSP mailbox, you must acquire your trading partner's signing certificate and create and/or provide to your trading partner your signing certificate.

Trading Partner's Certificates

Signing Certificate

The unique partner signing certificate for this mailbox.

Specify a value or click **Browse** to navigate to the file containing the trading partner's Signing Certificate.

My Certificates

Override Local Listener Certificates

Enables fields where you specify a signing certificate to use instead of the certificates you configured for the Local Listener. See Configuring certificates for Local Listener on page 758.

If you override the default certificates, you must also exchange the certificates you specify here with your partner.

Signing Certificate Alias

Password

The name of your signing certificate.

Specify a value or click **Browse** to navigate to and select a certificate. Enter the **Password** for your signing certificate's private key.

Overriding HSP Local Listener Certificates

By default, the signing certificate configured on the **Certificates** tab of the **Local Listener** panel will be the certificate used to authenticate messages sent to your trading partner. See Configuring certificates for Local Listener on page 758.

Use **Override Local Listener Certificates** to select alternate certificates for signing and decrypting messages with this trading partner. If you override the default certificates, do not forget to export and exchange these alternate certificates with your trading partner.

HSP Action

An action's parameters capture a repeatable transaction for your mailbox on the host system.

HSP Action: Action Tab

Use the HSP Action's **Action** tab to compose actions for the HSP mailbox.

Any commands specified in the host **HSP** tab (as well as the local commands) are available for use. See Composing an action on page 89. See also HSP Command Reference on page 511.

Note: If a parameter or header value has an embedded space, a `\s` must be used to represent the space within the command (e.g. `%OPQ\scompany` represents `%OPQ company`). This is done automatically in the dialog editor. If a space is left in the value, the command is not parsed correctly.

HSP Command Reference

CHECK

See CHECK Command for information about this command.

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

HSP Comment

```
#text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be a filename or a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.

- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

PUT

Send one or more files to the host.

```
PUT -DEL -UNI "source" "destination" name=value,...
```

-DEL

If the `PUT` is successful, delete the local file.

-UNI

Ensure the host filename is unique.

If the underlying HSP method for the command on the server is POST, this argument is not applicable and cannot be used. See HTTP Configuration on page 121 .

"*source*"

Local source path.

- Path can be to a filename or to a directory.
- `*` and `?`, or a regular expression, are supported in filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, it uses default outbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.

If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Remote destination path

If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

name=value,...

HSP parameter=value and header=value pairs

If the underlying HSP method for the command on the server is POST, then the argument is not applicable and cannot be used. See HTTP Configuration on page 121.

SCRIPT

See SCRIPT command on page 951 for information about this command.

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"path"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

Users Host

When you start your FTP/FTPs, SSH FTP, HTTP, or Cleo Portal (HTTPs) server for the first time, no Users exist and therefore no access is granted to your server. To initiate creation of Users, first activate the Users template (see Activating a host from a template on page 77) and then add a new user mailbox.

User mailboxes can have actions, but unlike remote host/mailbox actions that perform remote host operations, User actions can only perform operations that manipulate files within the user's home directory.

Users can be native users, LDAP users, Connector Host-authenticated users, or SAML-authenticated users.

Note: If you have an Administrator user configured in Cleo VLNavigator and a Users host user configured in Cleo Harmony or Cleo VLTrader with the same username, you might experience issues logging in to your system with the Adminstrator user. To resolve possible issues, you can rename or remove the Users host user or change the configuration of the Users host user to use VLNav Connector Host authentication.

Users host configuration

Members of a Users group share the same privileges and policies; however, usernames must remain unique across all user groups.

Users: General Tab

Home Directory

Select the check box to activate the **Home Directory** field, all of the user folders and the archive directories specified on this tab, and the FTP and SSH FTP protocols (see Users: Privileges Tab on page 517). Clear the check box to deactivate them. The check box is selected by default.

Use the **Home Directory** field to specify the default home path for each user in the group. The `%username%` macro, which resolves dynamically, is included in the path. You can override this path, however, using settings in the mailbox **Login** tab. See Users Mailbox: Login Tab on page 530.

Click the **[...]** button to browse and select a directory. Alternatively, select a custom macro variable from the drop-down menu. See Using Macro Variables (Default Root Directory context) for a list of the applicable macros. Once the change is applied, users that are already configured to use the default home are switched over to the new default home location.

You can use the home connector syntax to copy files to and delete files from a user folder. See Home connector on page 529.

You cannot specify a virtual subfolder for the home directory.

Optionally, you can specify folder-level permissions and file-level permissions to a home directory. Add permissions in parentheses at the end of the value in the **Home Directory** field. Permissions applied to the home directory apply only to the home directory.

Possible permissions include:

- `ALL` - User has all permissions. This is the default value.
- `LIST` - User has permissions to list the contents of a folder.
- `MKDIR` - User has permissions to make a directory.
- `MVDIR` - User has permissions to move a directory.
- `RMDIR` - User has permissions to remove a directory.
- `READ` - User has permissions to read a file.
- `WRITE` - User has permissions to write a file
- `OVERWRITE` - User has permissions to overwrite an existing file
- `RENAME` - User has permissions to rename a file
- `DELETE` - User has permissions to delete a file

For example, use this syntax to specify a home directory with `LIST` and `WRITE` permissions.

```
local\root\%username%(LIST,WRITE)
```

User Folders

The paths and names of folders for users of this group. These folders are automatically created under each user's home directory. You can use relative paths and configure virtual subfolders. See Virtual subfolders on page 528.

User Download Folder

User Upload Folder

The folders used by users in this group for downloading and uploading files.

You can modify this value in this context, but you cannot modify it at the user level.

Note: The configured user upload and download folders reflect the perspective of the *user*, while the `%inbox%` and `%outbox%` macros (if used elsewhere) reflect the perspective of the *server*. This means that the `%outbox%` macro resolves to the configured user *download folder* and the `%inbox%` macro resolves to the configured user *upload folder*.

Note: If **Archive Directories** are configured, files uploaded to the **User Upload Folder** are archived to the **Archive Directories/Receivedbox** and files downloaded from the **User Download Folder** are archived to the **Archive Directories/Sentbox**.

Other Folders

You can specify additional folders in the **Other Folders** field. You can add multiple paths (one path per line) to the **Other Folders**. All paths must be relative or use virtual subfolders and cannot include reserved macro variables (for example, `%mailbox%`). You can, however, use `%username%` in a virtual subfolder link.

If you need to add real or virtual subfolders on a per-user basis, use the **Add Folders** button on the **Users Mailbox** > **Login** tab. See Users Mailbox: Login Tab on page 530.

Not only can you modify this value in this context, you can also modify it at the user level.

Note: Files sent to or received from these folders are not archived.

Archive Directories

The location where you can save a copy of the sent and received files.

Click the **[…]** button to browse to and select a valid local or network location. Alternatively, select a custom macro variable from the drop-down list. See Using macro variables on page 59 (Default Local User Archive Directory context) for a list of the applicable macros. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables. Typically, the archive directory locations are set up outside of the Home Directory path to protect the archives from access by the configured users.

You can use the `%mailbox%` macro as part of these directory definitions to filter files for non-LDAP users into separate subdirectories. Files written to these directories are retained with unique file names and are archived if the **Sent/Received Box Archive** option is enabled on the **System Options** > **Other** tab. See Other system options on page 729.

You cannot specify a virtual subfolder for the archives directory.

Note: Only files sent to or received from the **User Upload Folder** and **User Download Folder** are archived.

Users: Privileges Tab

The following describes the **Privileges** tab.

Protocols

Specify which protocols are enabled for this user group.

Possible values: `FTP`, `SSH FTP`, or `HTTP`

Access

Specify the type of access enabled for this user group.

Possible values:

- `Read access` - Download files only.
- `File access` - Download, upload, modify, and delete files.
- `Full access` - Download, upload, modify and delete files; create, modify, and delete folders.

View Transfers

Select this check box to allow Cleo Portal users belonging to this group to view the **Transfers** tab.

Two-Factor Authentication

Select this check box to allow users belonging to this group to use two-factor authentication when autheticating to Portal.

Invitations

Use this section to configure users in this group to invite other users.

Invite unregistered users

Select the check box to allow the users in this group to invite other users into the system and enable the **Assign invited users to** field.

Assign invited users to

Select the group to which new users are invited by this group's members. You can choose any of the groups to which you have access.

Once added, the new users will have the privileges of the group to which they are invited.

Users: Policy Tab

The following describes the **Policy** tab.

Password Policy

The Password Policy defines the requirements and restrictions for passwords for local users. By default, the Password Policy used by all mailbox users is globally defined using the **Enforce Password Policy** option on the **System Options > Other** tab. See Other system options on page 729.

To specify a different set of password requirements and restrictions for all mailbox users defined for a particular local Users:

1. Select **Override System Settings** and click **Edit** to display the Password Policy dialog box.
2. Select **Enforce the following password rules** to make the fields in the dialog box editable and to activate the password rules you configure.
3. Modify the settings as needed, and click **OK**. See Configuring password policies on page 55 for detailed information about Password Policy options.

Security Policy

The Security Policy restricts incoming messages based on certain attributes.

Require IP filtering

Require all users of this group to log in from one of the whitelist IP addresses, as specified in each user's IP Filter tab. If the **Require IP filtering** check box is cleared, whitelist IP addresses are not required for the users

of this group, and the users can log in from anywhere. See Configuring IP filtering on page 886 for more information.

Disallow unsecured FTP

Limits users to SSL connections only. When selected, users can successfully authenticate only when an FTP/s or HTTP/s connection is used. (SSH FTP connections are always secure.)

Restrict file patterns

Patterns that files must match to be permitted inbound. Patterns can include wildcards and regular expressions. See Using wildcards and regular expressions on page 69. If you specify multiple file patterns, separate them with semi-colons (;) or commas (,). Alternatively, enter them on separate lines. Examples of valid patterns include:

- `*` – any file pattern
- `*.*` – file must have an extension
- `*.edi;*.xml` – only .edi and .xml extensions acceptable (case sensitive)
- `[(?i).*\.(edi|xml)]` – only .edi and .xml extensions acceptable (case insensitive)

Users: Advanced Tab

This section provides information about properties specific to Users. See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols.

Active Mode Source Data Port (FTP)

Specifies the FTP server source data port for Active Mode FTP when set to a value > 0. Default value is 0 where the data port is unspecified. Some FTP clients may require a specific port number (for example, 20) be used for the server data port.

Automatically Delete Retrieved Outbox Files (FTP)

When this option is selected, delete (remove) each file retrieved from the **User Download Folder** when the next FTP command is received from the client for a given FTP session. Files will only be deleted from the **User Download Folder** after retrieval from the defined **User Download Folder** or its subfolders. The delete confirmation response will be contained in a multi-line response (for example, 150-Retrieve of 'test.edi' confirmed…) for the next appropriate client command.

Possible values: `On` or `Off`

Default value: `Off`

Client Type (HTTP)

Indicates a specific HTTP client that requires special processing of the inbound message. The default value is **no** specified client type. Choose from Oracle Transport Agent or cXML.

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Repetitive Listener Failures

When "Email On Fail" is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, an email alert will be sent when the failure is resolved. Failure resolution email alerts will not be sent for general Listener failures since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Repetitive Listener Failures

When `Execute On Fail` is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, the `Execute On Fail` command will be executed again when the failure is resolved. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure. Executions of the "Execute On Fail" command for resolution of general Listener failures will not be done since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

- `\r` - carriage return
- `\n` - new line (linefeed)
- `\f` - form feed
- `\t` - horizontal tab
- `\0` - null
- `\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0 - n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

FTP Session Timeout

Specifies the maximum time (in minutes) that a user can be logged in to an FTP/SSHFTP session before being logged out of the system.

Default value: `-1` - Indicates the user will not be logged out.

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Ignore Exception Without Quit (FTP)

When this option is selected, FTP disconnect exceptions related to the client closing the connection abruptly without issuing a QUIT command will be suppressed.

Possible values: `On` or `Off`

Default value: `Off`

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

Interim File Extension (FTP, SSH FTP)

When applicable, specifies the temporary filename extension that a trading partner's FTP or SSH FTP client software uses while transferring a file. For the transfer logging feature, the Cleo Harmony application sets the transfer status to `Interim Success` rather than `Success` when a transfer with a temporary filename extension is finished. Then, when the trading partner client software renames the file to strip off the temporary filename extension, the application inserts an additional `Success` entry into the transfer log with the resulting filename to mark the transfer as complete. The dot preceding the extension can be included in the configured value, but it is not required. If multiple temporary filename extensions are used, they can be separated by commas or semicolons.

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Concurrent FTP Logins (FTP, SSH FTP)

The total number of logins allowed at any one time per user on FTP or SSH FTP (separately). With the default value of 0, the number of concurrent connections per user will be limited by the **Maximum Concurrent**

FTP Logins Per User setting in the Local Listener. A value other than zero will override the Local Listener **Maximum Concurrent FTP Logins Per User** setting.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512
```

Default value: `System Default`

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: `On` or `Off`

Default value: `On`

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: `On` or `Off`

Default value: `On`

PGP V3 Signature

Prefix SSH FTP Home Directory Path

Adds `/home/<username>` to the path displayed to the user.

Possible values: `On` or `Off`

Default value: `Off`

Request and Response Events

Indicates where FTP and SSH FTP user session request and response events should be captured. For high-volume systems, not logging these events may help with overall system performance.

Possible values: `Log`, `Debug`, or `None`

Default value: `Log`

Trigger At Upload Completion (FTP)

Select this property to indicate a trigger should be created when a file upload is completed successfully. This property applies only to files transferred using FTP. The trigger is created when the next command is received after the file upload.

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Use External IP Address In PASV Response (FTP)

Indicates, for passive (pasv) mode, that the external address (rather than the local IP address) should be included in data port response to the FTP client.

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

`System Default`
`TripleDES`
`AES-128`
`AES-192`
`AES-256`

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The

name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

Virtual subfolders

You can configure virtual subfolders as part of the **User Download Folder**, **User Upload Folder** and **Other Folders**.

Syntax

Use this syntax to specify virtual subfolders:

```
virtualFolderName=actualFolder(permissions)
```

`virtualFolderName`

The name displayed to the user.

`actualFolder`

An absolute path, a relative path, a UNC path, or a connector URI path (with optional connector parameters) to the actual folder.

`permissions`

Optional.

A list of permissions governing the virtual folder. You can specify folder-level permissions and file-level permissions.

You can specify multiple permissions separated by commas. For example, `(LIST,READ,WRITE)`.

Permissions applied to a subfolder apply to the subfolders and all files and folders under that subfolder.

Possible values:

- `ALL` - User has all permissions .
- `LIST` - User has permissions to list the contents of a folder.
- `MKDIR` - User has permissions to make a directory.
- `MVDIR` - User has permissions to move a directory.
- `RMDIR` - User has permissions to remove a directory.
- `READ` - User has permissions to read a file.
- `WRITE` - User has permissions to write a file
- `OVERWRITE` - User has permissions to overwrite an existing file
- `RENAME` - User has permissions to rename a file
- `DELETE` - User has permissions to delete a file

Default value: `ALL`

Examples

URI using system scheme name for a File connector

```
localserverfilesA=myfiles:
```

URI using a system scheme name for a SMB connector and a subdirectory:

```
remoteserverfilesABC=mysmb:/sub1/sub2
```

URI using an SMB connector overriding the Share Path based on the username:

```
MyHome=Smb:SmbHost?smb.SharePath=//filsvr01/users/home/%username%
```

URI using a S3 connector:

```
s3bucket=S3:S3-Prod
```

Using absolute path (local Linux VersaLex server):

```
archivedata=/opt/datadir/archive/companyx/
```

Using relative path (relative from VersaLex installation directory):

```
recs=home/install_records/
```

Using UNC path:

```
fileserver=\\fileserver01\public\data\
```

User Download Folder:

```
fromClar=clarify:Clarify202/Clarify-AS2-Outbound/fromclarify(LIST,READ)
```

User Upload Folder:

```
toClar=clarify:Clarify202/Clarify-AS2-Outbound/toclarify(WRITE)
```

Other Folders:

```
MyHDFS=hdfs:HDFSTest(LIST,READ,WRITE)
```

```
MyS3=S3:S3Test\sub1(LIST,READ,WRITE,MKDIR,RMDIR)
```

Home connector

Use the home connector to copy files to and delete files from a user folder.

Syntax

Use this syntax to specify a user's home directory.

```
home:username/path
```

username

The login username.

path

A path relative to the user's home folder. This value can be an actual path or a virtual folder path.

Examples

Copying files into a user subfolder

```
LCOPY *.edi home:/user1/S3Share
```

```
LCOPY *.edi home:/user1/subfolder1
```

Deleting files form a user subfolder

```
LDELETE home:/user1/S3Share/text.*
```

Users mailbox configuration

A user mailbox's settings establish the identity of a user or an LDAP subgroup.

Users Mailbox: Login Tab

Status

The **Status** field provides the current account status. Generally, this display is read-only. If, however, the account is locked due to multiple invalid login attempts (see Configuring password policies on page 55 for detailed information about Password Policy options), the **Unlock** button appears.

When an account is locked, you can wait for the lock duration to expire or click **Unlock** and then click **Apply** to reset the account immediately.

Authentication

Select the type of authentication you want to configure for this mailbox. This section displays different fields depending on the type of authentication you choose.

Default User

Select this option to use default authentication.

User ID

This value comes from the **User** field at the top of the **Mailbox** window. In the **User** field, enter an alias not already in use.

This field is required.

Password

The user's password.

This field is required.

SSH Key(s)

This field is applicable to SSH FTP only, and it is optional. If specified, this user, if logging in through SSH FTP, must use his user ID and one of the SSH key(s) to authenticate

Allow password or SSH Key authentication

Select this check box to allow password or public key to be used for authentication in User hosts for SSHFTP.

Require both

Select this check box to require both a password and public key be used for authentication in User hosts for SSHFTP.

Email address

When the user requests a password reset, a personal URL (PURL) is sent in an email to this address. The user can click this PURL to begin the process of resetting their password. This email address must be unique across the Cleo Harmony system.

Note: If you select the **LDAP** check box, this field is not available. In order for this user to receive password reset email, the LDAP email attribute must be set in the LDAP User Configuration screen. See User configuration reference on page 695.

This field is required.

System LDAP

Select this option to use LDAP authentication.

Override System Options

Select this option and then specify a **Base DN** in order to match the intended set of users for this mailbox. Or the **Extend Search Filter** can be used to append rules to the default system search filter. See LDAP server on page 691.

Override System Setting

Select this option to disable the **Extend Search Filter** field and then specify a **Search Filter**.

Extend Search Filter

Specify a value used to append rules to the default system search filter. This field is disabled if you select the **Override System Setting** check box.

List

Displays a list of users and their attributes matching the values you specified in the **Base DN** and **Search Filter** filters.

Connector Host

Select this option to use the authenticator API in the connector host, allowing Cleo Portal, FTP, and SFTP users to be provisioned and authenticated through an interface with another system, for example a CRM application.

Authenticator

Enter the URI of the connector host you want to use for authentication. Specify the URI as `scheme:alias`.

SAML User

Select this option to allow authentication via SAML.

Email Address

Enter the email address that identifies the user of this mailbox in SAML.

Home Directory

Select an option from the drop-down list.

- **Default Home** - Use the value specified in the **Home Directory** field for the user group. See Users: General Tab on page 516.
- **Custom Home** - Specify a home directory. You can browse your system and select a home directory or enter a directory path manually. Alternatively, you can select a custom macro variable from the drop-down menu. See Using macro variables on page 59 for a list of the applicable macros (Default Root Directory context).
- **LDAP Home** - Use the value specified for the LDAP group specified. Available only if LDAP is selected.

Add Folders

Click **Add Folders** to display the **Local User Subdirectories** dialog box. This dialog box displays host-level settings (read-only) for the current folder configuration and allows you to specify additional real or virtual subfolders at the mailbox level in the **Mailbox-level Settings** > **Other Folders** field. You can add multiple paths (one path per line) in the **Other Folders** field. All paths must be relative or use virtual subfolders and cannot include reserved macro variables (for example, `%mailbox%`). You can, however, use `%username%` in a virtual subfolder link.

Use the following format to specify the virtual subfolders: `virtualFolderName=actualFolder` where `virtualFolderName` is the name displayed to the user and `actualFolder` is an absolute path, a relative path, a UNC path, or a connector URI path. See Virtual subfolders on page 528.

To add folders at the host level, go to the **Users** > **General** tab. See Users: General Tab on page 516.

Users Mailbox: Activity Tab

Note: For LDAP or Connector Host authentication users, Activity Dates represent the most recent date from any user defined in the mailbox.

The Activity tab displays a table of information about login and transfer activities for the Mailbox. Each row in the table contains the following columns.

Activity

Displays the type of activity, for example, FTP Login or FTP Transfer.

Date

Displays the date of the most recent activity.

Other possible values:

No Activity

Indicates the user was created after the Activity tab functionality was introduced and there is no activity to report for this user.

Unknown

Indicates the user existed before the Activity tab functionality was introduced and there is no activity to report.

Days

Displays the number of days since the last activity.

Users Mailbox: IP Filter

The IP addresses you specify here are the only addresses that will be allowed to log into the user mailbox.

1. Go to the **IP Filter** tab for your user mailbox.
2. Click **New** to create a new entry or double-click an existing entry to edit it. Alternatively, you can right-click on the entry and select **Edit**.
3. Enter an IP address to be added to the whitelist.

   You can use both IPv4 and IPv6 addresses. IP addresses can be a single address or a range of addresses. The following are examples of valid IP addresses:

IP Address	Description
*	All IP addresses
10.11.12.13	Single IPv4 address matching 10.11.12.13
10.*	IPv4 addresses in the range 10.0.0.0-10.255.255.255

IP Address	Description
10.11.*	IPv4 addresses in the range 10.11.0.0-10.11.255.255
10.11.12.50-10.11.12.70	IPv4 addresses in the range 10.11.12.50-10.11.12.70
fe80::79ba:8815:4f62:e386	Single IPv6 address matching fe80::79ba:8815:4f62:e386
fe80::79ba:8815:4f62:e386-fe80::79ba:8815:4f62:ffff	IPv6 addresses in the range fe80::79ba:8815:4f62:e386-fe80::79ba:8815:4f62:ffff
fe80::79ba:8815:4f62:e386/90	IPv6 addresses matching the first 90 bits of address fe80::79ba:8815:4f62:e386

4. Click **Apply**.
5. Optionally, remove an entry by right-clicking it and selecting **Remove**.

Users Mailbox: Packaging Tab

See Configuring mailbox packaging on page 79 for information regarding payload file packaging.

User Action

An action captures a repeatable local procedure relative to the user mailbox.

1. Right-click the mailbox under the host in the active tree pane.
2. Select **New Action** to create a new action. Then, if desired, type a new alias in the content pane panel and click **Apply**.

Users Action: Action Tab

Use the **Action** tab to configure commands within an action.

See Composing an action on page 89. Also see Local command reference on page 876.

Users Command Reference

See FTP Command Reference on page 113, HTTP Command Reference on page 139, and SSH FTP Command Reference on page 276 for information about the server commands available to the users of this user group.

Connector Host

You can create connector hosts in the Cleo Harmony and Cleo VLTrader applications only.

Connector hosts all have the same general structure, which is slightly different from the other host types. Connector hosts do not have mailboxes. In addition, all properties specific to the connector type are segregated from other advanced properties. Several connector hosts ship with the product and are available in the **Templates** tree, including SMB, Clarify, EEI, File, S3 (Cleo Harmony only), HDFS (Cleo Harmony only), and LDAP. The SMB, Clarify, EEI, File S3, and HDFS connectors are all *data connectors*. The LDAP connector is an *authentication connector*, which is different from the rest.

A *data connector host* can be accessed from another host inbox or outbox or as the source or destination of a command by using one of the following URI syntaxes:

Long Form

```
scheme:host/subdir/filename?name=value
```

where,

- `scheme` is the scheme name built into the connector, sometimes named after a protocol. For example, SMB.
- `host` is the alias assigned to the active connector
- `subdir` and `filename` are optional depending on use case
- `name=value` is optional and can be used to override any connector or advanced properties. These properties temporarily override properties set in the connector host only during the use of the URI file instance.

Short Form

```
sysscheme:/subdir/filename?name=value
```

where,

- `sysscheme` is the value of the System Scheme Name property as set under the connector properties tab
- `subdir` and `filename` are optional depending on use case
- `name=value` is optional and can be used to override any connector or advanced properties. These properties temporarily override properties set in the connector host only during the use of the URI file instance.

These powerful constructs allow you to move data seamlessly across hosts and connectors.

An *authentication connector host* can be accessed through a Users' mailbox by selecting the **Connector Host** authentication type. The same URI syntax applies as above; however, the optional subdir and filename path would never be applicable for an authentication connector.

There are specific rules for URI accessibility. The connector must be located within the same branch as the host for access to be granted, but there are special rules for the root host folder:

- If the connector is in the root host folder, any host in any folder can access it via a URI. But a host in the root host folder can only access connectors also in the root host folder.
- Otherwise, the connector must be in the same host subfolder or below for it to be accessible from the host.

Examples of using an URI as Inbox and Outbox

The data connector URIs are typically used as the Inbox and/or Outbox locations for other hosts. This section contains examples of using connector URIs as inboxes and outboxes.

Examples of URIs configured as the host Inbox

`smb:MyServer/partner1/inbox`

Stores incoming files to an SMB/CIFS file server in the `partner1/inbox` folder under the share path folder. The name of the file server, login credentials, and share path folder are defined in the `MyServer` SMB connector.

`clarify:Prod/%host%/toclarify`

Sends incoming files directly to the Cleo Clarify system(s) configured in the `Prod` Clarify connector. These files are tagged as coming from the current host alias (`%host%`). This URI scheme should be used for all Inbox configurations sending directly to Clarify. No sub-path should be specified after `toclarify`.

`eei:Prod/`

Sends incoming files directly to the Cleo EEI system configured in the `Prod` EEI connector host. This URI scheme should be used for all Inbox configurations sending directly to EEI. No sub-path should be specified after the connector alias (`Prod` in this example).

`file:MyRoot/partner1/inbox`

Stores incoming files on the file system in the `partner1/inbox` folder under the root path folder. The root path folder is defined in the `MyRoot` File connector.

`s3:MyS3/partner1/inbox`

Sends incoming files directly to the `partner1/inbox` folder object in an Amazon S3 bucket. The Amazon S3 login credentials, region, and bucket are defined in the `MyS3` S3 connector.

`hdfs:MyHDFS/partner1/inbox`

Sends incoming files directly to the `partner1/inbox` folder in a Hadoop Distributed File System (HDFS). The HDFS login credentials are defined in the `MyHDFS` HDFS connector.

Examples of URIs configured as the host Outbox

`smb:MyServer/partner1/outbox`

Retrieves outgoing files from the `partner1/outbox` folder under the share path folder on an SMB/CIFS file server. The name of the file server, login credentials, and share path folder are defined in the `MyServer` SMB connector.

`clarify:Prod/%host%/fromclarify`

Retrieves outgoing files from the Cleo Clarify system(s) configured in the `Prod` Clarify connector. Clarify files for the current host alias (`%host%`) are retrieved directly from Clarify. This URI scheme should be used for all Outbox configurations sending directly from Clarify. No sub-path should be specified below `fromclarify`.

`eei:Prod/partner1`

Retrieves outgoing files for `partner1` from the Cleo EEI system configured in the `Prod` EEI connector host. This URI scheme should be used for all Outbox configurations sending directly from EEI. No sub-path should be specified after the EEI partner name (`partner1` in this example).

`file:MyRoot/partner1/outbox`

Retrieves outgoing files from the file system in the `partner1/outbox` folder under the root path folder. The root path folder is defined in the `MyRoot` File connector.

`s3:MyS3/partner1/outbox`

Retrieves outgoing files directly from the `partner1/outbox` folder object in an Amazon S3 bucket. The Amazon S3 login credentials, region, and bucket are defined in the `MyS3` S3 connector.

`hdfs:MyHDFS/partner1/outbox`

Retrieves outgoing files directly from the `partner1/outbox` folder in a Hadoop Distributed File System (HDFS). The HDFS login credentials are defined in the `MyHDFS` HDFS connector.

Connector Configuration

A connector host is configured using parameters that specify its location and how it is reached.

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab to find the host you want to use.
3. Right-click the *host* and select **Clone and Activate**.

   The entire pre-configured *host* branch (including actions) is copied and activated, the **Active** tab is selected in the tree pane, and the new active *host* is selected in the tree. If necessary, the new active host alias is appended with a number to make it unique.

   Note: The original pre-configured host remains in the pre-configured tree.

4. Enter host-level configuration information.
   a) Click the new host in the tree pane.
   b) Enter host-level configuration information on the tabs in the content pane. See Connector Host Configuration on page 536.
   c) Click **Apply** to save your work.
5. Enter action-level configuration information.
   a) Click an existing host action to display its configuration tabs. Alternatively, right-click the host and select **New Host Action**.
   b) Edit action information on the tabs in the content pane. See Connector Host Action Configuration on page 544.
   c) Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the native UI to prompt to you click **Apply** when changes are made. See Other system options on page 729. However, in the web UI, this is not valid. In the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

Connector Host Configuration

The connector host parameters indicate a host's location and how to reach it.

Connector Host: General Tab

Use the **General** tab to specify information about folders and directories the host uses before, during, and after transfers.

Default Directories

Modify the default directories, if necessary. You can use macro variables from the drop-down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and example usage. For Cleo Harmony and Cleo VLTrader, see URI File System interface overview on page 955 for information about you can use a Cleo-provided or custom URI for the Inbox and/or Outbox. See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

Inbox

Default directory for incoming files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `%system%\`

Outbox

Default directory for outgoing files. Enter a value directly or click **…** to navigate to and select a directory.

Possible values: Any local or shared directory.

Default value: `%system%\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Note: `Sentbox` might not be available for all Connector Hosts.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies. Enter a value directly or click **…** to navigate to and select a directory.

Note: `Receivedbox` might not be available for all Connector Hosts.

Possible values: Any local or shared directory.

Default value: No default value.

Connector Host: Properties Tab

The label of the **Properties** tab reflects the name of the connector. When you activate a connector, it has connector properties for which you assign values, some of which are required. This tab is where you assign these values.

You can press **Help** to display a dialog box containing documentation for all connector properties.

Some properties have buttons associated with them that perform special functions. These functions vary from connector to connector. If a connector property is represented by a table of properties, click the **[…]** button to display a **Connector Property** table. See Connector Property table on page 537 for more information.

You can filter these properties using the filter options at the bottom of the table.

If you are using an authentication-type connector, you can use **Test Authentication** to enter a **Username** and **Password** to check against this connector. Optionally, click **List Users** to view a list of users who belong to this authenticator.

When you are satisfied with your changes, click **Apply**. You can click **Reset** to clear any information added or edited in this session.

Note: When using the URI syntax to access this connector host, some connector properties might overlap with properties of the originating host (for example, **Command Retries** or **Do Not Send Zero Length Files**). When this occurs, the property used (originating host or connector host) depends on the host making the decision. In the case of **Do Not Send Zero Length Files**, it is the originating host making the decision and that same property in the connector host is not used.

Connector Property table

The **Connector Property** table displays information about a connector. The columns of the table are sized based on the properties involved. The user can change the data in this table directly.

The following right-click options are available:

- **Remove Row**: Remove the selected row
- **Clone Row**: Make a copy of the selected row
- **Move Row...**: Enter a new row position for the selected row in a dialog box
- **Edit Row...**: Edit data in the selected row in a dialog box
- **Find...**: Enter a string to find in the table
- **Find Next**: Find the next occurrence of the string in the table

The following options are available below the table:

- **Find...**: Prompts user for a string to find in the table
- **Find Next**: Finds the next occurrence of the string in the table
- **Add Row**: Adds a new row to the bottom of the table
- **OK**: Saves changes to the table. You must click **Apply** in the **Properties** tab to permanently save these changes.
- **Cancel**: Cancels changes to the table
- **Help**: Displays a dialog box containing documentation on the fields in the table

If the order of the rows in the table is important, then three additional columns is displayed. The first column in the table is **Order**, which can be edited to move a row. The next two are positional buttons, **Up** and **Down**. Clicking these buttons changes the position of your selected row.

Connector Host: Advanced Tab

This section provides information about advanced properties of connector hosts. See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols and connectors.

Note: When using the URI syntax to access this connector host, some Connector Host Advanced Properties might overlap with properties of the originating host (for example, Email On Fail or Terminate On Fail). When this occurs, which property is used (originating host or Connector) depends on the host making the decision. In the case of Terminate On Fail, it is the originating host making the decision and that same property in the connector host is not used.

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *`n`* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0` - `n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the host should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not Cleo Harmony's or Cleo VLTrader's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of Cleo Harmony or Cleo VLTrader is both the client and server (for example, a local looptest).

Possible values:

`Incoming`
`Outgoing`
`Both`

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Log Transfers For PUT and GET

Enables and disables transfer logging for connector hosts when invoking `PUT` and `GET` commands within the connector host itself.

When using the URI syntax to access a connector host, **Log Transfers For PUT and GET** defaults to `Off` regardless of its setting within the connector host itself. This is because transfers are typically logged by the invoking host and duplicated transfer logging is not desired. However, you can explicitly turn the connector host transfer logging back on using a URI parameter (`?LogTransfersForPutAndGet=On`). You can also use the `%this%` macro as a URI parameter (`?LogTransfersForPutAndGet=%this%`) in an `LCOPY` destination or source to log the `LCOPY` URI transfer against the originating host/mailbox instead of the connector host.

Possible values: `On`, `Off`, or `%this%`

Default value: `On` or `Off` depending on context.

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

Outgoing Insert EOL Between Interchanges

If `Fixed Record Outgoing Insert EOL` is active, indicates to also insert EOL characters between EDI interchanges while sending the file.

Possible values: `On` or `Off`

Default value: `Off`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

Connector Host: Info Tab

The **Info** tab provides information specific to the connector host type in question. For example, the **Info** tab for an SMB connector contains information specific to the SMB connector only.

Connector Host Action Configuration

An action's parameters capture a repeatable transaction for your host.

Connector Host Action: Action Tab

Use the **Action** tab to configure commands within an action.

See Composing an action on page 89. Also see Connector Host Command Reference on page 545.

Connector Host Command Reference

Descriptions of commands and their options, arguments, and parameters.

ATTR

Get attributes for a file on the connector

```
ATTR "source"
```

source

Source directory path

CHECK

See CHECK Command for information about this command.

CLEAR

Clear an action property string value. The cleared value only affects the commands that **follow** the `CLEAR`.

```
CLEAR property
```

property

Action property name with no embedded spaces.

comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

DELETE

Remove a file from the connector

```
DELETE "source"
```

source

Source directory path

DIR

Get a directory listing of available files from the host

```
DIR "source"
```

source

Source directory path

GET

Receive one or more files from the host

```
GET [-DIR] [-DEL] [-UNI] "source" "destination"
```

-DIR

Get one or more files using a directory listing from the host.

Note: If -DIR is used, then there is no source parameter in the command.

-DEL

If GET is successful, delete remote file.

-UNI

Ensure local filename is unique.

source

Remote source path.

destination

Local destination path.

- Path can be a filename or a directory.
- If relative path, then uses the configured Inbox.
- Use of macro variables is supported. See Using Macro Variables (Destination File context) for a list of the applicable macros.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the -UNZ option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the LCOPY command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The LCOPY command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many

other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).

- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

"*source*"

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the user's home directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*input bytes*"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"*output bytes*"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

MKDIR

Make a directory on the connector

```
MKDIR "source"
```

source

Source directory path

PUT

Send one or more files to the host.

```
PUT [-DEL] [-UNI|-APE] "source" "destination"
```

-DEL

If PUT is successful, delete local file.

-UNI

Ensure remote filename unique

-APE

Append to existing destination file

source

Local source path

- Path can be a filename or a directory.
- * and ?, or a regular expression, are supported in filename. See Using wildcards and regular expressions on page 69 for additional information.
- If relative path, then uses the configured Outbox.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.

destination

Remote destination path. Use of macro variables is supported. See Using macro variables on page 59 (Destination File context) for a list of the applicable macros.

RENAME

Remove a directory from the connector

```
RENAME "source" "destination"
```

source

Source directory path.

destination

Destination path.

RMDIR

Remove a directory from the connector. This command recursively deletes the specified folder and all its subfolders and included file.

```
RMDIR "source"
```

source

Source directory path

SCRIPT

See SCRIPT Command for information about this command.

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

Use the `SET` command to set both Advanced properties and Connector properties. To set a Connector property, the scheme name must be used as a prefix. For example, to set the **EnableDebug** property to **true** for an **SMB** connector: `smb.EnableDebug=True`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

Note:

You can use the `SET` command to override the values for `setbox` and `receivedbox` set on the Connector Host **General** tab using the `general.Sentbox` and `general.Receivedbox` properties. For example, to set the `setbox` to the `sentbox2` folder, use this command:

```
SET general.Sentbox=sentbox2
```

To disable `setbox` or `receivedbox`, use the `%none%` macro. For example, to turn off the `receivedbox` folder, use this command:

```
SET general.Receivedbox=%none%
```

To set these properties back to their host-level settings, use the `SET` command without any values:

```
SET general.Sentbox=
```

```
SET general.Receivedbox=
```

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"path"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

Standalone Actions

Note: Standalone actions are supported only in the Cleo Harmony application.

Standalone actions are actions that are not tied to a specific host or user. They exist beside, and not within, hosts or users.

You can use standalone actions for a variety of purposes, such as:

- Filtering incoming payload (for example, the Antivirus Scan action)
- Listening for and acting on log events
- Processing new file arrival or user session end events
- Scheduling periodic maintenance tasks

A standalone action can access configured hosts and users (and their related incoming payload and events) when they are *in-scope*, which means that relative to the standalone action, the host or user is located in the same host tree resource folder or below, or in the root host tree folder (which is always accessible). A standalone action contains only JavaScript commands.

Similar to other actions, you can run standalone actions interactively, through the Java API, and through command line operations (for example, `Harmonyc -r "MyStandaloneAction"`). You can also schedule standalone actions to run periodically, or trigger them to run when a new file arrives or a session ends.

Standalone Action Configuration

A standalone action captures a repeatable logical function you can use with in-scope hosts and users.

1. Click the **Templates** tab in the tree pane.
2. If necessary, expand the **Hosts** tree in the **Templates** tab.
3. Expand the **Standalone Actions** folder, right-click the action you want to use, and select **Clone and Activate**.

   The pre-configured *Standalone Action* is copied and activated, the **Active** tab is selected in the tree pane, and the new active *Standalone Action* is selected in the tree. If necessary, the new standalone action is appended with a number to make it unique.

   Note: The original pre-configured standalone action remains in the templates tree.
4. Enter configuration information.
   a) Click the standalone action to display its configuration tabs.
   b) Edit the action. See Standalone Action: Action Tab on page 552.
5. Click **Apply** to save your work.

Important: If you leave any of these panels without clicking **Apply**, your work will not be saved. You can configure the native UI to prompt to you click **Apply** when changes are made. See Other system options on page 729. However, in the web UI, this is not valid. In the web UI, if you make updates to a host and then click a part of the product not related to a host, for example any of the buttons in the banner, the product will not prompt you to click **Apply** and your updates will not be saved.

Standalone Action: Action Tab

Use the **Action** tab to compose an action. See Composing an action on page 89.

Note: Since standalone actions are not tied to a specific host or user, they do not support the Commands language and rather only support the JavaScript language.

Select the **Automatically run at startup** check box to execute the action automatically each time the Cleo Harmony application is first launched. This is useful depending on the purpose of the standalone action, such as an incoming filter or log listener that needs to register itself at startup.

Standalone Action: Messages Tab

The **Messages** tab scrolls runtime messages for the standalone action. The contents of the **Messages** tab is retained until the next time the action is run, even if the system is restarted.

Chapter

5

Connectors

A Connector is a component that facilitates communication between Cleo Harmony and Cleo VLTrader on the one hand, and external systems on the other.

AMQP Connector

AMQP 1.0 Connector is used for communicating messages to and from AMQP 1.0 compliant messaging systems. AMQP 1.0 is a network protocol at the Application Layer which give a standard specification on how the connections and sessions needs to be established and how messages are sent and acknowledged. For more info on AMQP, visit http://www.amqp.org/sites/amqp.org/files/amqp.pdf.

There are various AMQP 1.0 messaging applications, like Azure Service Bus (ASB), ActiveMQ. The current version of the connector is tested and verified to be working with Azure Service Bus. Some of the broker specific feature, like ReceiveMode, are not yet supported. Metadata from source that comes to the Connector is handled and sent as a header to AMQP messages.

Messaging

Publishing to queue and topics can be done using the AMQP Connector. Mandatory properties for enabling publisher are Hosts, Username, Password, and Queue/Topic name. Publishing text and binary file is supported by the AMQP Connector. For enabling broker-specific features, Vendor must be selected. For AMQP generic features, `Common` can be selected in Vendor.

Receiving from queues and topics is supported by AMQP Connector. To enable to the receiver, select the EnableReceiver checkbox. Mandatory properties for receiver are Hosts, Username, Password, and SubscribeTo name. Receiving text and binary files is supported. Creating an ASB topic subscriber requires that you create a subscription for that topic in ASB portal and provide that name in SubscribeTo in the format `<topicName>/subscribers/<subscriptionName>`. For ASB Queue subscription the queue name must be entered in SubscribeTo field.

The MessageSelector feature is not currently functional as it is not supported by ASB.

Security

AMQP 1.0 can be implemented with SSL/TLS. In the current version, TLS is supported only with ASB. ASB by default enforces TLS.

Duplicate Detection

The AMQP Connector has Duplicate Detection capability using the JMS Message ID to identify duplicate messages. This feature can be enabled by checking DuplicateDetection checkbox in AMQP10 connector configuration. After the expiry of DuplicateDetectionTimeout, the JMS Ids are deleted from the cache, so if a duplicate message arrives after the timeout, it cannot be detected. This feature would fail if multiple receivers are in a cluster with the same subscription because the message id cache is maintained within the local instance.

For filtering only AMQP-specific configuration, select Connect.Advanced from the configuration screen.

File size limit

File size limit (in the Connector) can be configured by setting `MessageMaxByteSize`. The default size is 1 MB. By default, ASB broker has a message size limit of 1 MB. To increase the message size, both of these settings must be changed.

Limitations

- Volatile subscriptions are currently not supported with ASB.
- Transactions are not supported with ASB.

AMPQ Connector Properties

Each instance of the AMPQ Connector can be configured using the following settings:

Property	Description	Required
Broker Url	The broker url.	Yes
Vendor	The broker vendor. Currently supported values are ’AzureServceBus’ and 'Common'	Yes
Topics	AMQP topics. Comma-separated (topic1,topic2)Valid pattern: `[([a-zA-Z0-9]|-|_|\.|,){0,249}]`	
Queue	Name of the QueueValid pattern: `[([a-zA-Z0-9]|-|_|\.|,){0,249}]`	
Message Max Size Bytes	Message size limit for sending. Increasing this value will enable sending a larger file from the connector. Broker configuration also needs to be changed to receive a larger file.	Yes
Username	user / sas key name using which the connection is established.Valid pattern: [([a-zA-Z0-9]|-|_|\.|,){0,249}]	Yes
Password	password or sas key using which the connection is established	Yes
Enable Receiver	To enable to receiver	
Subscribe To	Name of the entity to subscribe to (Queue Name/Subscription name)	
Duplicate Detection	Enabling duplicate detection ignores the duplicate messages received from the broker. Duplicates are detected using the message ID.	

Property	Description	Required
Duplícate Detection Timeout (seconds)	Timeout for duplicate elements to be detected. If a duplicate message is received after this timeout has expired for the message, the duplicate will not be detected.	
Delivery Mode	This is the default delivery mode. If we use this delivery mode, then it forces the JMS provider to take extra care to avoid the loss of a message if a provider failure occurs. If a provider failure occurs, then the message will be persisted. When the provider comes up the message will be delivered. This ensures reliable message delivery.	Yes
Publish To Destination	Publish to Queue/Topic	Yes
Subscription Destination	Subscribe to Queue/Topic	Yes
Acknowledgement Mode	There are three acknowledge modes available: CLENT_ACKNOWLEDGE, AUTO_ACKNOWLEDGE, and DUPS_OK_ACKNOWLEDGE	Yes
Message Selector	Used by messaging application that needs to filter the messages it receives. A message selector is a String that contains an expression. The syntax of the expression is based on a subset of the SQL92 conditional expression syntax. Example value is `NewsType = 'Sports' OR NewsType = 'Opinion'`	
Message Properties	Additional message properties to be set (Message metadata/headers)	
Amqp Vhost	The vhost to connect to. Used to populate the SASL and Open hostname fields. Default value is the main hostname from the Connection URI.	
Amqp Sasl Layer	Controls whether connections should use a SASL layer or not. Default value is 'true'.	
UseSsl	If the connection is over SSL. Default value is 'true'.	

Property	Description	Required
Amqp Sasl Mechanisms	Which SASL mechanism(s) the client should allow to be selected if offered by the server and usable with the configured credentials. Comma-separated list if specifying more than 1 mechanism. The client-supported mechanisms are currently EXTERNAL, SCRAM-SHA-256, SCRAM-SHA-1, CRAM-MD5, PLAIN, ANONYMOUS, and GSSAPI for Kerberos.Default is to allow selection from all mechanisms except GSSAPI, which must be specified here to enable.	
Amqp Max Frame size	The max-frame-size value (in bytes) that is advertised to the peer.Default is 1048576	
Amqp Drain Tmeout (seconds)	The time in milliseconds that the client will wait for a response from the remote peer when a consumer drain request is made. If no response is seen in the allotted timeout period, the link is be considered failed and the associated consumer is closed.Default is 60000 (1 minute).	
Amqp Idle Timeout (seconds)	amqp.idleTimeout The idle timeout in milliseconds after which the connection will be filled if the peer sends no AMQP frames. Default is 60000 (1 minute).	
Amqp Alow Non Secure Redirects	Controls whether the client allows an AMQP redirect to an alternative host over a connection that is not secure when the existing connection is secure. For example, redirecting an SSL/TLS connection to a raw TCP connection. Default is false.	
Transport Key Store Location	Default is to read from the system property javax.net.sslkeyStore	
Transport Key Store Password	Default is to read from the system property javax.net.ssLkeyStorePassword	
Transport Trust Store Loca Don	Default is to read from the system property javax.net.ssLtrustStore	

Property	Description	Required
Transport Trust Store Password	Default is to read from the system property javax.net.ssltrustStorePassword	
Transport Key Store Type	Default is to read from the system property javax.net.ssLkeyStoreType	
Transport Context Protocol	The protocol argument used when getting an SSLContext. Default is TLS, or TLSvl.2 if using OpenSSL	
Transport Enabled Cipher Suites	A comma-separated list of cipher suites to enable. No default, meaning the context-default ciphers are used. Any disabled ciphers are removed from this list.	
Transport Disabled Protocols	A comma-separated list of protocols to disable. Protocols listed here are removed from the enabled protocol list. Default is SSLv2Heto.	
Transport Trust All	If enabled, trust the provided server certificate implicitly, regardless of any configured trust store. Default is false.	
Transport Verify Host	If enabled, verify that the connection hostname matches the provided server certificate. Default is true.	
Transport Key Alias	The alias to use when selecting a key pair from the key store is required to send a dent certificate to the server. No default.	
Transport Use Open SSL	If enabled, use native OpenSSL ! >raries for SSL/TLS connections if available. Default is false.	
System Scheme Name	The URI scheme name used as a shortcut to this host.Valid pattern: `[([a-zA-Z0-9]|-|_|\.|,){0,249}]`	
System Public	A switch that indicates whether the connector is public.	

AzureBlob Connector

The AzureBlob connector is used to communicate with Microsoft Azure Blob Storage (Blob Storage). Azure Blob Storage is Microsoft's object storage solution for the cloud. Blob Storage is optimized for storing massive amounts of unstructured data, such as text or binary data. Blob Storage exposes three resources: the Azure storage account,

the containers within the account, and the blobs within a container. Azure offers three types of blobs – block blobs, append blobs, and page blobs. The Cleo AzureBlob connector supports block and append blobs for upload operations and all three types for download operations. When creating a new blob through an upload operation, use the Blob Type property to designate the type you want. Block blobs are the default.

The blobs within a container have a flat structure, without the hierarchy you might see in a typical file system. However, for organizational simplicity, the Cleo AzureBlob connector supports the folder concept as a means of grouping objects. Therefore, you can treat your folder and file objects as you would in a standard hierarchical file system. For example:

```
PUT example.txt AzureTestFolder/example.txt
```

This command transfers the local file, example.txt, to the configured container within a "folder" object called AzureTestFolder. Note that AzureTestFolder must exist as an object in blob container.

Two different authentication methods are supported.

- The first method is to use the access key directly with the property 'Access Key'.
- The second is to use the access key stored inside of an Azure Key Vault secret.

To setup this second method, you need to have an Azure Key Vault with a secret that contains the access key. The key vault name and secret name must be supplied through the properties 'Key Vault Name' and 'Key Vault Secret Name', respectively. You also need an application service principal that has access to the Key Vault. The application clientId and clientSecret must be supplied through the properties 'Application Client ID' and 'Application Client Secret', respectively.

Notes:

- The `ATTR` command currently supports a subset of all Azure blob attributes.
- The Pseudo Folders property can be used to control whether actual folder objects are created and needed by the connector.
- `LCOPY -DEL` commands that attempt to move files will use the connector RENAME, thereby avoiding download/upload Azure charges.
- `LCOPY -DEL` commands that attempt to move files between two different containers by overriding the destination container with a query parameter will also use the connector RENAME to avoid download/upload Azure charges. However, defining any destination query parameters other than the container will cause the file to be downloaded from one container and uploaded to the other container which will most likely incur an Azure charge.
- If during an `LCOPY -DEL` the source container is overridden with a query parameter the destination will also use the same container. If desired, both the source and destination containers can be overridden with query parameters to copy between containers.

AzureBlob Connector Properties

Each instance of the AzureBlob Connector can be configured using the following settings:

Property	Description	Required
Storage Account Name	The Azure Storage account name.	Yes
Access Key	The Azure Storage account access key. If not supplied, then Azure Key Vault authentication will be used.	
Key vault Name	The Azure Key Vault name.	

Property	Description	Required
Key Vault Secret Name	The name of the secret n the Azure Key Vault.	
Application Client ID	The ID of the client registered as an application in Azure Active Directory. Used to authenticate to Azure Key Vault.	
Application Client Secret	The secret for the client registered as an application n Azure Active Directory. Used to authenticate to Azure Key Vault.	
Endpoint Suffix	The Azure Storage endpoint suffix.	Yes
Container	The Azure Storage container name.Valid pattern: [^[a-z0-9]{1}[a-z0-9-]{1,62}]	Yes
Btob Type	The Azure Blob Storage blob type. This setting controls the blob type for created blobs.	Yes
Pseudo Folders	Whether MKDIR/RMDIR should create/remove pseudo folder objects and where pseudo folder objects are required for DIR.	
Proxy Address	An optional HTTP proxy IP address or hostname.	
Proxy Port	An optional HTTP proxy IP port.Valid range: [0-65535]	
Headers	A list of optional additional HTTP headers.	
Command Retries	The number of Ornes the command should be retried when an error or exception occurs.Valid range: [10-51]	Yes
Command Retry Delay (seconds)	The number of seconds to wait between retries.Valid range: [0-120]	Yes
Do Not Send Zero Length Fies	For PUT, a switch that indicates to not send a file if it is zero-length.	
Delete Received Zero Length Fies	For GET, a switch that indicates to remove a received file that is zero-length.	
Retrieve Directory Sort	For PUT, the sorting options for the list of outbound files.	
Enable Debug	A switch that indicates whether to perform debug logging.	

Property	Description	Required
System Scheme Name	The URI scheme name used as a shortcut to this hostValid pattern: [[a-zA-Z]{1}{a-zA-Z0-9+\-\.]{1.23}].	
System Public	A switch that indicates whether the connector is public.	

Clarify Connector

The Clarify connector is used to integrate inbound and outbound file transfers directly with Cleo Clarify. The inbox and outbox of each Cleo Harmony host to be integrated with Clarify must point to an instance of this connector.

Only one Clarify connector is needed for an integration with a Cleo Clarify cluster. Consider giving the Clarify connector a meaningful name such as `Prod', 'Test', 'Dev', and so on. To make it easier to configure the inbox and outbox for each Cleo Harmony host, consider adding Custom Directory Variables such as `clarify:Prod/%host%/fromclarify` and `clarify:Prod/%host%/toclarify`. In this way, the user can select `clarify:Prod/%host%/toclarify` as the host inbox and `clarify:Prod/%host%/fromclarify` as the host outbox from the Inbox and Outbox pull-down menus, respectively.

When an integrated host receives an inbound file, Cleo Harmony attempts to connect to the first server in the Clarify connector's list of servers. If the server is not available, Cleo Harmony tries each subsequent Clarify server in the list until a connection is established or the list of servers is exhausted. If the list of Clarify servers is exhausted, the transfer fails. When a connection has been established, the data is streamed to the Clarify server on the port specified. This port is configured in Clarify in the Harmony Monitor object. For more information on how the data is processed when Clarify's Harmony Monitor receives it, see the Cleo Clarify User Guide.

For outbound dataflow, the **SendMessageToHarmony** business process task in Cleo Clarify takes a Cleo Harmony host alias as an argument. The integrated host's `<send>` action can then be scheduled to run automatically either by polling Clarify or periodically. For more information on how to send data from Clarify to a particular Harmony host, see the Cleo Clarify User Guide.

Note: The Clarify connector only supports the AS2, FTP, and SFTP protocols to the extent that Cleo Dashboards will associate the file flow between Cleo Harmony and Cleo Clarify.

Clarify Connector Properties

Each instance of the Clarify Connector can be configured using the following settings:

Property	Description	Required
Clarify Servers	A semicolon separated 1st of the Qeo Clarify server addresses.Valid pattern: `[^+:\d+(;.+:\d+)*$]`	Yes
Command Retries	The number of times the command should be retried when an error or exception occurs.Valid range: [0-5].	Yes

Property	Description	Required
Store And Forward	A switch that indicates controls or not to store the contents locally when the connector endpoint is down and subsequently forward to the connector endpoint when it is back up.Note: For this feature to work, the Receivedbox must be configured in the host using this Connector and Adminstration>Other>Dsable Date/ Time Portion Of Filenames Sent/ Recieved Box must be unchecked.	
Store And Forward Retry Delay (seconds)	The number of seconds to wait between 'Store And Forward' retries.Vaid range: [0-900].	Yes
Enable Debug	A switch that indicates whether to perform debug logging.	
System Scheme Name	The URI scheme name used as a shortcut to this host.Valid pattern: `[[a-zA-Z]{l}[a-zA-Z0-9+\-\.]{l,23}]`.	

EEI Connector

The EEI connector is used to integrate inbound and outbound file transfers with Cleo EEI. The inbox and outbox of each Cleo Harmony host to be integrated with Cleo EEI must point to an instance of this connector.

Only one EEI connector is needed for an integration with Cleo EEI. Consider giving the EEI connector a meaningful name, such as *Prod* or *Test*. To use the EEI connector, set the host inbox to `EEI:Prod/` and the host outbox to `EEI:Prod/partner1`, where *Prod* is the alias of the connector and *partner1* is the trading partner name configured in Cleo EEI. Cleo Harmony allows you to map many EEI partners to one host connection by entering them as a comma-separated list in the Harmony host outbox, for example, `EEI:Prod/partner1,partner2,partner3,partner4`. All outbound trading partner files are placed in the same outbound directory identified by the first partner in the list. The first name in the list can actually correspond to what is referred to as a *port* in EEI. If the trading partner is defined in more than one enabled host outbox, the file is not sent, and EEI is sent an error notification.

When an integrated host receives an inbound file, Harmony attempts to connect with the Cleo EEI server. If the server is unavailable, the transfer fails. When a connection has been established, the data is streamed to the Cleo EEI inbound data queue. For more information on how Cleo EEI processes the data, see the Cleo EEI User Guide.

For outbound data flow, Cleo EEI places data on its outbound data queue. The integrated host's `<send>` action can then be scheduled to run either periodically or automatically by polling Cleo EEI. All data for the trading partner name specified in the Cleo EEI connector is then streamed to the trading partner. For more information on how data is sent from Cleo EEI, see the Cleo EEI User Guide.

NOTES:

When migrating a large number of trading partners from ESX, you can transition trading partners in batches either by migrating the associated hosts to Harmony in sets or by initially disabling all of the imported hosts and enabling a set of hosts at a time. When a host is not found or is disabled in Harmony:

- Outbound messages in Cleo EEI are placed on a secondary outbound data queue (EXTESXOUT2) that is processed by ESX. The secondary EXTESXOUT2 outbound data queue should be manually created in the same library as the EXTESXOUT data queue at the beginning of the migration phase and set as the outbound data queue in ESX. The AS/400 command to create the EXTESXOUT2 outbound data queue is:

  ```
  CRTDTAQ DTAQ(&DTAQLIB/EXTESXOUT2) MAXLEN(325) AUTORCL(*YES) TEXT('EEI to ESX
   actions (Outbound data)')
  ```

  After the migration is complete, the command to remove the secondary outbound data queue is:

  ```
  DLTDTAQ DTAQ(&DTAQLIB/EXTESXOUT2)
  ```
- Inbound AS2 messages for unknown trading partners can be redirected to ESX through Cleo VLProxy (Version 3.6.1 or later) by setting the 'Unknown Partner Message Action' to (U)RL-Redirect and its value to the URL where ESX is installed. See the Cleo VLProxy User Guide for further information.

EEI Connector Properties

Each instance of the EEI Connector can be configured using the following settings:

Property	Description	Required
AS/400 Address	The IP address of the remote AS/400 where EEI is installed.	Yes
AS/400 User	The user name for the remote AS/400 where EEI is installed.	Yes
AS/400 Password	The user password for the remote AS/400 where EEI is installed.	Yes
Inbound Data Queue	The fully qualified path for the inbound EEI data queue.	
Outbound Data Queue	The fully qualified path for the outbound EEI data queue.	
Lock Data Queue	The fully qualified path for the EEI lock queue used to synchronize outbound queue access between multiple VersaLexes.	
IFS Inbound Path	The IFS path on the remote AS/400 where the inbound files are stored.	
IFS Outbound Path	The IFS path on the remote AS/400 where the outbound data is stored.	
Environment Name	An optional EEI environment name.	
Activate ESX Migration	Enable the ability to use ESX secondary outbound data queue for unknown or disabled	

Property	Description	Required
Command Retries	The number of times the command should be retried when an error or exception occurs.Valid range: [0-5].	Yes
Command Retry Delay (seconds)	The number of seconds to wait between retries.Valid range: [0-120].	Yes
Store And Forward	A switch that indicates whether or not to store the contents locally when the connector endpoint is down and subsequently forward to the connector endpoint when it is back up.Note: For this feature to work, the Received box must be configured in the host using this Connector and Administration>Other>Disable Date/Time Portion Of Filenames In Sent/Received Box must be unchecked.	
Store And Forward Retry Delay (seconds)	The number of seconds to wait between 'Store And Forward' retries.Valid range: [0-900].	Yes
Do Not Send Zero Length Fies	For PUT, a switch that controls whether to send a file if it is zero-length.	
Delete Received Zero Length Fies	For GET, a switch that controls whether to remove a received file that is zero-length.	
Retrieve Directory Sort	For PUT, the sorting options for the list of outbound files.	
Enable Debug	A switch that indicates whether to perform debug logging.	
System Scheme Name	The URI scheme name used as a shortcut to this host.Valid pattern: `[[a-zA-Z]{1}[a-zA-Z0-9+\-\.[{1.23}].`	
System Public	A switch that indicates whether the connector is public.	

File Connector

The File connector is used to communicate with a native file system not requiring authentication and allows a script to be run after a PUT. Folders and files accessed by this connector use the credentials of the user running the Cleo Harmony process.

If a *Root Path* is configured in the File properties tab, files and folders at or below this path are accessible while those above are not accessible. If a *Root Path* is not configured, the file being accessed must be described by an absolute path.

If accessing a UNC path through a URI using this connector and the *Root Path* is not configured, the short-form URI syntax must be used. For example:

```
LCOPY ..\outbox\test\test.edi myfiles://filsvr01/public/subdir01/subdir02/
test1.edi
```

where there is a File connector whose *System Scheme Name* property is set to *myfiles*.

Post Processing Commands

The *Post Processing Command* property is a string that supports a replacement token syntax, which allows the name of the file that was just PUT to be placed in the command line arbitrarily. The replacement token mechanism also supports additional tokens and expressions to allow the command line to include formatted timestamps, source metadata, and JavaScript expressions.

Tokens and expressions are embedded in the command line using the `${expression}` syntax, where the simplest expression is a direct token reference. The following tokens and expressions are supported:

Token/Expression	Description
file	the filename including path and full filename
filename	the full filename, excluding the path
path	the filename path (filename removed, trailing / or \ included)
base	the base portion of the filename (path and .extension removed)
noext	the base portion of the filename (.extension removed)
ext	the filename extension (including the . prefix)
date('format')	the current date/time formatted with format string based on Java SimpleDateFormat
source['metadata']	metadata propagated from the source (see below)
expression	a JavaScript expression, possibly including the above

The following describes the relationship between the various filename components for `/path/to/file/basefilename.extension`

file	`/path/to/file/basefilename.extension`
filename	`basefilename.extension`
path	`/path/to/file/`
base	`basefilename`
noext	`/path/to/file/basefilename`
ext	`.extension`

The following expressions all evaluate to the same result:

- `${path}${base}${ext}`
- `${noext}${ext}`
- `${file}`
- `${path+base+ext}`

As a performance optimization, any JavaScript expression of the form `${token}` for one of the tokens above is expanded without invoking the JavaScript engine. Also, the primitives `${date('string')}` or `${date("string")}` are similarly expanded without invoking JavaScript. This means that although the four examples above produce the same result, the first three execute much more quickly. But the JavaScript engine provides more capability for some use cases.

This (Linux) example renames the file by inserting the last portion of the DocDBTransferID (a GUID) before the extension:

```
/bin/mv ${file}
            ${noext}.${source.DocDBTransferID.replace(/.*-/,'')}${ext}
```

A word about source['metadata']

If a script connection is used directly through a URI reference as the inbox of another Harmony connection (or host or mailbox), additional protocol-specific metadata may be available in addition to the file content being stored. The metadata is represented as a JavaScript array (so use square brackets to access the values). For example, values available for AS2 include:

Some examples of source['metadata']:

`${source['AS2-From']}`	The AS2-From (partner) name
`${source['AS2-To']}`	The AS2-To (local) name
`${source['ClientServer.Role']}`	"Server" in a typical use case as described
`${source['Content-Disposition']}`	HTTP.header.Content-Disposition
`${source['Content-Type']}`	HTTP.header.Content-Type
`${source['DocDBTransferID']}`	The Harmony REST API transfer ID
`${source['HTTP.header.'+header]}`	The HTTP header header
`${source['Protocol']}`	"AS2"
`${source['Subject']}`	The AS2 Subject
`${source['TransferID']}`	The Harmony transfer ID
`${source['VersaLex.Serial.Number.Short']}`	The Harmony serial number, e.g. "HY1234"

To inspect the available metadata for a particular configuration, use a post-process command like the following.

- On Linux:

  ```
  /bin/sh -c 'echo ${JSON.stringify(source)}'
  ```
- On Windows:

  ```
  cmd.exe /c echo.exe ${JSON.stringify(source)}
  ```

Command Output Logging

The intent of the Post Processing command is to process the file and indicate success with a process return code of 0 or failure with any nonzero return code. To aid with troubleshooting, the script connector also captures any output,

including "standard output" (stdout) and "error output" (stderr) and copies them as detail records to the log, one log message per line.

Standard output records are prefixed with [stdout] and are logged at log level LOW, while standard error records are prefixed with [stderr] and are logged at log level ESSENTIAL.

File Connector Properties

Each instance of the File Connector can be configured using the following settings:

Property	Description	Required
Root Path	The file system root path. Custom macros may be used at the beginning of the path.	
Expand Fie Name On Put	Controls whether ${expressions} should be expanded in destination file names on a PUT.	
Post Processing Command	The operating system command to be executed after a PUT. Use ${fie} to represent the file to be processed.	
Post Process Working Directory	The optional working subdirectory of the Root Path in which to run the post processing command. Custom macros may be used at the beginning of the path.	
Post Process Timeout (seconds)	The number of seconds to wait for the Post Processing Command to complete before killing the process and forcing an error, or 0 to disable the timeout feature. Vald range: [0-2147483647].	
Command Retries	The number of tunes the command should be retried when an error or exception occurs.Valid range: [0-5].	Yes
Command Retry Delay (seconds)	The number of seconds to wait between retries.Valid range: [0-120].	Yes
Do Not Send Zero Length Fies	For PUT, a switch that controls whether to send a file if it is zero-length.	
Delete Received Zero Length Fies	For GET, a switch that controls whether to remove a received file that is zero-length.	
Retrieve Directory Sort	For PUT, the sorting options for the list of outbound files.	
Enable Debug	A switch that controls whether to perform debug logging.	

Property	Description	Required
System Scheme Name	The URI scheme name used as a shortcut to this host.Valid pattern: `[[a-zA-Z]{ 1 }[a-zA-Z0-9+\-V]{ 1.23}].`	
System Public	A switch that indicates whether the connector is public.	

GCS Connector

The Google Cloud Storage Connector is used to communicate with Google Cloud Storage (GCS) and supports Blobs for Google's Cloud Storage service. In GCS, buckets and objects are the primary resources, where objects are stored in buckets. GCS buckets have a flat structure without a hierarchy like you might see in a typical file system. However, for organizational simplicity, the Cleo GCS Bucket connector supports the folder concept as a means of grouping objects. Therefore, you can treat your folder and file objects as you would in a standard hierarchical file system.

GCS Connector Properties

Each instance of the GCP Connector can be configured using the following settings:

Property	Description	Required
Project Id	Google Project ID.	Yes
Google Account Key	Import Service Account Key JSON file.	Yes
Bucket Name	The name of the GCS bucket.	
Pseudo Folders	Whether MKDIR/RMDIR should create/remove pseudo folder objects and where pseudo folder objects are required for DIR.	
Mark Directories	Append ".dir" to directory names to distinguish them from object names.	
Proxies	Optional addresses of HTTP proxies to use for the connection. Connects to proxies using round robin. If there is a proxy connection failure, it will wait for 60 seconds before retrying that proxy.	
Command Retries	The number of times the command should be retried when an error or exception occurs.Valid range: [0-5].	Yes
Command Retry Delay (seconds)	The number of seconds to wait between retries.Valid range: [O-120].	Yes
Do Not Send Zero Length Fies	For PUT, a switch that controls whether to send a file if is it zero-length.	

Property	Description	Required
Delete Received Zero Length Fies	For GET, a switch that controls whether remove a received file that is zero-length.	
Retrieve Directory Sort	For PUT, the sorting options for the list of outbound files.	
Enable Debug	A switch that indicates whether to perform debug logging.	
System Scheme Name	The URI scheme name used as a shortcut to this host.Valid pattern: `[[a-zA-Z]{ 1 }[a-zA-Z0-9+\-\.]{ 1,23}].`	
System Public	A switch that indicates whether the connector is public.	

HDFS Connector

The HDFS connector is used to communicate with a Hadoop Distributed File System (HDFS). The HDFS site-specific information files (core-site.xml and hdfs-site.xml) are imported into the connector configuration through the HDFS properties tab. You should obtain these files from your Hadoop administrator.

The HDFS connector supports both simple and Kerberos authentication. When using simple authentication, only the HDFS User property is required. When using Kerberos, you must import a keytab file into the connector configuration through the HDFS properties tab. You should obtain the keytab file from your Hadoop administrator.

The HDFS connector also supports transparent encryption. While no additional configuration is needed in the connector, your Hadoop administrator will need to configure it on the server and enable encryption zones from which you will send and receive files. See the Apache Hadoop website for a further description of transparent encryption in HDFS.

Notes:

- The ATTR command currently supports a subset of all HDFS attributes.
- The Cleo HDFS connector uses the Apache Hadoop API. This API defines a "wire compatibility" policy consisting of rules for compatibility between the client (the HDFS connector) and the server (your HDFS repository). In summary, this policy states that compatibility will be maintained as long as both the client and server are operating under the same major release. To understand the current client release level, refer to Help>About where thIBMMQ Connector on page 571e Hadoop API release numbers are identified.

HDFS Connector Properties

Each instance of the HDFS Connector can be configured using the following settings:

Property	Description	Required
HDFS User	The user to use for HDFS access.	Yes
core-site.xml	Import core-site.xml file.	Yes
hdfs-site.xml	Import hdfs-site.xml fie.	Yes

Property	Description	Required
Keytab	Import keytab for Kerberos authentication.	
Command Retries	The number of times the command should be retried when an error or exception occurs. Valid range: [0-5].	Yes
Command Retry Delay (seconds)	The number of seconds to wait between retries.Valid range: [0-120].	Yes
Do Not Send Zero Length Fies	For PUT, a switch that controls whether to send a file if it is zero-length.	
Delete Received Zero Length Fies	For GET, a switch that controls whether to remove a received file that is zero-length.	
Retrieve Directory Sort	For PUT, the sorting options for the list of outbound files.	
Enable Debug	A switch that controls whether to perform debug logging.	
System Scheme Name	The URI scheme name used as a shortcut to this host. Valid pattern: `[[a-zA-Z]{1}[a-zA-Z0-9+\-\.]{1,23}]`	
System Public	A switch that indicates whether the connector is public.	

IBMMQ Connector

The IBMMQ Connector is used to talk to IBM MQ servers using Java Message Service (JMS).

Configuration

The server is identified using the MQ Host and MQ Port setup options. The Queue Manager, Queue, Channel, Username, and Password should also be configured to talk to the IBM MQ Server.

The Default Filename is used to set a filename that will be used for incoming messages. The default setting for this is `${source['jms.messageid']}`, which uses `message id` received from the IBM MQ server. This supports user metadata - see User metadata.

Message Selector can be set to limit the messages that are selected from the IBMMQ servers. The format for this field is the IBM MQ message selector (for more information see https://www.ibm.com/docs/en/ibm-mq/9.3?topic=queues-message-selector-syntax)

Message properties can be set up to add properties to a message that is added to a queue. This supports the user metadata - see User metadata.

To enable SSL, add the cipher suite that is to be used to the Cipher Suite option. You will then need to import an SSL KeyStore and TrustStore (in JKS format) and provide the password of these stores.

The following ciphers are supported:

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- ECDHE_RSA_AES_256_GCM_SHA384
- ECDHE_RSA_AES_128_GCM_SHA256

Other ciphers that may also work are listed here: https://www.ibm.com/docs/en/ibm-mq/9.3?topic=jms-tls-cipherspecs-ciphersuites-in-mq-classes.

To enable the receiver, select 'Enable Receiver'. Messages are pulled from the queue when they are added and placed into the inbox folder configured within the host. The 'Default Filename' will set the filename that the message will be stored as.

The connector has the ability to update most of the settings through the URI interface. The queue can be overridden by using the following format (assuming the IBM MQ Connector queue is named 'MQ'):

```
IBMMQ:MQ?IBMMQ.Queue=overrideQueue
```

This will override the queue to use 'overrideQueue' instead of the queue defined in the settings panel.

There is an additional field that can be used to set properties from the URI interface as well. These are passed in a comma-separated format. For example, the following adds message properties to the files that are sent. These properties also support the macro engine.

```
IBMMQ:MQ?IBMMQ.AddProperties=name1=value1,name2=value2
```

To enable debugging of the IBM MQ library, add the following flag to lax.nl.java.option.additional in the lax file:

```
-Dcom.ibm.msg.client.commonservices.trace.status=ON
```

a restart will be needed after this is added. It will create a file ending in .trc in the Harmony directory.

User metadata

The user metadata allows replacement using macros. The IBM MQ connector supports using any message properties as macros for the Default Filename.

To use a message property that is defined within the message, use this format:

```
${source['property_name']}
```

where `property_name` is the name defined on the message.

The following properties are also provided:

- `jms.messageid`
- `jms.timestamp`
- `jms.correlationid`
- `jms.priority`
- `jms.deliverymode`
- `jms.deliverytime`
- `jms.expiration`
- `jms.replyto`
- `jms.messagetype`

Tokens and expressions are embedded in the Value using the `${expression}` syntax, where the simplest expression is a direct token reference. The following tokens and expressions are supported:

Token	Description

`file`	the filename including path and full filename
`filename`	the full filename, excluding the path
`path`	the filename path (filename removed, trailing / or \ included)
`base`	the base portion of the filename (path and .extension removed)
`noext`	the base portion of the filename (.extension removed)
`ext`	the filename extension (including the . prefix)
`date('format')`	the current date/time formatted with 'format' (see http://docs.oracle.com/javase/8/docs/api/java/text/SimpleDateFormat.html)
`source['metadata']`	metadata propagated from the source (see below)
`expression`	a JavaScript expression, possibly including the above

The following diagram describes the relationship between the various filename components:

```
/path/to/file/basefilename.extension
|<------------- file ------------->|
|<-- path -->||<---- filename ---->|
             |<- base ->||<- ext >|
|<-------- noext ------->||<- ext >|
```

Examples: The following expressions all evaluate to the same result:

```
${path}${base}${ext}
```

```
${noext}${ext}
```

```
${file}
```

```
${path+base+ext}
```

As a performance optimization, any JavaScript expression of the form `${token}` for one of the tokens above is expanded without invoking the JavaScript engine. Also, the primitives `${date('string')}` or `${date("string")}` are similarly expanded without invoking JavaScript. This means that although the four examples above produce the same result, the first three execute much more quickly. But the JavaScript engine provides more capability for some use cases. This example illustrates computing a Value extracted from the last portion of the DocDBTransferID (a GUID):

```
${source.DocDBTransferID.replace(/.*-/,'')}
```

IBMMQ Connector Properties

Property	Description	Required
MQHost	MQ Server Address	Yes
MQPort MQ Server Port.	Default is 1414	Yes
QueueManager	Queue manager	Yes
Channel	Channel	Yes
Queue	Queue name	

Username	Queue Manager Username	Yes
Password	Queue Manager Password	Yes
DefaultFilename	Filename to be used when receiving files. Default is "Filename".	Yes
EnableReceiver	Enables the receiver. Default is "false".	
MessageSelector	Message properties to be used when selecting messages	
MessageProperties	Additional message properties to be set (Message metadata/headers)	
MessageType	The message type used when putting a message on the queue	
CipherSuite	A comma-separated list of cipher suites to enable	
SSLKeyStore	Upload the SSL KeyStore file	
SSLKeyStorePassword	Password to SSL KeyStore	
SSLTrustStore	Upload SSL TrustStore file.	
SSLTrustStorePassword	Password to SSL TrustStore	

ICAP Connector

The ICAP connector is used to communicate over the Internet Content Adaptation Protocol (ICAP). In Cleo Harmony's case, ICAP is used for streaming inbound files through an anti-virus scanner.

After filling in the required ICAP properties, use the connector's <send> action to pre-test both infected and non-infected files. A harmless "infected" file can be found here: http://www.eicar.org/85-Download.html

To enable antivirus scanning of incoming files:

- Activate the Standalone Actions>Antivirus Scan action.
- Within the Antivirus Scan action, change the *scanner*, *errorMessage*, and *includeScanErrorMessage* parameters as necessary. These parameters are described within the action, as well as what happens when a scan fails.
- Keep the action as *Automatically Run at Startup*, as the action needs to register an incoming filter for subsequent inbound files. You can also run the action interactively to register the filter or re-register a modified filter.
- If you are setting up ICAP for a Harmony cluster, you must run the Antivirus Scan action manually on each node in the cluster or restart each node.
- Disabling or deleting the Antivirus Scan action will disable or delete the filter.

NOTE: The location of the ICAP connector and Antivirus Scan action in relation to the partner hosts dictates which incoming payload is in-scope and scanned. For more information, refer to Standalone Actions in the Cleo Harmony Online User Guide.

ICAP Connector Properties

Each instance of the ICAP Connector can be configured using the following settings:

Property	Description	Required
Address	The host server connection address.	Yes
Port	The host server connection port.Valid range: [1-65535].	Yes
ICAP Service	The name of the antivirus service on the ICAP server.	Yes
Response Profile	The response header returned when an infection is found.	Yes
Override Transfer Ignore	If enabled, the 'Transfer-Ignore' response header is ignored and all files are sent to the ICAP server for scanning regardless	
Maximum Size	A positive integer value limits the maximum content size (in bytes) to be sent to the ICAP server post-preview. Any other value implies no limit.	Yes
Request Method	The ICAP request method to use. The default value is RESPMOD.	
Command Retries	The number of times the command should be retried when an error or exception occurs.Valid range: [0-5].	Yes
Command Retry Delay (seconds)	The number of seconds to wait between retries. Valid range: [O-120].	Yes
Do Not Send Zero Length Fies	For PUT, a switch that controls whether to send a file if it is zero-length.	
Enable Debug	A switch that controls whether to perform debug logging.	
System Scheme Name	The URI scheme name used as a shortcut to this host.Valid pattern: `[[a-zA-Z){1}[a-zA-Z0-9+\-\.]{ 1,23}]`.	
System Public	A switch that indicates whether the connector is public.	

Kafka Connector

The Kafka Connector is used to communicate with Apache Kafka system. In Kafka, messages are stored in queues that are managed by Kafka brokers. Kafka broker maintains topics to which the processes using Kafka can subscribe. A message to a Kafka topic is published using Kafka Producer and messages can be read from Kafka using Kafka

Consumer. A topic can be divided into partitions that can exist across multiple brokers. A partition is identified with an integer value. A message to a Kafka queue can be published using the PUT command in the following format.

```
PUT sourcepath <partition>/<key>/
```

Examples:

```
PUT test/testfile.txt
```

```
PUT test2/testfile2.txt 1/somekey
```

Here the partition and key are optional. In the example, the first command publishes the content of the file `*test/testfile.txt*` to the configured Kafka topic. The next command publishes the content of the file `*test2/testfile2.txt*` to partition **1** of the configured topic with record key `*somekey*`.

Kafka Receiver can be enabled by checking `*Enable Receiver*`, setting `*PollIntervalMs*` to a positive integer value and setting `*Consumer Group Id*`. When Kafka Receiver is enabled, messages are polled and stored in the inbox. Receiver receives messages from Kafka Consumer as *String* and then converts them to *byte stream* while creating a Receive instance.

Security

Kafka supports SSL and SASL authentication and encryption. Kafka Connector supports both SSL and SASL authentication. For SASL authentication, Kakfa connector supports the PLAIN, SCRAM-SHA-256 and SCRAM-SHA-512 SASL mechanisms. It also supports both one-way and two-way authentication.

To enable basic one-way authentication using SSL select the *Enable SSL* check box, upload your client trust store, and enter the password for client trust store. Client trust store should have the server's root certification install in it. Kafka broker should be started with SSL authentication enabled.

To enable two-way authentication, select the "Enable Client Authentication" check box. Then, upload the client keystore, and enter the keystore password and key password. The client root certificate should be installed in the broker trust store.

For the SASL authentication, the Username and Password must be entered.

For information about how to enable SSL authentication on the broker, see the Kafka security documentation: https://kafka.apache.org/documentation/#security

File size limit

File size limit (in the connector) can be configured by setting *MessageMaxByteSize*, the default size is **1 MB**. Kafka broker by default has a message size limit of 1 MB which can be configured by setting *message.max.byte* (in server properties). In order to increase the message size both these settings must be changed.

Kafka Connector Properties

Each instance of the Kafka Connector can be configured using the following settings:

Property	Description	Required
Host Cluster	The host cluster.	Yes
Topics	Kafka topics. Comma-separated (topic1,topic2)Valid pattern: `[([a-zA-Z0-9]|-|_|\.){0,249}]`	Yes

Property	Description	Required
SASL Mechanism	SASL mechanism used to connect (Kafka property 'sasl.mechanism' property). Must match one of the servers 'sasl.enabled.mechanisms' setting values.	Yes
SASL Security Protocol	SASL security protocol used to connect (Kafka property 'security.protocol'). Must match the servers scheme of the 'listeners' (or 'advertised.listeners') setting matching the port in 'Host Cluster'.	Yes
Username	Username for SASL connection. Used to build Kafka 'sasl.jaas.config' property.	
Password	Password for SASL connection. Used to build Kafka 'sasl.jaas.config' property.	
Enable Receiver	Enable Kafka receiver client. Once set, the Kafka receiver will start polling from the topics.	
Poll Interval Ms	Intervals at which Kafka consumer needs to be polled.	
Auto Commit Offset	Kafka optbn for auto commit offset. (Kafka consumer property 'enable.auto.commit')	
Auto Commit Interval Ms	Auto-commit interval_ms in case the auto commit offset is enabled. (Kafka consumer property 'auto.commit.interval ms.ms')	Yes
Consumer Group Id	Kafka consumer group id. (Kafka consumer property 'group.id')	Yes
Poll Time Out Ms	Incoming poll timeout.	
Fetch Min Bytes	The minimum amount of data the server should return for a fetch request. If insufficient data is available the request will wait for that much data to accumulate before answering the request. The default setting of 1 byte means that fetch requests are answered as soon as a single byte of data is available or the fetch request times out waiting for data to arrive.	Yes

Property	Description	Required
Heartbeat Interval Ms	The expected time between heartbeats to the consumer coordinator when using Kafka's group management facilities. Heartbeats are used to ensure that the consumer's session stays active and to facilitate rebalancing when new consumers join or leave the group. The value must be set lower than session.timeout.ms, but typically should be set no higher than 1/3 of that value. It can be adjusted even lower to control the expected time for normal rebalances.	Yes
Max Partition Fetch Bytes	The maximum amount of data per partition the server will return. Records are fetched in batches by the consumer. If the first record batch in the first non-empty partition of the fetch is larger than this limit, the batch will still be returned to ensure that the consumer can make progress.	Yes
Session Timeout Ms	The timeout used to detect consumer failures when using Kafka's group management facility. The consumer sends periodic heartbeats to indicate its liveness to the broker. If no heartbeats are received by the broker before the expiration of this session timeout, then the broker will remove this consumer from the group and initiate a rebalance.	Yes
Auto Offset Reset	What to do when there is no initial offset in Kafka or if the current offset does not exist anymore on the server (for example, because that data has been deleted): • earliest: automatically reset the offset to the earliest offset • latest: automatically reset the offset to the latest offset • none: throw exception to the consumer if no previous offset is found for the consumer's group • anything else: throw exception to the consumer.	Yes

Property	Description	Required
Default Api Timeout Ms	Specifies the timeout (in milliseconds) for consumer APIs that could block. This configuration is used as the default timeout for all consumer operations that do not explicitly accept a timeout parameter.	Yes
Exclude Internal Topics	Whether records from internal topics (such as offsets) should be exposed to the consumer. If set to true, the only way to receive records from an internal topic is by subscribing to it.	Yes
Fetch Max Bytes	The maximum amount of data the server should return for a fetch request. Records are fetched in batches by the consumer, and if the first record batch in the first non-empty partition of the fetch is larger than this value, the record batch will still be returned to ensure that the consumer can make progress. As such, this is not an absolute maximum. The maximum record batch size accepted by the broker is defined by message.max.bytes (broker config) or max.message.bytes (topic config). Note that the consumer performs multiple fetches in parallel.	Yes
Isolation Level	Controls how to read messages written transactionally.If set to read_committed, consumer.poll() will only return transactional messages that have been committed.If set to read_uncommitted (the default), consumer.poll() will return all messages, even transactional messages that have been aborted. Non-transactional messages will be returned unconditionally in either mode.	Yes

Property	Description	Required
Max Poll Interval Ms	The maximum delay between invocations of poll() when using consumer group management. This places an upper bound on the amount of time that the consumer can be idle before fetching more records. If poll() is not called before this timeout expires, then the consumer is considered failed and the group will rebalance in order to reassign the partitions to another member.	Yes
Max Poll Records	The maximum number of records returned in a single call to poll().	Yes
Partition Assignment Strategy	The class name of the partition assignment strategy that the client will use to distribute partition ownership amongst consumer instances when group management is used.	Yes
Send Buffer Bytes	The size of the TCP send buffer (SO_SNDBUF) to use when sending data. If the value is -1, the OS default will be used.	Yes
Acks	Controls the criteria under which requests are considered complete. When writing to Kafka, producers can choose whether they wait for the message to be acknowledged by 0, 1, or all (-1) replicas.	Yes
Delivery Timeout Ms	Kafka producer property delivery.timeout.ms. An upper bound on the time to report success or failure after a call to send() returns. This limits the total time that a record will be delayed prior to sending, the time to await acknowledgment from the broker (if expected), and the time allowed for retriable send failures.	Yes

Property	Description	Required
Compression Type	The compression type for all data generated by the producer. The default is none (that is, no compression). Valid values are **none**, **gzip**, **snappy**, **lz4**, or **zstd**. Compression is of full batches of data, so the efficacy of batching will also impact the compression ratio -- more batching means better compression.	Yes
Linger Ms	Kafka producer property linger.ms. Wait period for buffer space to be filled before sending the message.	Yes
Client Id	An id string to pass to the server when making requests. The purpose of this is to be able to track the source of requests beyond just ip/port by allowing a logical application name to be included in server-side request logging.	
Max Bbck Ms	The configuration controls how long KafkaOutgoing.send() and KafkaOutgoing.partitbnsFor() will block. These methods can be blocked either because the buffer is full or metadata is unavailable. Blocking in the user-supplied serializers or partitioner will not be counted against this timeout.	Yes
Max Request Size Bytes	The maximum size of a request in bytes. This setting will limit the number of record batches the producer will send in a single request to avoid sending huge requests. This is also effectively a cap on the maximum record batch size. Note that the server has its own cap on record batch size which may be different from this.	Yes
Partitioner Class	Partitioner class that implements the org.apache.kafka.cfients.producer.Partitioner interface.	Yes

Property	Description	Required
Batch Size Bytes	The producer will attempt to batch records together into fewer requests whenever multiple records are being sent to the same partition. This helps performance on both the client and the server. This configuration controls the default batch size in bytes.	Yes
Buffer Memory Bytes	The total bytes of memory the producer can use to buffer records waiting to be sent to the server. If records are sent faster than they can be delivered to the server, the producer will block for max.bbck.ms after which it will throw an exception.	Yes
Enable Idempotence	The idempotent producer strengthens Kafka's delivery semantics from at least once to exactly once delivery. In particular, producer retries will no longer introduce duplicates. If set, the retries config will default to Integer.MAX VALUE and the acks config will default to all.	Yes
Retries	If the request fails, the producer can automatically retry. Enabling retries also opens up the possibility of duplicates.	Yes
Message Max Size Bytes	Message size limit for sending. Increasing this value will enable sending larger files from the connector. Broker configuration also needs to be changed to receive larger files. This value should be the same as message.max.bytes on broker confiq.	Yes
Connections Max Idle Ms	Close idle connections after the number of milliseconds specified by this config.	Yes
Receive Buffer Bytes	The size of the TCP receive buffer (SO_RCVBUF) to use when reading data. If the value is -1, the OS default is used.	Yes

Property	Description	Required
Request Timeout Ms	Controls the maximum amount of time the client will wait for the response to a request. If the response is not received before the timeout elapses, the client will resend the request if necessary or fail the request if retries are exhausted.	Yes
Client DNS Lookup	Controls how the client uses DNS lookups. If set to use_all_dns_ips, when the lookup returns multiple IP addresses for a hostname, attempts are made to connect all before failing the connection. Applies to both bootstrap and advertised servers. If the value is resolve_canonical_bootstrap_servers_only each entry will be resolved and expanded into a list of canonical names.	Yes
Enable SSL	Enable Authentication and Encryption using SSL protocol.	
SSL Trust Store	Upload SSL TrustStore file.	
Trust Store Password		
Enable Client Authentication	Enable server authenticating client	
SSL Key Store	Upload the keystore file	
SSL Keystore Password	Password for keystore	
SSL Key Password	Password for certificate	
SSL Trust Store Type	SSL Truststore type	
SSL Keystore Type	SSL Keystore type	
SSL Provider	Name of security provider for SSL connection.	
SSL Cipher Suite	A cipher suite is a named combination of authentication, encryption, MAC, and key exchange algorithm used to negotiate the security settings for a network connection using TLS or SSL network protocol.	
SSL Enabled Protocol	It should list at least one of the protocols configured on the broker side	

Property	Description	Required
SSL Endpoint Identification Algorithm	The endpoint identification algorithm to validate server hostname using server certificate.	
Command Retries	The number of times the command should be retried when an error or exception occurs.Valid range: [0-5].	Yes
Command Retry Delay (seconds)	The number of seconds to wait between retries.Valid range: [0-120].	Yes
Do Not Send Zero Length Files	For PUT, a switch that controls whether to send a file if it is zero-length.	
Delete Received Zero Length Files	For GET, a switch that controls whether to remove a received file that is zero-length.	
Retrieve Directory Sort	For PUT, the sorting options for the list of outbound files.	
Enable Debug	A switch that indicates whether to perform debug logging.	
System Scheme Name	The URI scheme name used as a shortcut to this host.Valid pattern: `[[a-zA-Z]{l}[a-zA-Z0-9+\-\.]{l,23}]`.	
System Public	A switch that indicates whether the connector is public.	

LDAP Connector

The LDAP connector is used to provision and authenticate users against a directory service using LDAP. The connector supports both DNS lookup or manual configuration of SRV records. Several user attribute fields can be configured, but only username and email address are required.

Below are sample base organizational units for the different directory types:

- Active Directory: `'OU=Employees,DC=company,DC=com'`
- Apache Directory Services: `'OU=Users,DC=example,DC=com'`
- Apache Directory Services: `'OU=Users,DC=example,DC=com'`
- Lotus Domino: `'O=SCNotes'`
- Novell eDirectory: `'O=Company Organization'`
- DirX: `'ou=Users,o=Company'`

And below are example search filter attribute names and values:

- `'department=EDI'` limits to entries that match the attribute *name=value*.
- `'department=EDI,group=administrators'` limits to entries that match two attributes.
- `'department=EDI,telephoneNumber=800*'` limits to an attribute that starts with a value.

- `'objectclass=person'` limits to just people; it can contain other entries (for example, computers).
- `'!(userAccountControl:1.2.840.113556.1.4.803:=2)'` excludes disabled accounts

In Active Directory, if an account is disabled, *bit 0x02* in the *userAccountControl* attribute value is **on**. 1.2.840.113556.1.4.803 is the rule object ID (*ruleOID*) for the LDAP bitwise `AND` operator.

Finally, these are the typical username attributes for the different directory types:

- Active Directory: `'sAMAccountName'`
- Apache Directory Services: `'uid'`
- Lotus Domino and Novell eDirectory: `'CN'`
- DirX: `'cn'`

To then use an LDAP connector, go to a Users' mailbox and select the *Connector Host Authentication Type*. Point to the LDAP connector by using a URI reference (for example *ldap:External* where *External* is the LDAP host connector alias).

Notes:

- Use the *Test Authentication* and *List Users* buttons to validate that authentication is working and that the expected list of users and attributes is returned.
- The configured Base DN and Search Filter property values can be overridden when using the connector for a specific user mailbox by adding URI request parameters (for exmple, *ldap:External?SearchFilter=department=EDI*). Furthermore, the configured SearchFilter can be extended rather than overridden by adding '.extend' to the name (for example, *ldap:External?SearchFilter.extend=,department=EDI*).
- Multiple LDAP connectors can be configured and then used across different user mailboxes. The LDAP server configured within system options can still be used as well, but is limited to a single directory service.
- You must provide values for the following properties:
  - Directory Type
  - Security Mode
  - SRV Records
  - Base DN
  - Username Attribute
  - Email Address Attribute
  - User UID Attribute
  - Sync Account User Name
  - Sync Account Password

LDAP Connector Properties

Each instance of the LDAP Connector can be configured using the following settings:

Property	Description	Required
Directory Type	The product used for the LDAP directory service.	Yes
Security Mode	If the directory server requires using SSL, specify a security mode. Otherwise, select None.	Yes
SRV Records	The LDAP SRV records.	Yes

Property	Description	Required
DNS Domain Name	The DNS domain name from which you want to look up SRV records.	
Automatic DNS Lookup	Automatically look up SRV records at runtime using DNS.	
Base DN	The base organizational unit where the users are defined. Contact your directory administrator for the correct Base DN value.	Yes
Search Filter	Used to limit the amount of information returned from the LDAP server when many users are defined. A more restrictive filter can be specified as a comma-separated `attribute name=value` list. Characters that have special meaning – `* ( ) \ ,` – need to be escaped with a `\` if they are part of a search value. A two-character hex representation can also be used (for example, `NUL`is `\00`). If necessary, contact your directory administrator to determine the appropriate filter.	
Username Attribute	The directory attribute that matches the username entered when a login is required.	Yes
Email Address Attribute	The directory attribute that is the user's email address.	Yes
Phone Attribute	The directory attribute that is the user’s registered phone number.	
First Name Attribute	The directory attribute that is the user's first name.	
Last Name Attribute	The directory attribute that is the user's last name.	
Full Name Attribute	The directory attribute that is the user's full name.	
Home Directory Attribute	The directory attribute that is the user's home directory path.	
User UID Attribute	Required field for user ID lookup if using SAML Single Sign On. This directory attribute must match the SAML assertion NameId value passed by the IDP in order for a user to successfully log in through SAML.	Yes

Property	Description	Required
Sync Account User Name	Username for extracting the users from the LDAP directory service.	Yes
Sync Account User Password	Password value for the Sync Account User Name.	Yes
Enable Debug	A switch that indicates whether to perform debug logging.	
System Scheme Name	The URI scheme name used as a shortcut to this host.Valid pattern: `[[a-zA-Z]{l}[a-zA-Z0-9+\-\.]{l/23}]`.	
System Public	A switch that indicates whether the connector is public.	

Router Connector

The router connector is included with Cleo Harmony.

On the `Template` tab in the host tree under `Connections>Generic>Generic ROUTER`, select `Clone and Activate` and a new `ROUTER` connection (host) will appear on the `Active` tab.

The new `ROUTER` needs to have one or more routes defined. From the `ROUTER` tab, click the `...` on the right of the `Routing Table` line. Enter `214` in the `Type` column and `local/root/${base}.${icn}${ext}` in the `Destination` column.

Create a sample EDI file in `$CLEOHOME/outbox/test.edi` from the content below:

```
ISA*00*          *00*          *02*SCAC           *01*006922827HUH1
 *080903*1132*U*00401*000010067*0*P*>~
GS*QM*SCAC*006922827HUH1*20080903*1132*9951*X*004010~
ST*214*099510001~
B10*4735103*5365205*SCAC~
L11*5365205*LO~
L11*01*QN~
L11*392651*PO~
L11*392651*PO~
N1*SH*HUHTAMAKI FSBU~
N3*5566 NEW VIENNA ROAD~
N4*NEW VIENNA*OH*45159*US~
N1*CN*HUHTAMAKI~
N3*100 HIGGENSON AVE~
N4*LINCOLN*RI*02865*US~
LX*1~
AT7***AA*NA*20080903*16000000*ET~
MS1*NEW VIENNA*OH*US~
AT8*G*L*6240*402~
SE*17*099510001~
```

Note: this sample is drawn from Ryder's EDI documentation here.

Change the default `<send>` action to read `PUT test.edi` (instead of `PUT -DEL *`) and run the action. You will find a routed file `test.000010067.edi` as output in `local/root`.

Router Connector Properties

Each instance of the Router Connector can be uniquely configured using the following settings:

Setting	Description
Routing Table	The heart of Router Connector configuration is an ordered set of routing rules organized in a routable. These rules define destinations based on analysis of the filename and file content. See The Routing Table.
Route To First Matching Route Only	If this option is selected, only a single output will be produced for each routed message, based on the first routing table entry matched (the routing table columns can be ordered). Otherwise, multiple outputs per message will be produced, one for each matching route.
Preview Size	EDI and HL7 files are analyzed based on their known structure. Other files are analyzed by matching the first portion of the file content against some matching patterns that can extract tokens for route matching (such as XML elements). The Preview Size is the amount of data buffered from the initial portion of non-EDI/HL7 files for this analysis. See Named Content Patterns.
Preview EDI Segments	For EDI files, the number of additional segments to buffer beyond the transaction set header for use in the `segment` and `segments` functions. See A word about segment (id).
Preview EDI Stop Segment	For EDI files, the name of a segment that should halt preview buffering before the full Preview EDI Segments limit has been reached. See A word about `segment(id)`.
Error Destination	Files not matching any routes may be discarded (and the file transfer will fail). Alternatively, files that cannot be routed may be copied to an error destination (and the file transfer will end with a warning status).
Force Unique	If this option is selected, route destinations (and the error destination) will never overwrite existing content, even if `PUT -UNI` is not used in an action. This option may be useful when the router is used as a URI (e.g. `router:...`) as an inbox or in an LCOPY in other parts of Harmony where the `-UNI` option may not be specified in context.

Improperly Padded ISA Handling	X12 envelopes begin with a fixed length `ISA` segment. In some cases, the partner identifiers (`ISA06` and `ISA08`) are not properly padded to the required 15-character width by trading partners. These improperly formed X12 envelopes are treated as errors by default (`Forward to Error Destination`), but the router may be configured to ignore (`Route as is`) or correct (`Correct and Route`) these malformed `ISA` segments using this option.

The Routing Table

The routing table is an unordered list of matching rules that specify the routing destination.

Enabled	Filename	Content	Sender	Receiver	Group Sender	Group Receiver	Function	Type	Condition	Destination	Max Messages

All matching columns are regular expressions except:

- the `Condition` is a general JavaScript expression to express conditions beyond simple pattern matching (blank means `true`),
- the `Destination` is a template with embedded JavaScript expressions (enclosed in `${...}`) used to calculate the destination location, and
- `Max Messages` is an integer (blank or `0` means no limit)

If a matching column is left blank in a routing table entry, then it always matches the associated criterion.

The routing process proceeds in stages:

1. First, the filename is matched against the `Filename` rules, and any rules not matching a specified pattern are eliminated from further matching.
2. Next, the file content is inspected, with three possible outcomes: EDI (X12, EDIFACT, or TRADACOMS are supported), HL7 or not EDI.
3. Based on the classification of the file, metadata is extracted for further routing. If the file is EDI or HL7, the standard envelope headers are parsed and the Sender, Receiver, Group Sender, Group Receiver, Function, and transaction Type are extracted. The qualifiers for the sender and receiver IDs are also extracted, although they are not used for routing. Rules with a `Content` pattern are eliminated from further consideration for EDI files.
4. For non-EDI files, a preview buffer is loaded from the file and is matched against the `Content` pattern. Rules whose `Content` pattern is empty or does not match the preview are eliminated from further consideration. Matching rules are then inspected for named capture groups, which then populate a metadata object for the file (see Metadata Extraction below).
5. The extracted metadata is now matched against the corresponding patterns in the remaining rules. If a `Condition` expression is provided, it is also evaluated (see Condition Expressions below). Rules all of whose metadata patterns match the file and whose `Condition` is satisfied are considered activated.
6. For each activated rule, the `Destination` template is expanded to calculate the destination filename. Expressions of the form `${expression}` are replaced with the appropriate values (which can be simple metadata tokens or arbitrary JavaScript expressions — see Destination Expressions below).
7. The file contents are copied to the destination(s).
8. If a file matches no routes, but an error destination is configured, the file is copied to the error destination. Note that metadata tokens can be expanded in the error destination string.
9. If a file matches no routes and no error destination is configured, the transfer ends in error.

EDI Splitting

EDI files differ from non-EDI files not only in the way metadata is parsed. Since EDI segments are formally structured with starting and ending segments, it is common for files to contain separate EDI interchanges simply concatenated in a single file.

When the router discovers an EDI file, it automatically separates the interchanges into messages (for example, `ST...SE` for X12), and routes each independently. Sequences of messages that activate the same set of routes are concatenated into the output destinations, including the necessary enveloping segments to enclose the messages in groups and interchanges. It is also possible that messages in a single group or interchange may be routed to different destinations, in which case the enclosing interchange and group envelopes will be included as needed in each destination.

It is possible for some messages to route successfully while others fail to match any routing rules. In this case, the overall transfer will fail even if some messages were routed successfully.

Non-EDI Preview Size

Metadata extraction for non-EDI files requires that first a preview of the file content is read from the source file for matching against the `Content` pattern. The `Preview Size` is configured as a property of the Router Connector, and defaults to `8k`. You may enter values for the `Preview Size` using *human-readable* suffixes for convenience. In the table below,*nnn* represents an arbitrary integer value.

Preview Size	Result
nnn	up to *nnn* bytes are loaded for preview
*nnn*k or*nnn*kb	*nnn* kibibytes (× 1024) bytes are loaded
*nnn*m or*nnn*mb	*nnn* mebibytes (× 1024²) bytes are loaded

The preview buffer is held entirely in memory, so be mindful of practical resource limits when configuring the preview size.

HL7 Handling

HL7 is a bit different in structure from the three supported EDI standards. When an HL7 file is detected, the `MSH` segment is parsed and some of its fields are mapped to the routing table entries as described here. Unlike the EDI formats, HL7 files are not split, so the file is not inspected for subsequent `MSH` segments.

Item	Type	Length	Description	Mapped To
MSH-01	ST	1	Field separator	
MSH-02	ST	4	Encoding characters	
MSH-03	HD	180	Sending Application	`groupSender` and `groupSenderQualifier`
MSH-04	HD	180	Sending Facility	`sender` and `senderQualifier`
MSH-05	HD	180	Receiving Application	`groupReceiver` and `groupReceiverQualifier`
MSH-06	HD	180	Receiving Facility	`receiver` and `receiverQualifier`

Item	Type	Length	Description	Mapped To
MSH-07	TS	26	Date/Time Of Message	
MSH-08	ST	40	Security	
MSH-09	ST	7	Message Type	`type` and `function`
MSH-10	ST	20	Message Control ID	`icn`
MSH-11	PT	3	Processing ID	
MSH-12	ID	8	Version ID	
MSH-13	NM	15	Sequence Number	
MSH-14	ST	180	Continuation Pointer	
MSH-15	ID	2	Accept Acknowledgment Type	
MSH-16	ID	2	Application Acknowledgment Type	
MSH-17	ID	2	Country Code	
MSH-18	ID	6	Character Set	
MSH-19	CE	60	Principal Language Of Message	

The HL7 Message Type comprises a message type ID and trigger event ID. The message type ID is mapped to the EDI `type` and the trigger event ID is mapped to the `function`. For example, a message with a MSH-09 message type of `ADT^A04` would be parsed into a `type` of `ADT` (Admit Discharge Transfer) with a `function` of `A04` (Register a patient).

The sender and receiver HL7 types are `HD` (Hierarchic Designator), which can have up to three sub-composites, with the first part optional. If more than two parts are found, the first part is discarded, the second mapped to the appropriate identifier, and the third is mapped to the associated qualified. If two parts are found, the first and second are mapped to the identifier and its qualifier. If there are no sub-composites, the entire value is mapped to the identifier and the qualifier is blank.

HL7 detection depends on successfully parsing the `MSH` segment into at least 12 parts (up to `MSH-12` "Version ID") and a Version ID that starts with `2.`.

Metadata Extraction

For non-EDI files for which a preview is matched against a `Content` filter pattern, the filter pattern may include capture groups that describe metadata values to extract from the content.

Named capture groups are expressed in a pattern as `(?<token>pattern)` where `token` is one of the supported token names from the list below and `pattern` is a regular expression matching the content to be extracted.
For example, if a route is matching an XML document that may contain embedded elements `<sender>some value</sender>` or `<receiver>some value</receiver>`, the following expression will match and extract the `some value` portions, irrespective of the order in which the `<sender>` and `<receiver>` elements appear in the document:

```
(?:.*?(?:<sender>(?<sender>[^<]*)</sender>|<receiver>(?<receiver>[^<]*)</
receiver>))*.*
```

The anatomy of this regular expression comprises:

- an outer framework of `(?:.*?thing)*.*` (keep in mind that `(?:pattern)` is a non-capturing grouping expression) which means a sequence of interesting `thing`s, separated by padding text `.*?`, followed by arbitrary padding text `.*`.
- a definition of `thing` as a choice between alternatives `(?:a|b)` (this could be extended to `(?:a|b|c|...)` as needed).
- each alternative is an XML fragment `<tag>value</tag>`.
- each `value` is captured as a token `(?<token>...)` and contains arbitrary text up to the closing tag `[^<]*`.

The following metadata tokens are supported (the tokens are case sensitive):

Expression	Description
`file`	the source filename
`base`	the base portion of the filename (.extension removed)
`ext`	the filename extension (including the . prefix)
`sender`	the sender metadata
`receiver`	the receiver metadata
`groupSender`	the functional group sender metadata
`groupReceiver`	the functional group receiver metadata
`function`	the functional group identification
`type`	the transaction type
`icn`	the interchange control number

Named `Content` Patterns

Often when routing based on parsed content a single metadata extraction and matching pattern will be used to select between multiple destinations based on the extracted values (since EDI and HL7 have well-known fixed schemas, the routing table naturally supports this use case).

Since the routing table combines the metadata extraction pattern in the `Content` column with metadata matching patterns in the `Sender`, `Receiver`, etc. columns, the same `Content` metadata extraction pattern might have to be repeated for each matching pattern and destination:

Content	Sender	Destination
`.*?<token>(?<sender>[^<]*)</token>.*`	Acme	/files/inbound/acmebrands
`.*?<token>(?<sender>[^<]*)</token>.*`	Bigco	/files/inbound/bigfoods

To better support this kind of routing, the router connector allows `Content` patterns to be named and reused. A name starts with a letter a-z or A-Z, followed by any number of letters or digits a-z, A-Z, or 0-9. If a `Content` pattern starts with `name:`, any text following the `name:` will be parsed as the matching pattern and the metadata results will be stored and associated with `name`. Any subsequence references in the same routing table to `name:` without a pattern will re-use the same metadata.

Content	Sender	Destination
`sender:.*?<token>(?<sender>[^<]*)</token>.*`	Acme	/files/inbound/acmebrands
`sender:`	Bigco	/files/inbound/bigfoods

Since the `Destination` is technically optional (although no file will be delivered to an empty destination), the table can also designed to separate pattern definitions from references:

Content	Sender	Destination
`sender:.*?<token>(?<sender>[^<]*)</token>.*`		
`sender:`	Acme	/files/inbound/acmebrands
`sender:`	Bigco	/files/inbound/bigfoods

Often it is convenient to separate the metadata extraction patterns into multiple patterns, for example, when tokens may appear in any order. The named patterns can be combined to help with this:

Content	Sender	Receiver	Destination
`sender:.*?<from>(?<sender>[^<]*)</from>.*`			
`receiver:.*?<to>(?<receiver>[^<]*)</to>.*`			
`sender,receiver:`	Usinc	Acme	/files/inbound/acmebrands
`sender,receiver:`	Usinc	Bigco	/files/inbound/bigfoods

Note:

- If a pattern appears after a name list `name1,name2:pattern`, the `pattern` replaces any previous pattern for `name1`, but `name2` will reference a previous pattern.
- Whitespace may appear around the< code>,or before the `:`, but whitespace after the `:` is considered part of the pattern.
- To avoid having a pattern starting with `name:` being interpreted as a name instead of part of the pattern, surround it with a non-capturing group `(?:name:)`.

Destination Expressions

The route destination is a string that may include embedded expressions of the form `${expression}`. Any arbitrary JavaScript expression is supported as an `expression`, but typically simple variable references to metadata pre-loaded into the JavaScript engine's environment suffice.

The following primitives are supported:

Token	X12	EDIFACT	TRADACOMS	HL7	non-EDI
`sender`	ISA06	UNB02:1	STX02:1	MSH-04.2	`(?<sender>...)`

Token	X12	EDIFACT	TRADACOMS	HL7	non-EDI
receiver	ISA08	UNB03:1	STX03:1	MSH-06.2	(?<receiver>...)
groupSender	GS02	UNG02:1			(?<groupSender>...)
groupReceiver	GS03	UNG03:1			(?<groupReceiver>...)
senderQualifier	ISA05	UNB02:2		MSH-04.3	
receiverQualifier	ISA07	UNB03:2		MSH-06.3	
groupSenderQualifier		UNG02:2			
groupReceiverQualifier		UNG03:2			
function	GS01	UNG01		MSH-09.2	(?<function>...)
type	ST01	UNH09:1	MHD02	MSH-09.1	(?<type>...)
icn	ISA13	UNB05:1	STX05:1	MSH-10	(?<icn>...)
gcn	GS06	UNG05	BAT01		(?<gcn>...)
tscn	ST02	UNH01	MHD01		(?<tscn>...)
source['metadata']					
segment('ID')					
segments('ID')					

A word about `source['metadata']`

If a router connection is used directly through a URI reference as the inbox of another Harmony connection (or host or mailbox), additional protocol-specific metadata may be available in addition to the file content being routed. The metadata is represented as a JavaScript array (so use square brackets to access the values). Values available include:

Protocol	Key	Description
AS2	${source['AS2-From']}	The AS2-From (partner) name
	${source['AS2-To']}	The AS2-To (local) name
	${source['ClientServer.RoleIsServer']}	"Server" in a typical use case as described
	${source['Content-Disposition']}	HTTP.header.Content-Disposition |
	${source['Content-Type']}	HTTP.header.Content-Type |
	${source['DocDBTransferID']}	The Harmony REST API transfer ID |
	${source['HTTP.header.'+header]}	The HTTP header _header_ |
	${source['Protocol']}	"AS2" |

Protocol	Key	Description
	`${source['Subject']}`	The AS2 Subject |
	`${source['TransferID']}`	The Harmony transfer ID |
	`${source['VersaLex.Serial.Number']}`	The Harmony serial number, e.g. "HY1234"

A word about `segment('ID')`

While the router is breaking EDI content down to the message level, it parses and retains the envelope segments (interchange, group, and transaction set) to use in matching routes and for destination expressions. The router also reads ahead a number of additional segments (up to the *Preview EDI Stop Segment*, if configured, but no more than< em>Preview EDI Segments) inside the transaction set header, as in many cases these segments contain information that may be useful for routing in condition expressions or formatting into destination filenames.

The `segment` function (so use round brackets) provides access to these segments, elements, and subelements by name.

- `segment(name)` returns the entire segment for `name` (e.g. `segment('ISA')`)
- `segment(namenn)` returns element `nn` of segment`name` (e.g. `segment('ISA06')`)
- `segment(namenn.mm)` returns subelement `mm` of element `nn` of segment `name` (e.g. `segment('UNB02.2')`)

If a named segment appears more than once while buffering preview segments, the `segment` function returns the first named segment encountered. To access additional segments, use the `segments(name)` function, which returns a JavaScript array of segments using the same segment/element/subelement naming conventions as the `segment` function.

To construct routing condition expressions using the JavaScript array returned from the `segments(name)` function, the typical practice is to use the `array.every()` and `array.some()` methods to evaluate and condition over all or any of the values in the array. These methods take as an argument a testing function to apply over the array. For example, the condition expression:

```
segments("N102").some(function(s){return s=="SMITH";})
```

will be satisfied if any of the `N1` segments encountered has an `N102` element (free-form name) of `SMITH`. In order to simplify the use of the `every` and `some` methods, the router connector includes two built-in function generators:

- `match(regex)` generates a function that compares the array values to a regular expression
- `equal(string)` generates a function that compares the array values to a fixed string

So the previous example could be more simply expressed as:

```
segments("N102").some(equal("SMITH"))
```

Or if the requirement were to check that all encountered names contained a specific substring:

```
segments("N102").every(match(/XYZCO/))
```

While some of the simple primitives (`type`) could also be referenced (in a syntax-dependent way) by segment/element name (`segment('ST01')`), this mechanism provides access to additional data elements that are not represented as simple primitives.

File-level (EDI and non-EDI) primitives

The following file-level primitives are also supported, but do not depend on metadata extraction or EDI parsing:

Token	Description
`file`	the source filename
`base`	the base portion of the filename (.extension removed)
`ext`	the filename extension (including the . prefix)
`date('format')`	the current date/time formatted with'format'
`unique`	a uniqueness token, either empty or `.n` where`n` starts at`1` and counts up as needed
`counter`	a message counter, starting at`1`, incremented for each EDI message parsed

Examples

For example, the destination:

```
/path/${file}.${icn}${ext}
```

will expand the three embedded metadata variable references from the destination filename and file content parsing. This could also be expressed using JavaScript as:

```
/path/${file+'.'+icn+ext}
```

As a performance optimization, any JavaScript expression of the form `${token}` for one of the tokens above is expanded without invoking the JavaScript engine. Also, the primitives `${date('string')}` or `${date("string")}` are similarly expanded without invoking JavaScript. This means that although the two examples above produce the same result, the first one executes much more quickly.

Note that URI destinations are supported, so a destination of the form:

```
scheme:connection/path
```

can be used to route a file through a URI.

Unique Filenames

If the `-UNIque` option is used with the connector `PUT` command, the connector will test expanded destination expressions for existence in order to prevent overwriting an existing file. If the expanded destination exists, the connector begins inserting a uniqueness token into the filename until it can find an unclaimed filename. Uniqueness tokens include a leading `.` followed by the counter, e.g. `.1`, `.2`, etc.

The placement of the uniqueness token can be explicitly controlled by placing the `${unique}` token in the destination expression (or some JavaScript expression deriving a value from the `unique` string variable, which will either be empty or `.n` as described).

If a destination expression does not explicitly include `${unique}`, the uniqueness token will automatically be inserted just before the filename extension, or at the end of the filename if there is no extension, e.g.

- `filename.txt→filename.1.txt→filename.2.txt...`
- `filename→filename.1→filename.2...`

This calculation of unique filenames depends on route processing. In the context of a `PUT` command, this is easy to control. But when the use of the connector is most convenient through a URI `router:host` and `LCOPY` commands, the `-UNI` flag to `LCOPY` will not work. In this case, set the `Force Unique` property on the connector.

Condition Expressions

A Condition Expression may be provided as part of a route, in place of or in addition to matching columns. If a condition expression is provided, it must be a valid JavaScript expression (not enclosed in `${...}`). A condition is considered satisfied if:

- it evaluates to a boolean value `true`
- it evaluates to a numeric value other than `0` or `0.0`
- it evaluates to a non-empty string

Values of `null`, `false`, `0`, `0.0`, and `""` will prevent the route from matching.

The JavaScript expression may make use of all of the same variables and functions available in aDestination Expression. For example, a route with a matching `type` column value

```
204
```

could be equivalently expressed as a condition expression

```
type.match(/^204$/)
```

Keep in mind that the route matching columns areregular expressionsthat must match the entire value, not a substring match. This differs from the JavaScript `match` function illustrated above, which is a substring match. For example, consider the following table comparing `type` column matching with equivalent Condition expressions.

`type` Column	**Condition Expression**	**Meaning**
`204`	`type.match(/^204$/)`	full string match "only type `204`"
`204`	`type=="204"`	direct string equality "only type `204`
`.*2.*`	`type.match(/2/)`	substring match "any type containing `2`"
`2.*`	`type.match(/^2/)`	prefix match "any type starting with `2`"
`2.*`	`type.startsWith("2")`	prefix match "any type starting with `2`"

Condition expressions allow more expressive richness, but also make available metadata values pulled from segments or elements not represented as matching columns in the route table.

Condition Expression	**Description**
`senderQualifier=="ZZ"`	`senderQualifier` is available as a variable, but there is no route table column for it
`segment("B206")=="CC"`	Element 6 of the B2 segment (Shipment Method of Payment for an X12 204 Motor Carrier Load Tender) is "CC" (Collect)

S3 Connector

The S3 connector is used to communicate with the Amazon Simple Storage Service (Amazon S3). In Amazon S3, buckets and objects are the primary resources, where objects are stored in buckets. Amazon S3 has a flat structure without the hierarchy you might see in a typical file system. However, for organizational simplicity, the Cleo S3 connector supports the folder concept as a means of grouping objects. Therefore, you can treat your folder and file objects as you would in a standard hierarchical file system. For example:

```
PUT example.txt S3TestFolder/example.txt
```

This command transfers the local file, example.txt, to the configured S3 bucket within a "folder" object called S3TestFolder. Note that S3TestFolder must exist as an object in S3.

Notes:

- This connector supports server-side encryption. The methods supported at this time are Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) and with Amazon KMS-Managed Keys (SSE-KMS).
- The ATTR command currently supports a subset of all Amazon S3 attributes.
- The Pseudo Folders property can be used to control whether actual folder objects are created and needed by the connector.

User Metadata

The User Metadata property is a table of Key/Value pairs where the Key is a simple string, but the Value is an expression that can expand metadata available in a PUT operation. The Value expression supports a replacement token syntax, which supports filename tokens, additional tokens, and expressions to allow the Value to include formatted timestamps, source metadata, and JavaScript expressions.

Tokens and expressions are embedded in the Value using the `${expression}` syntax, where the simplest expression is a direct token reference. The following tokens and expressions are supported:

Token	Description
`file`	the filename including path and full filename
`filename`	the full filename, excluding the path
`path`	the filename path (filename removed, trailing / or \ included)
`base`	the base portion of the filename (path and .extension removed)
`noext`	the base portion of the filename (.extension removed)
`ext`	the filename extension (including the . prefix)
`date('format')`	the current date/time formatted with 'format' (see http://docs.oracle.com/javase/8/docs/api/java/text/SimpleDateFormat.html)
`source['metadata']`	metadata propagated from the source (see below)
`expression`	a JavaScript expression, possibly including the above

The following diagram describes the relationship between the various filename components:

```
/path/to/file/basefilename.extension
|<------------- file ------------->|
|<-- path -->||<---- filename ---->|
             |<- base ->||<- ext >|
|<-------- noext ------->||<- ext >|
```

For example, the following expressions all evaluate to the same result:

- ${path}${base}${ext}
- ${noext}${ext}
- ${file}

- ${path+base+ext}

As a performance optimization, any JavaScript expression of the form `${token}` for one of the tokens above is expanded without invoking the JavaScript engine. Also, the primitives `${date('string')}` or `${date("string")}` are similarly expanded without invoking JavaScript. This means that although the four examples above produce the same result, the first three execute much more quickly. But the JavaScript engine provides more capability for some use cases. This example illustrates computing a Value extracted from the last portion of the DocDBTransferID (a GUID):

```
${source.DocDBTransferID.replace(/.*-/,'')}
```

Source Metadata

If an S3 connection is used directly through a URI reference as the inbox of another Harmony connection (or host or mailbox), additional protocol-specific metadata may be available in addition to the file content being stored. The metadata is represented as a JavaScript array, so use square brackets to access the values. For example, values available for AS2 include the following:

Key	Description
`${source['AS2-From']}`	The AS2-From (partner) name
`${source['AS2-To']}`	The AS2-To (local) name
`${source['ClientServer.Role']}`	"Server" in a typical use case as described
`${source['Content-Disposition']}`	HTTP.header.Content-Disposition
`${source['Content-Type']}`	HTTP.header.Content-Type
`${source['DocDBTransferID']}`	The Harmony REST API transfer ID
`${source['HTTP.header.'+header]}`	The HTTP header "header"
`${source['Protocol']}`	"AS2"
`${source['Subject']}`	The AS2 Subject
`${source['TransferID']}`	The Harmony transfer ID
`${source['VersaLex.Serial.Number.Short']}`	The Harmony serial number, e.g. "HY1234"

To inspect the available metadata for a particular configuration, use a Value like the following:

```
${JSON.stringify(source)}
```

S3 Connector Properties

Each instance of the S3 Connector can be configured using the following settings:

Property	Description	Required
Access Key	Part of the AWS credentials; the access key ID.	Yes
Secret Access Key	Part of the AWS credentials; the secret access key.	Yes
Assume Role Arn	Role ARN to use when assuming an AWS role for special permissions. Leave blank if not assuming a role.	

Assume Role Duration (seconds)	Assume Role credentials duration. Must be in the range 900-43200 to conform to AWS specs. The resource owner may set a lower maximum than 43200.Valid range: [900-43200].	.
Assumed Session Name	Session name used when assuming an AWS role for special permissions.	
Assume Role External ID	External ID used to assume an AWS role if required by the policy owner. Optional when assuming a role.	
Assume Role Source Identity	Source identity of principal assuming the AWS role. The policy owner may require it, but it is optional when assuming a role.	
Canned Access Control List	The Canned Access Control List (ACL) to use when new S3 objects are created. Blank indicates no canned ACL deferring, to existing bucket trust poles.	
Region	The regional endpoint to use for this S3 connection. Defaults to DEFAULT_REGION.	
Bucket	The S3 bucket to use.	Yes
User Metadata	The list of user metadata key/value pairs to add to new S3 objects when they are created.	
Put Object Key	The object key (or key ${expression}) to use when creating a new S3 object, overriding the destination filename.	
Force Unique	Force new S3 Object keys to be unique, even if -UNI is not specified.	
Endpoint	The endpoint to use for the S3 connection.**Note**: It is recommended to use the Region setting instead of this setting. This setting should be configured only for non-standard S3 connections.	
Enable Path Style Access	Force path-style access to the bucket.**Note**: It is recommended to use the default setting instead of enabling this option. This setting should be configured only for non-standard S3 connections.	

Protocol	The protocol (for example, HTTP or HTTPS).	Yes
Use Gap	Whether gzip compression should be used.	
MuRipart Buffer Size (mbytes)	The part size used for a multipart upload.Valid range: [5-5120].	
Multipart Attempts	Number of times to try each part of a multipart transfer.Valid range: [1-10].	
Server side Encryption	The options for server-side encryption. Blank indicates no server-side encryption.	
Kms Key Id	The KMS Key ID to use when encrypting with KMS. Leave blank to use the default KMS key for the bucket.	
Pseudo Folders	Whether MKDIR/RMDIR should create/remove pseudo folder objects and where pseudo folder objects are required for DIR.	
Preemptive Basic Proxy Auth	Whether to attempt to authenticate preemptively against proxy servers using basic authentication.	
Client Execution Timeout (milliseconds)	The amount of time to allow the client to complete the execution of an API call.Valid range: [0-2147483647]	
Connection Max Idle Time (milliseconds)	The maximum amount of time that an idle connection may sit in the connection pool and still be eligible for reuse.Valid range: [0-9223372036854775807]	
Connection Timeout (milliseconds)	The amount of time to wait when initially establishing a connection before giving up and timing out.Valid range: Í0-2147483647]	
Connection TTL (milliseconds)	The expiration time for a connection in the connection pool.Valid range: [-1-9223372036854775807]	
Local Address	The optional local address the client will bind to.	
Max Connections	The maximum number of open HTTP connections allowed.Valid range: [2-2147483647]	

Request Timeout (milliseconds)	The amount of time to wait for the request to complete before giving up and timing out.Valid range: [0-2147483647]	
Response Metadata Cache Size	The response metadata cache size.Valid range: [0-2147483647]	
Signer Override	The name of the signature algorithm to use for signing requests made by this client.	
Socket Send Buffer Size Hint (bytes)	The optional size hint for the low-level TCP send buffer.Valid range: [0-2147483647]	
Socket Receive Buffer Size Hint (bytes)	The optional size hint for the low-level TCP receive buffer.Valid range: [0-2147483647]	
Socket Timeout (milliseconds)	The amount of time to wait for data to be transferred over an established, open connection before the connection times out and is closed.Valid range: [0-2147483647]	
Use Expect Continue	Whether "use expect continue" should be enabled.	
Use Reaper	Whether the IdleConnectonReaper is to be started as a daemon thread.	
Use Tcp Keep Alive	Whether or not to enable TCP KeepAlve support at the socket level.	
Use Throttled Retries	Whether throttled retries should be used.	
Use Transfer Acceleration	Whether S3 transfer acceleration should be used.	
Multipart Upload Threads	Number of threads to use for a multipart transfer.Valid range: [1-32].	
Command Retries	The number of times the command should be retried when an error or exception occurs.Valid range: [0-5].	Yes
Command Retry Delay (seconds)	The number of seconds to wait between retries.Valid range: [0-120].	Yes
Do Not Send Zero Length Fies	For PUT, a switch that indicates to not send a fife if it is zero-length.	
Delete Received Zero Length Fies	For GET, a switch that indicates to remove a received file that is zero-length.	

Retrieve Directory Sort	For PUT, the sorting options for the list of outbound files.
Enable Debug	A switch that indicates whether to perform debug logging.
System Scheme Name	The URI scheme name used as a shortcut to this host.Valid pattern: `[[a-zA-Z]{1}[a-zA-Z0-9+\-\.]{1,23}].`
System Public	A switch that indicates whether the connector is public.

SFTP Connector

The SFTP Connector supports a connection to a remote SFTP server. It is similar to

SSH FTP Host, but is packaged as a Connector instead of a Host. Most of the features of SSH FTP Host

are supported with the SFTP Connector, but as a Connector, it can be also used in a URI

reference for the Home Directory of a Users Host or as part of a Virtual subfolder.

Connector Access & Licensing

Connectors require separate licenses and are governed by commercial terms. Although all connectors are accessible in-product by default, usage beyond the Customer's contract is subject to audit and adjustment.

For compliance or subscription inquiries, please contact Cleo Sales.

SFTP Connector Properties

Each instance of the SFTP Connector can be configured with the following settings:

Property	Description	Required
Host	The hostname or IP address of the SFTP server.	Yes
Port	The port of the SFTP server (usually 22)	Yes
Connection Timeout (seconds)	The number of seconds to wait for an SSH connection to complete.	Yes
Username	The SSH username.	Yes
Connect.Password	The SSH authentication password.	
User Auth Key	The SSH authentication certificate.	
User Auth Key Password	The password for the authentication key.	Yes

Property	Description	Required
Proxies	Optional addresses of HTTP proxies to use for the connection. Connects to proxies using round robin. If there is a proxy connection failure, it will wait for 60 seconds before retrying that proxy.	
Maximum Packet Size	The SSH maximum packet size.	Yes
Preferred Compression Algorithm	The preferred SSH compression algorithm.	
Preferred Key Exchange Algorithm	The preferred SSH key exchange algorithm.	
Preferred Cipher Algorithm	The preferred SSH encryption algorithm.	
Preferred Mac Algorithm	The preferred SSH MAC algorithm.	
Preferred Public Key Algorithm	The preferred SSH public key algorithm.	
Resume Failed Transfers	Select to enable attempts to retry failed transfers.	
Resume Cache Size		
Command Retries	The number of times the command should be retried when an error or exception occurs.Valid range: [0-5].	Yes
Command Retry Delay (seconds)	The number of seconds to wait between retries.Valid range: [O-120].	Yes
Do Not Send Zero Length Fies	For PUT, a switch that controls whether to send a file if is it zero-length.	
Delete Received Zero Length Fies	For GET, a switch that controls whether remove a received file that is zero-length.	
Retrieve Directory Sort	For PUT, the sorting options for the list of outbound files.	
Enable Debug	A switch that indicates whether to perform debug logging.	
System Scheme Name	The URI scheme name used as a shortcut to this host.Valid pattern: `[[a-zA-Z]{ 1 }[a-zA-Z0-9+\-\.]{ 1,23}].`	
System Public	A switch that indicates whether the connector is public.	

PGP Encryption and Signing

The SFTP Connector supports Partner Packaging using PGP. When Partner Packaging is enabled for Outgoing transfers, files are optionally PGP encrypted, compressed and signed before they are transferred to the remote SFTP server using the PUT command. When Partner Packaging is enabled for Incoming transfers, files are decrypted, decompressed and have their signatures verified after they are retrieved from the remote SFTP server using the GET command.

PUT Command Properties

Set the following properties to enable and control PGP signing and encryption for files being PUT.

Property	Description
Outgoing.Partner Packaging	Select to enable PGP encryption and/or signing on PUT.
Type	Only pgp packaging is supported.
Encryption.Cert	Select the PGP certificate to use for encryption on PUT.
Encrypt	Select to enable PGP encryption on PUT.
Sign	Select to enable PGP signing on PUT.
Compress	Select to enable PGP compression on PUT.
Armor	Select to enable ASCII-armor encoding with PGP on PUT.
Compression Algorithm	Select the compression algorithm, if Compress is selected.
Encryption Algorithm	Select the encryption algorithn, if Encrypt is selected.
Hash Algorithm	Select the hash algoritm, ff Sign is selected.
V3 Signature	Select if V3 PGP signature should be used.

GET Command Properties

Set the following properties to enable and control PGP decryption and signature verification for files being retrieved with GET.

Property	Description
Incoming.Partner Packaging	Select to enable PGP decryption and/or signature verification on GET.
Type	Only pgp packaging is supported.
Decryption.Cert	Select the PGP certificate to use for decryption on GET.
Require Encryption	Fail GET for files that are not PGP encrypted.
Require Signature	Fail GET for files that are not PGP signed.
Decryption.Cert.Password	Provide the password for the Decryption Cert.

Algorithm Reference

The SFTP Connector supports the following SSH and PGP algorithms.

Type	Supported Algorithms
SSH Compression	zlipzlib@openssh.com
SSH Key Exchange	• curve25519-sha256@libssh.org • diffie-hellman-group-exchange-sha256 • diffie-hellman-group14-sha256 • diffie-hellman-group16-sha512 • diffie-hellman-group18-sha512
SSH Cipher	• aes256-ctr • aes192-ctr • aes128-ctr
SSH Mac	hmac-sha2-256
SSH Public Key	ssh-rsassh-dss
PGP Compression	zipzlib
PGP Encryption	• des • 3des aes/128 • aes/192 • aes/256 • cast5 • twofish • blowfish
PGP Hash	• md2 • md5 • ripemd160 • sha1 • sha256 • sha384 • sha512

SharePoint Connector

This connector is used to communicate with Microsoft SharePoint document libraries. SharePoint allows users to share files easily with each other via document libraries, also known as *drives*. A single site can contain multiple drives that can each contain both files and folders. The Cleo SharePoint connector supports creating directories and uploading and downloading files.

The SharePoint connector only supports Application Client authentication. For this, the user must configure an application that has the ability to access the SharePoint site in Azure AD. For more information, see Configuring an Azure application for Sharepoint Connector. During setup the 'TenantId', 'ApplicationId', and 'ApplicationSecret' properties must be obtained and set in the connector.

The path to files and folders must be in the format `hostname:siteName/driveName/fileOrFolder`. Please note that root sites will have only the hostname and not an additional site name. In this case, the path would be `hostname/driveName/fileOrFolder`.

The hostname and site name can be found in two different ways:

1. If a Directory Listing is performed without specifying `hostname:site`, available sites are listed and the path of the desired site can be used.
2. This information can be found in the web URL for the SharePoint site itself. If the URL for my SharePoint site is `https://test.sharepoint.com/sites/MySite`, the hostname is `test.sharepoint.com`, and the site name is `MySite`. If the URL looks like `https://test.sharepoint.com/`, it is the root site and no site name should be supplied.

If a Root Path is configured in the SharePoint properties tab, only resources located below this path are available to traverse. All paths in actions should be a continuation of the Root Path. For example, if the root path is set to `hostname:siteName`, all actions must include the `driveName` in the path, for example, `driveName/myFile.txt`. This allows the user to traverse multiple drives within the same connector host.

If the Root Path is not configured, the full path must always be specified in actions. This allows the user to traverse multiple different sites and drives in actions.

Notes:

- Directory Listings are the only operations that can be performed without specifying `hostname:siteName/driveName`.
- Performing a listing without specifying `hostname:siteName` will list available sites.
- Performing a listing where 'hostname:siteName' is specified but drive name is not will list available drives in that site.
- Renaming can be used to move files into different folders and even to different drives and sites as long as the Root Path property allows access to those resources.
- SharePoint allows deletion of folders that are not empty. Please be careful when deleting directories to avoid unintended deletions.

SharePoint Connector Properties

Property	Description	Required
TenantId	The ID of the tenant	Yes
ApplicationId	The Application ID of the registered application	
ApplicationSecret	The secret for the registered application	Yes
RootPath	The root path to use. This should be in the format `hostname:siteName/driveName/folder`.	
Command Retries	The number of times the command should be retried when an error or exception occurs.Valid range: [0-5].	Yes
Command Retry Delay	The number of seconds to wait between retries.Valid range: [0-120].	Yes

Do Not Send Zero Length Fies	For PUT, a switch that indicates to not send a fife if it is zero-length.
Delete Received Zero Length Fies	For GET, a switch that indicates to remove a received file that is zero-length.
Retrieve Directory Sort	For PUT, the sorting options for the list of outbound files.
Enable Debug	A switch that indicates whether to perform debug logging.
Proxy Address Proxy Port	Allows use of an HTTP proxy for connections to SharePoint.**Note**: VLProxy 3.10.0.5 is required if using VLProxy as the HTTP proxy.

SMB Connector

The SMB connector is used to communicate with network file shares using the Common Internet File System (CIFS) protocol, which is a dialect of the Server Message Block (SMB) protocol.

This connector allows access to a file share as a specific network user configured in the connector. A Share Path is defined through the SMB properties tab as the path that appears as the root of the files accessible through the connector. Files and folders at or below the Share Path are accessible while those above are not.

The connector will attempt to use the highest dialect set by the **Max Smb Version** and will negotiate down to the **Min Smb Version** until a dialect is selected that both the client and the server support.

A list of additional properties that can be added using "Additional SMB Properties" is available at https://jcifs.samba.org/src/docs/api/overview-summary.html#scp

To enable debugging for the underlying SMB library, select SMB: in the Include Debug Options found in *Administration* > *Logs*. Debug log messages are written to the standard debug log.

If running Cleo Harmony in FIPS mode, the FIPS mode option must be enabled for the connection to work correctly. When the SMB connector is running in FIPS mode the maximum protocol version is set to SMB 1 and the "jcifs.smb.client.useExtendedSecurity" is disabled as it requires ciphers that are not supported in FIPS.

Encryption is supported. See **Encrypt SMB3** in the table below.

NOTE:

- The SMB connector currently supports SMB 1 (NT LM 0.12), SMB2.02, SMB2.1, SMB3.0, SMB3.0.2, and SMB3.1.1

Property	Description	Required
Share Path	The SMB root path.Valid patterns: `[^smb://.*$, ^//.*$, ^%.^%]`.Custom macros may be used at the beginning of the path.	Yes
User Name	The host server connection account user name.	Yes

Property	Description	Required
User Password	The host server connection account user password.	Yes
Domain	The domain name.	
Max Smb Version	Set the maximum SMB version.	Yes
Min Smb Version	Set the minimum SMB version.	Yes
Smb Cache Expiration	The amount of time to cache attributes about a file.Valid pattern: `[[0-9]*].`	
Additional SMB Properties	Custom properties.	
Force Make Directories	Create parent folders that do not exist for a destination file.	
FIPS Mode	When running with FIPS this option must be selected. When FIPS Mode is enabled, only SMB 1 is supported.	
Command Retries	The number of times the command should be retried when an error or exception occurs.Valid range: [0-5].	Yes
Command Retry Delay (seconds)	The number of seconds to wait between retries.Valid range: [0-120].	Yes
Do Not Send Zero Length Files	For PUT, a switch that controls whether to send a file if it is zero-length.	
Delete Received Zero Length Files	For GET, a switch that controls whether to remove a received file that is zero-length.	
Retrieve Directory Sort	For PUT, the sorting options for the list of outbound files.	
Enable Debug	A switch that indicates whether to perform debug logging.	
System Scheme Name	The URI scheme name used as a shortcut to this host.Valid pattern: `[[a-zA-Z]{1}[a-zA-Z0-9+\-\.]{1,23}].`	
System Public	A switch that indicates whether the connector is public.	

Property	Description	Required
Encrypt SMB3	When true, SMB 3.0 and above will attempt to encrypt data. If the server does not support encryption, it will fall back to unencrypted communication. This option has no effect on SMB versions below 3.0. Default value is "True".	

Chapter

6

Scheduler

You can schedule actions to run based on a time and date or based on an event.

You use the Scheduler to run actions automatically at specific times, when files are present, or when certain events occur.

Scheduling actions - Native and Classic Web UI

You can schedule actions to run based on a time and date or based on an event.

You use the Scheduler to run actions automatically at specific times, when files are present, or when certain events occur.

1. In the native UI, select **Tools** > **Scheduler** in the menu bar or click **Schedule** in the toolbar.

   Each action and host action branch in the active tree pane is listed in the schedule table. Scheduled actions are listed at the top and unscheduled actions are listed below. Sorting by columns only affects the scheduled action rows.

   A schedule of actions that you can edit appears.
2. Select the action you want to schedule. You can right-click the action row and select **Schedule**, double-click the action row to select the action and display the **Scheduling** dialog box, or single-click the action row and click the clock icon.

   Alternatively, you can right-click a host or user mailbox action in the **Active** tab of the tree pane.

   The **Scheduling** dialog box appears.
3. In the **Scheduling** dialog box, select the **Run this action automatically** check box to enable the following scheduling options.

   - **polling for files**: checks your folder for the files at intervals you define and runs the action when files are present. See Scheduling actions to run automatically by polling for files on page 613.
   - **scheduled date/time**: applies date- and time-based scheduling for your action. See Scheduling actions to run at specific dates and times on page 612.
   - **events**: runs the action when the selected event occurs. See Scheduling actions to run based on events on page 615. **Cleo Harmony and Cleo VLTrader applications only.**

   Note: If you selected an action that is already scheduled, you can click **Edit** to modify the existing schedule. You can also clear the **Run this action automatically** check box to unschedule the action.
4. When you finish specifying values for scheduling parameters above and click **Schedule**.

   The **Scheduling** dialog box is dismissed and the new schedule information is displayed on the **Schedule** page

By default, the schedule does not automatically start when the application is started. You can, however, configure your system to run schedules at start up using the property **Automatically run schedules at startup**. See Other system options on page 729.

For the Cleo LexiCom application, the schedule will only run one action at a time. If more than one action is scheduled for the same time, the actions are run sequentially. If a scheduled action is still running when another action's scheduled time arrives, the action is not started until the running action ends.

For the Cleo Harmony and Cleo VLTrader applications, you control concurrently running scheduled actions using the property **Allow Scheduled Actions to Run Concurrently**. See Other system options on page 729.

Scheduling actions to run at specific dates and times

You can schedule actions to run automatically based on a weekly, monthly, or one-time period. For weekly and monthly scheduling, it is possible to set up multiple day and time ranges.

1. In the **Scheduling** dialog box, select **Run this action automatically**.
2. Select **at scheduled date(s) and time(s)**, and then click **Continue**.

   The **Schedule for** dialog box appears.
3. Specify a weekly, monthly, or one-time schedule. See Scheduling actions to run weekly on page 612, Scheduling actions to run monthly on page 613, and Scheduling actions to run one time on page 613 for more information.
4. After you specify a schedule, click **OK** on the **Schedule for** dialog box.

   The **Schedule for** dialog box is dismissed and the **Scheduling** dialog box appears.
5. Click **OK** on the **Scheduling** dialog box.

   Your action is scheduled and the schedule is reflected in the table of actions on the **Scheduler** page.

Scheduling actions to run weekly

You can schedule actions to run automatically on a weekly schedule. You can set up multiple day and time ranges.

1. In the **Schedule for** dialog box, select the **Weekly** radio button.
2. Select a time zone.

   The times you select for this schedule are relative to this time zone. The time zone you select is displayed in the **Scheduler** dialog box in the **Scheduled** column.
3. **Optional**: Select **Every Other Week** to run the action on alternating weeks. The action runs only on the selected days during those weeks.
4. Select one or more days of the week within the **Day(s) of Week** section.
5. Specify one or more start times (24-hour clock). A start time of `00:00` indicates 12:00 midnight; a start time of `17:00` indicates 5:00 PM.
6. **Optional**: For each start time, specify a recurrence. A recurrence can be scheduled either continuously, by selecting the **Recurring continuously** check box, or at an interval, by selecting the **Recurring every** check box and specifying the interval in hours, minutes, and seconds. Finally, choose when the recurrence should stop by selecting a time from the **Until** menu. An end time of `24:00` indicates the end of the day.
7. If a different time schedule is required on different days (for example, weekdays and weekends), click **New Day(s)** and repeat the steps above.

   When you configure multiple days, you can scroll through them using the arrow buttons in the upper left of the dialog box.

   You can click **Remove Day(s)** to delete the schedule for the days currently displayed.
8. Click **OK**.

   Your new schedule is saved and the schedule table is displayed, including your new schedule information.

Scheduling actions to run monthly

You can schedule actions to run automatically on a monthly schedule. You can set up multiple day and time ranges.

1. In the **Scheduling** dialog box, select the **Monthly** radio button.
2. Select a time zone.

   The time zone you select is displayed in the **Scheduler** dialog box in the **Scheduled** column.
3. Select one or more months and then one or more days of the month within the **Day(s) of Month** section.
4. Specify one or more start times (24-hour clock). A start time of `00:00` indicates 12:00 midnight; a start time of `17:00` indicates 5:00 PM.
5. **Optional**: For each start time, specify a recurrence. A recurrence can be scheduled either continuously, by selecting **Recurring continuously**, or at an interval, by selecting **Recurring every** and specifying the interval in hours, minutes, and seconds. Finally, choose when the recurrence should stop by selecting a time from the **Until** dropdown menu. An end time of 24:00 indicates the end of the day.
6. If a different time schedule is required on different months (for example, even months versus odd months), click **New Month(s)** and repeat the steps to specify days and times.

   When you configure multiple months, you can scroll through them using the arrow buttons in the upper left part of the dialog box.

   You can click **Remove Month(s)** to delete the schedule for the months currently displayed.
7. Click **OK**.

   Your new schedule is saved and the schedule table is displayed, including your new schedule information.

Scheduling actions to run one time

You can schedule actions to run automatically one time at a specific date and time.

1. In the **Scheduling** dialog box, select **One Time**.
2. Select a time zone.

   The time zone you select is displayed in the **Scheduler** dialog box in the **Scheduled** column.
3. Select a single year, month, day, and time.
4. Click **OK**.

   Your new schedule is saved and the schedule table is displayed, including your new schedule information.

Scheduling actions to run automatically by polling for files

You can configure your system to poll folders for files and then run actions automatically when files are present.

Note: This option is available only for **Commands** actions.

1. In the **Scheduling** dialog box, select the **Run this action automatically** check box, and then select **by polling for files**.
2. If you want to poll for files continuously, click **OK**.

   If you want to specify how often to poll for files, click **Edit**. The **Schedule for** dialog box appears. See Scheduling actions to run at specific dates and times on page 612 for more information.

   If you do not explicitly specify how often to poll for files, default polling period values are used.
3. Click **OK**.

Requirements when polling for files

When you set up an action to run by **polling for files**, the action will *potentially* be run according to the period you've configured. However, it will only *actually* run if one of these conditions are true:

- A PUT, PUT+GET, or LCOPY command within the action has a file to send or copy.
- The CHECK command is present in the action and specific conditions for that command are met.

Note that if an action contains both PUT/LCOPY and CHECK commands, it is the first command encountered that determines whether autosend properties (for PUT and LCOPY) or autocheck properties (for CHECK) are used. Since this could make it difficult to determine the actual schedule, actions designated for autocheck should contain only the CHECK command.

The frequency at which the scheduler checks to see if there are files to send or copy is controlled by the **Autosend Check Every** property. This indicates that even schedules set up for continuous polling are not actually continuous. Rather, their minimum frequency of polling is determined by **Autosend Check Every**.

PUT, PUT+GET, and LCOPY command rules

The following rules apply to actions containing PUT, PUT+GET, or LCOPY commands scheduled by polling for files.

- For an action to be scheduled this way, at least one of its PUT, PUT+GET, or LCOPY commands must use the delete after transfer (-DEL) option. For an action to be scheduled this way, at least one of its PUT, PUT+GET, or LCOPY commands must use the delete after transfer (-DEL) option, or LCOPY -DEL must be configured under either (1) ExecuteOnSuccessfulSend for PUT actions or (2) ExecuteOnSuccessfulCopy for LCOPY actions.
- If an action contains both PUT (or PUT+GET) and LCOPY commands, whichever type is found first in the action drives its scheduling. Even though this is allowed, it is highly recommended that autosend actions contain only *one* autosend-type command (for example, PUT/LCOPY -DEL). This ensures all autosends process only stable files. Furthermore, if multiple scheduler threads are in use, separating autosend commands should increase the throughput of the scheduler loop.
- When autosend is activated, files are checked for stability before they are sent or copied. This is an important feature to prevent to an unstable or incomplete file from being sent or copied. For this reason, all PUT and LCOPY commands should use autosend.

CHECK command rules

Note: The CHECK command is available only in the Cleo Harmony and Cleo VLTrader applications.

The following rules apply to actions containing CHECK commands scheduled by polling for files.

- The CHECK command must have a CHECK -FIL or CHECK -DIR command in the action.
- The CHECK command must specify an Age value of >*nn*[D|H|M|S] (where *nn* is a value of 0-99).
- The CHECK command may not specify the **Count** parameter. Therefore, by default, the count will be only one (1).
- If a file is reported on a particular CHECK run, and it is not subsequently handled (for example, moved somewhere else or processed in some way), it will be reported again on future executions of the command. For this reason, it is recommended that the **Execute On Check Conditions Met** property is specified, and that it contains the proper system commands needed to clean up the file.
- For details of the CHECK command, see CHECK command on page 943.
- The frequency of autochecks is based on the setting of the **Age** parameter and the age of the files found. It is easiest to understand this by example:

  Example 1 -- *Age* is >1D

  Given the command CHECK -FIL * Age=>1D

and given the initial files and their ages:

- `File1 (0.9D)`
- `File2 (0.9D)`
- `File3 (0.7D)`
- `File4 (0.7D)`

Since no files are currently older than one day, the first check would be run in 0.1 days, when `File1` and `File2` become one day old. After that, the next check is run 0.2 days later, when `File3` and `File4` become one day old. After that, if there are no additional files present, the next check will be run one day later (based on the `1D` value set for the *Age*).

Note:

When the first check is run, `File1` and `File2` are reported. Their file paths are available to any *%file%* macro present within the **Execute On Check Conditions Met** property. When the command is run again, if the same files are present, they are counted and reported again. Therefore, if you do not want to be notified multiple times regarding the same file, it is imperative that the files are dealt with (that is, removed) in the **Execute On Check Conditions Met** command.

Example 2 -- *Age* is `>0D`

Given the command: `CHECK -FIL * Age=>0D`

and given the initial files and their ages:

- `File1 (0.9D)`
- `File2 (0.9D)`
- `File3 (0.7D)`
- `File4 (0.7D)`

Since there are four files with an age greater than zero days (that is, they simply exist), the initial check reports all files. After that, subsequent checks will take place at a frequency determined by the **Autosend Check Every** property.

Note: The option to **only run Action if files are found to send or check** is not available for JavaScript actions.

Scheduling actions to run based on events

You can configure your system to run actions based on a *trigger* created when certain events occur. When the trigger is created, the action runs immediately. Note that, by default, actions configured to be triggered for an FTP server (under a Users host or a Local FTP Users host) are not triggered immediately. They are triggered when the connected FTP client issues another command or the session is closed. See *Trigger At Upload Completion* in Local FTP users mailbox advanced properties on page 818.

Triggers are generated when:

- a new file arrives in a folder
- a new file fails to arrive in a folder
- a user session ends successfully
- a user session fails to end.

Important: Only actions that are *in scope* of the triggering event are actually run. The trigger event's scope is limited to actions whose host is in the same host folder as the trigger's mailbox or in a parent host folder of the trigger's mailbox.

When you schedule an action to be run based on a trigger, the **Scheduler** window displays the triggering event in the **Scheduled** column. If there are multiple events, they are displayed in the **Scheduled** column as a comma-separated list.

1. In the **Scheduling** dialog box, select **Run this action automatically** check box and then select **when ANY of the following events occur**.
2. Select the events you want to trigger actions. Choose from the following:

   New file arrives

   Runs the action when a new file arrives in the folder. You can choose successful or failed file transfers or both to trigger the action.

   This event type is valid only for FTP and SFTP uploads, AS2 and HSP receives, and `LCOPY` commands.

   For a Commands action scheduled for `new file arrives`, the Commands action will be run only if at least one of the sources of the `PUT` or `LCOPY` commands in the action match the path of the new file. And then at runtime, all of the sources of the `PUT`, `LCOPY`, `LDELETE`, and `LREPLACE` commands that match the new file's path are modified to explicitly point to the new file.

   Note: If there are additional commands with wildcards that do not match the triggered file(s), those commands will pick up any files matching that wildcard, which may include non-triggered files. Therefore, it is not recommended to have additional commands with wildcards that would not match the triggered files.

   User session ends

   Runs the action when an FTP or SFTP user session ends. Choose successful or failed session end or both to be the trigger event.

   Note: This option is available only for **JavaScript** actions.

   Note: For both `new file arrives` and `user session ends` triggers, the trigger object is accessible in the JavaScript action via `ISessionScript.getTrigger()`. The user session end trigger includes all the relevant `new file arrives` triggers that occurred during the session.
3. Click **OK**.

   When the trigger event occurs, the action runs.

Scheduling actions - Web UI

In the web UI, you can schedule actions to run based on a time and date or based on an event.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

You use the Scheduler to run actions automatically at specific times, when files are present, or when certain events occur.

1. In the web UI, click **Scheduler**.

   Each action, host action, and standalone action in the active tree pane is listed in the schedule table.
2. Select the action you want to schedule. You can right-click the action row and select **Schedule**, double-click the action row, or single-click the action row and click the clock icon.

   Alternatively, you can right-click the action in the **Active** tab of the tree pane.

   The **Schedule Action** dialog box appears.
3. In the **Schedule Action** dialog box, the following top-level scheduling actions are available:

- **by Polling**: checks your folder for files continuously. See Scheduling actions to run automatically by polling for files on page 613.
- **by Date/Time**: applies date- and time-based scheduling for your action. See Scheduling actions to run at specific dates and times on page 612.
- **by Events**: runs the action when the selected event occurs. See Scheduling actions to run based on events on page 615. **Cleo Harmony and Cleo VLTrader applications only.**

4. When you finish specifying values for scheduling parameters above, click **Schedule**.

   The **Schedule Action** dialog box is dismissed and the new schedule information is displayed on the **Scheduler** page.

Note: You can modify an existing schedule by simply changing, adding, or removing the scheduling parameters for a selected action. To remove an action from the schedule, select **Unschedule** in the **Schedule Action** dialog box.

By default, the schedule will automatically start when the application is started. You can, however, override this behavior by turning off **Run Scheduler Automatically at Startup**. See Other system options on page 729.

For the Cleo LexiCom application, the schedule will only run one action at a time. If more than one action is scheduled for the same time, the actions are run sequentially. If a scheduled action is still running when another action's scheduled time arrives, the action is not started until the running action ends.

For the Cleo Harmony and Cleo VLTrader applications, you control concurrently running scheduled actions using the property **Allow Scheduled Actions to Run Concurrently**. See Other system options on page 729.

Scheduling actions to run automatically by polling for files

You can configure your system to poll folders for files and then run actions automatically when files are present.

Note: This option is available only for **Commands** actions.

1. In the **Scheduling** dialog box, select the **Run this action automatically** check box, and then select **by polling for files**.
2. If you want to poll for files continuously, click **OK**.

   If you want to specify how often to poll for files, click **Edit**. The **Schedule for** dialog box appears. See Scheduling actions to run at specific dates and times on page 612 for more information.

   If you do not explicitly specify how often to poll for files, default polling period values are used.
3. Click **OK**.

Requirements when polling for files

When you set up an action to run by **polling for files**, the action will *potentially* be run according to the period you've configured. However, it will only *actually* run if one of these conditions are true:

- A `PUT`, `PUT+GET`, or `LCOPY` command within the action has a file to send or copy.
- The `CHECK` command is present in the action and specific conditions for that command are met.

Note that if an action contains both `PUT/LCOPY` and `CHECK` commands, it is the first command encountered that determines whether autosend properties (for `PUT` and `LCOPY`) or autocheck properties (for `CHECK`) are used. Since this could make it difficult to determine the actual schedule, actions designated for autocheck should contain only the `CHECK` command.

The frequency at which the scheduler checks to see if there are files to send or copy is controlled by the **Autosend Check Every** property. This indicates that even schedules set up for continuous polling are not actually continuous. Rather, their minimum frequency of polling is determined by **Autosend Check Every**.

PUT, PUT+GET, and LCOPY command rules

The following rules apply to actions containing PUT, PUT+GET, or LCOPY commands scheduled by polling for files.

- For an action to be scheduled this way, at least one of its PUT, PUT+GET, or LCOPY commands must use the delete after transfer (-DEL) option. For an action to be scheduled this way, at least one of its PUT, PUT+GET, or LCOPY commands must use the delete after transfer (-DEL) option, or LCOPY -DEL must be configured under either (1) ExecuteOnSuccessfulSend for PUT actions or (2) ExecuteOnSuccessfulCopy for LCOPY actions.
- If an action contains both PUT (or PUT+GET) and LCOPY commands, whichever type is found first in the action drives its scheduling. Even though this is allowed, it is highly recommended that autosend actions contain only *one* autosend-type command (for example, PUT/LCOPY -DEL). This ensures all autosends process only stable files. Furthermore, if multiple scheduler threads are in use, separating autosend commands should increase the throughput of the scheduler loop.
- When autosend is activated, files are checked for stability before they are sent or copied. This is an important feature to prevent to an unstable or incomplete file from being sent or copied. For this reason, all PUT and LCOPY commands should use autosend.

CHECK command rules

Note: The CHECK command is available only in the Cleo Harmony and Cleo VLTrader applications.

The following rules apply to actions containing CHECK commands scheduled by polling for files.

- The CHECK command must have a CHECK -FIL or CHECK -DIR command in the action.
- The CHECK command must specify an Age value of >*nn*[D|H|M|S] (where *nn* is a value of 0-99).
- The CHECK command may not specify the **Count** parameter. Therefore, by default, the count will be only one (1).
- If a file is reported on a particular CHECK run, and it is not subsequently handled (for example, moved somewhere else or processed in some way), it will be reported again on future executions of the command. For this reason, it is recommended that the **Execute On Check Conditions Met** property is specified, and that it contains the proper system commands needed to clean up the file.
- For details of the CHECK command, see CHECK command on page 943.
- The frequency of autochecks is based on the setting of the **Age** parameter and the age of the files found. It is easiest to understand this by example:

  Example 1 -- *Age* is >1D

  Given the command CHECK -FIL * Age=>1D

  and given the initial files and their ages:

  - File1 (0.9D)
  - File2 (0.9D)
  - File3 (0.7D)
  - File4 (0.7D)

  Since no files are currently older than one day, the first check would be run in 0.1 days, when File1 and File2 become one day old. After that, the next check is run 0.2 days later, when File3 and File4 become one day old. After that, if there are no additional files present, the next check will be run one day later (based on the 1D value set for the *Age*).

  Note:

  When the first check is run, File1 and File2 are reported. Their file paths are available to any *%file%* macro present within the **Execute On Check Conditions Met** property. When the command is run again, if the same files are present, they are counted and reported again. Therefore, if you do

not want to be notified multiple times regarding the same file, it is imperative that the files are dealt with (that is, removed) in the **Execute On Check Conditions Met** command.

Example 2 -- *Age* is >0D

Given the command: `CHECK -FIL * Age=>0D`

and given the initial files and their ages:

- `File1 (0.9D)`
- `File2 (0.9D)`
- `File3 (0.7D)`
- `File4 (0.7D)`

Since there are four files with an age greater than zero days (that is, they simply exist), the initial check reports all files. After that, subsequent checks will take place at a frequency determined by the **Autosend Check Every** property.

Note: The option to **only run Action if files are found to send or check** is not available for JavaScript actions.

Scheduling actions to run at specific dates and times

You can schedule actions to run automatically based on a weekly, monthly, or one-time period. For weekly and monthly scheduling, it is possible to set up multiple day and time ranges.

1. In the **Scheduling** dialog box, select **Run this action automatically**.
2. Select **at scheduled date(s) and time(s)**, and then click **Continue**.

   The **Schedule for** dialog box appears.
3. Specify a weekly, monthly, or one-time schedule. See Scheduling actions to run weekly on page 612, Scheduling actions to run monthly on page 613, and Scheduling actions to run one time on page 613 for more information.
4. After you specify a schedule, click **OK** on the **Schedule for** dialog box.

   The **Schedule for** dialog box is dismissed and the **Scheduling** dialog box appears.
5. Click **OK** on the **Scheduling** dialog box.

   Your action is scheduled and the schedule is reflected in the table of actions on the **Scheduler** page.

Scheduling actions to run weekly

You can schedule actions to run automatically on a weekly schedule. You can set up multiple day and time ranges.

1. In the **Schedule for** dialog box, select the **Weekly** radio button.
2. Select a time zone.

   The times you select for this schedule are relative to this time zone. The time zone you select is displayed in the **Scheduler** dialog box in the **Scheduled** column.
3. **Optional**: Select **Every Other Week** to run the action on alternating weeks. The action runs only on the selected days during those weeks.
4. Select one or more days of the week within the **Day(s) of Week** section.
5. Specify one or more start times (24-hour clock). A start time of `00:00` indicates 12:00 midnight; a start time of `17:00` indicates 5:00 PM.
6. **Optional**: For each start time, specify a recurrence. A recurrence can be scheduled either continuously, by selecting the **Recurring continuously** check box, or at an interval, by selecting the **Recurring every** check box

and specifying the interval in hours, minutes, and seconds. Finally, choose when the recurrence should stop by selecting a time from the **Until** menu. An end time of `24:00` indicates the end of the day.

7. If a different time schedule is required on different days (for example, weekdays and weekends), click **New Day(s)** and repeat the steps above.

   When you configure multiple days, you can scroll through them using the arrow buttons in the upper left of the dialog box.

   You can click **Remove Day(s)** to delete the schedule for the days currently displayed.

8. Click **OK**.

   Your new schedule is saved and the schedule table is displayed, including your new schedule information.

Scheduling actions to run monthly

You can schedule actions to run automatically on a monthly schedule. You can set up multiple day and time ranges.

1. In the **Scheduling** dialog box, select the **Monthly** radio button.
2. Select a time zone.

   The time zone you select is displayed in the **Scheduler** dialog box in the **Scheduled** column.

3. Select one or more months and then one or more days of the month within the **Day(s) of Month** section.
4. Specify one or more start times (24-hour clock). A start time of `00:00` indicates 12:00 midnight; a start time of `17:00` indicates 5:00 PM.
5. **Optional**: For each start time, specify a recurrence. A recurrence can be scheduled either continuously, by selecting **Recurring continuously**, or at an interval, by selecting **Recurring every** and specifying the interval in hours, minutes, and seconds. Finally, choose when the recurrence should stop by selecting a time from the **Until** dropdown menu. An end time of 24:00 indicates the end of the day.
6. If a different time schedule is required on different months (for example, even months versus odd months), click **New Month(s)** and repeat the steps to specify days and times.

   When you configure multiple months, you can scroll through them using the arrow buttons in the upper left part of the dialog box.

   You can click **Remove Month(s)** to delete the schedule for the months currently displayed.

7. Click **OK**.

   Your new schedule is saved and the schedule table is displayed, including your new schedule information.

Scheduling actions to run one time

You can schedule actions to run automatically one time at a specific date and time.

1. In the **Scheduling** dialog box, select **One Time**.
2. Select a time zone.

   The time zone you select is displayed in the **Scheduler** dialog box in the **Scheduled** column.

3. Select a single year, month, day, and time.
4. Click **OK**.

   Your new schedule is saved and the schedule table is displayed, including your new schedule information.

Scheduling actions to run based on events

You can configure your system to run actions based on a *trigger* created when certain events occur. When the trigger is created, the action runs immediately. Note that, by default, actions configured to be triggered for an FTP server (under a Users host or a Local FTP Users host) are not triggered immediately. They are triggered when the connected

FTP client issues another command or the session is closed. See *Trigger At Upload Completion* in Local FTP users mailbox advanced properties on page 818.

Triggers are generated when:

- a new file arrives in a folder
- a new file fails to arrive in a folder
- a user session ends successfully
- a user session fails to end.

Important: Only actions that are *in scope* of the triggering event are actually run. The trigger event's scope is limited to actions whose host is in the same host folder as the trigger's mailbox or in a parent host folder of the trigger's mailbox.

When you schedule an action to be run based on a trigger, the **Scheduler** window displays the triggering event in the **Scheduled** column. If there are multiple events, they are displayed in the **Scheduled** column as a comma-separated list.

1. In the **Scheduling** dialog box, select **Run this action automatically** check box and then select **when ANY of the following events occur**.
2. Select the events you want to trigger actions. Choose from the following:

   New file arrives

   Runs the action when a new file arrives in the folder. You can choose successful or failed file transfers or both to trigger the action.

   This event type is valid only for FTP and SFTP uploads, AS2 and HSP receives, and `LCOPY` commands.

   For a Commands action scheduled for `new file arrives`, the Commands action will be run only if at least one of the sources of the `PUT` or `LCOPY` commands in the action match the path of the new file. And then at runtime, all of the sources of the `PUT`, `LCOPY`, `LDELETE`, and `LREPLACE` commands that match the new file's path are modified to explicitly point to the new file.

   Note: If there are additional commands with wildcards that do not match the triggered file(s), those commands will pick up any files matching that wildcard, which may include non-triggered files. Therefore, it is not recommended to have additional commands with wildcards that would not match the triggered files.

   User session ends

   Runs the action when an FTP or SFTP user session ends. Choose successful or failed session end or both to be the trigger event.

   Note: This option is available only for **JavaScript** actions.

   Note: For both `new file arrives` and `user session ends` triggers, the trigger object is accessible in the JavaScript action via `ISessionScript.getTrigger()`. The user session end trigger includes all the relevant `new file arrives` triggers that occurred during the session.
3. Click **OK**.

   When the trigger event occurs, the action runs.

Schedule formats

VersaLex displays scheduling information in a proprietary format. The REST API uses the same format for the `schedule` attribute. This section is intended to help you understand what is displayed in the Scheduler UI and to help you use schedule data in an API.

Schedules and their formats are based on either date and time or the occurrence or an event.

Note: Schedule formats are case insensitive, except for *timezone*.

Date/time-based schedule format

Data for date/time-based schedules use a single general format with variations for one-time, weekly, and monthly schedules.

```
[on file polling][for timezone] schedule
```

on file polling

Runs schedule when there are files available to send or check.

This parameter is not valid if the action type being scheduled is JavaScript.

for *timezone*

Indicates the timezone to be considered when the schedule is evaluated for execution by the server.

timezone is expressed in the format used in the tz database, `Area/Location`. For example: `America/Chicago` or `Asia/Tokyo`. If no timezone is specified as part of a schedule string, this value defaults to the timezone in which the server is located.

schedule

A schedule consists of series of parameters (described below) that indicate when an action should be executed.

You can create the following types of schedules:

- One-time: see One-time schedule on page 622.
- Weekly: see Weekly schedule on page 623.
- Monthly: see Monthly schedule on page 624.

One-time schedule

```
on date @time
```

Parameters

date

Expressed in `yyyy/mm/dd` format and must be in the future. A date specified is affected by the timezone in question.

time

Expressed using a 24-hour clock format, `HH:mm[:ss]` (where seconds are optional) and must be in the future. The time you specify is affected by the timezone in question. For example, a user is in Chicago (CST) at 10:00 on 12/18/2020 and tries to make a schedule `for America/New_York on 12/18/2020 @10:30`. This will not work because the time specifed is already in the past.

Examples

for America/Chicago on 2018/08/01 @08:00

Schedule set to run on August 1, 2018 in the America/Chicago timezone at 0800 hours.

on 2018/09/10 @14:30:30

Schedule set to run September 10, 2018 in the timezone in which the server is located at 1430 hours and 30 seconds.

Weekly schedule

This is the format the product uses to display weekly schedule information. You can also use this format to programmatically schedule actions continuously.

```
on day1[day2][day3-day4] @start-time[[/interval]-stop-time]
[,start-time[[/interval]-stop-time]] [+on day5[day6-day7] @start-
time[[/interval]-stop-time]][,start-time[[/interval]-stop-time]]
```

Alternatively, you can use the following syntax to schedule actions to run continuously:

```
continuously
```

Parameters

day

Specifies a day or days of the week on which you want the action to be executed.

When specifying a weekly schedule, days are expressed as two-letter abbreviations that represent the day of the week. For example, `Su` for Sunday, `Mo` for Monday, `Tu` for Tuesday, and so on. You can specify a range of days of the week by delimiting the start and end days in the range using a hyphen (`-`).

Day ranges must be distinct and cannot overlap.

start-time

interval

stop-time

Indicates the time (or time range) of day an action should be executed.

`start-time` is the beginning of the range.

`interval` is how often the action is executed.

`stop-time` is the end of the range.

All three are expressed in `HH:mm[:ss]` format, where seconds are optional.

You cannot specify duplicate or overlapping times. For example, `on We @00:00-01:00,00:30` is not allowed.

continuously

Runs the action continuously. This is a shortcut for and equivalent to specifying `Su-Sa @00:00-24:00`.

Note: Continuous scheduling is actually semi-continuous. The minimum period of processing continuous operations is governed by the **Options** > **Other** > **Autosend Check Every** setting. The default value is 5 seconds. See Other system options on page 729.

Note: Scheduling an action to run continuously could impact your system performance. It is recommended that you schedule actions to run at a longer frequency than the default, for example, 30 seconds.

on file polling continuously

Run the action only when there are files available to send or check. This is a shortcut for and equivalent to specifying `on file polling Su-Sa @00:00-24:00`.

Note: Continuous scheduling is actually semi-continuous. The minimum period of processing continuous operations is governed by the **Options** > **Other** > **Autosend Check Every** setting. The default value is 5 seconds.

Examples of weekly schedules

on file polling for Asia/Tokyo Mo @17:00

Sets the schedule to run on Mondays at 1700 hrs in the timezone for Tokyo, only when files are available to send/check.

on file polling Mo-Fr @17:00

Sets the schedule to run on Monday through Friday at 1700 hrs in the timezone in which the server resides, only when files are available to send/check.

on MoWe-Fr @17:00

Sets the schedule to run on Monday and Wednesday through Friday at 1700 hrs.

on Mo-Fr @00:00-24:00

Sets the schedule to run on Monday through Friday, running continuously.

on Su-Sa @09:00/00:02:30-17:00

Sets the schedule to run on Sunday through Saturday from 0900 to 1700 hrs, running every 2 minutes and 30 seconds.

on Su-Sa @09:00/00:02:30-17:00,18:00/00:00:30-22:00

Sets the schedule to run on Sunday through Saturday from 0900 to 1700 hrs, running every 2 minutes and 30 seconds, and from 1800 to 2200, running every 30 seconds.

on Mo-We @09:00/01:00-12:00+on Th-Sa @13:00/01:00-17:00

Sets the schedule to run on Monday through Wednesday between 0900 hrs and 1200 hrs with a recurrence interval of 1 hr and Thursday through Saturday between 1300 hrs and 1700 hrs with a recurrence interval of 1 hr.

continuously

Sets the schedule to run on Sunday through Saturday, running continuously.

on file polling continuously

Sets the schedule to run on Sunday through Saturday, running continuously, only when files are available to send/check.

Monthly schedule

This is the format the product uses to display monthly schedule information.

```
in m1[m2][m3-m4] on day d1[,d2][,d3-d4] @start-time[[/interval]-stop-
time][,start-time[[/interval]-stop-time]][+in m5[m6][m7-m8] on day d6[,d7]
[,d8-d9] @start-time[[/interval]-stop-time][,start-time[[/interval]-stop-
time]]
```

Parameters

m

A month in which the action should be executed.

You can specify any number on months individually or you can specify a range of months.

d

Specifies a day of the month on which you want the action to be executed.

When specifying a monthly schedule, days are expressed as numerical values that represent the day of the month. You can specify a range of days of the month by delimiting the start and end days in the range using a hyphen (-).

Day ranges must be distinct and cannot overlap.

Note: You can also specify days as `first Monday`, `second Tuesday`, `every Thursday`, and so on, rather a specific day of the month. See Examples of monthly schedules on page 625 for more information.

`start-time`

`interval`

`stop-time`

Indicates the time (or time range) of day an action should be executed.

`start-time` is the beginning range.

`interval` is how often the action is executed.

`stop-time` is the end of the range.

All three are expressed in `HH:mm[:ss]` format, where seconds are optional.

You cannot specify duplicate or overlapping times. For example, `on We @00:00-01:00,00:30` is not allowed.

Examples of monthly schedules

`in JanFebJul-Sep on day 1,8-15 @08:00`

Sets the schedule to run in Jan, Feb, and Jul through Sep on 1st and 8th through 15th days at 0800 hrs.

`on file polling in JanFebJul-Sep on day 1,8-15 @08:00+in Oct-Dec on day 1,8-15 @08:00`

Sets the schedule to run only when files are available in Jan, Feb, and from Jul through Sep on the1st, the 8th through 15th days at 0800 hrs and from Oct through Dec on the 1st and the 8th through 15th at 0800 hrs.

`in JanFebJul-Sep on day 1,8-15 @09:00/01:00-17:00`

Sets the schedule to run in Jan, Feb, and Jul through Sep on 1st and 8th through 15th days between 0900 hrs and 1700 hrs recurring every hour.

`in JanFebJul-Sep every day @08:00`

Sets the schedule to run in Jan, Feb, and Jul through Sep every day at 0800 hrs.

`in JanFebJul-Sep every monday @08:00`

Sets the schedule to run in Jan, Feb, and Jul through Sep every Monday at 0800 hrs.

`in JanFebJul-Sep on the first day @08:00`

Sets the schedule to run in Jan, Feb, and Jul through Sep on the 1st day at 0800 hrs.

`in JanFebJul-Sep on the last friday @08:00`

Sets the schedule to run in Jan, Feb, and Jul through Sep on the last Friday at 0800 hrs.

Continuous schedule

You can set a schedule to run continuously by specifying that it should run Sunday through Saturday without specifying an interval.

This schedules the action to run as often as is allowed by the **Autosend Check Every** setting, whose default value is 5 seconds. See Other system options on page 729.

Note: Scheduling an action to run continuously could impact your system performance. It is recommended to schedule actions to run at a longer frequency than the default, for example, 30 seconds.

Event-based schedule format

Event-based schedules use a single format.

```
[on new file arrives [success|failure]] [,on user session ends [success|
failure]]
```

Parameters

`new file arrives [success | failure]`

Runs schedule when a new file arrives.

Specify `success` or `failure` to add a dependency on whether the file arrives successfully or unsuccessfully, respectively.

If you do not specify `success` or `failure`, the schedule runs whether the file arrives successfully or not.

You can combine this parameter with the `user session ends` parameter in any order.

`user session ends [success | failure]`

Runs schedule when the user's session ends.

Specify `success` or `failure` to add a dependency on whether the session ends successfully or unsuccessfully, respectively.

If you do not specify `success` or `failure`, the schedule runs whether the session ends successfully or not.

You can combine this parameter with the `new file arrives` parameter in any order.

Valid only for JavaScript actions.

Examples

`on new file arrives success`

Runs the action when a new file arrives successfully.

`on user session ends failure`

Runs the action when the user session ends unsuccessfully.

`on user session ends failure,on new file arrives`

Runs the schedule when the user session ends unsuccessfully or when a new file arrives (whether successfully or not).

Chapter

7

Router

Setting up automated outgoing routes

Note: This feature is being deprecated. For similar functionality, use a Router host, which is a type of Connector host. See Connector Host on page 534 for more information.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

1. In the web UI, click **Router**. In the native UI, select **Tools** > **Router** in the menu bar.
2. By default, the router does not automatically start when the Cleo Harmony or Cleo VLTrader application is started. Either manually start the router by clicking or select Automatically run at startup.
3. The automated routing directory defaults to `autoroute\` in the Cleo Harmony or Cleo VLTrader home directory. The defined set of routing rules are automatically applied to files or subdirectories placed in this directory. Click **...** to select a different autoroute directory.
4. Click **Find Route** to find an existing route by filename or EDI parameters.
5. Click **New Route** to define a new routing rule.

   At least one routing criterion is required - either a filename or EDI header map. The filename can be wild carded (for example, `*.dcx`) and applies to files and subdirectories alike. If the mailbox protocol supports it, subdirectories can be used to send multipart payload messages. More than one filename can be listed separated by either a comma (,) or a semicolon (;). EDI routes only apply to single file routes and not subdirectory routes.
6. Click **New** to define a new EDI criterion.

   The **Note** field is used to capture trading partner or other relevant information – it is not an EDI criteria for routing. When searching for a route (Step 4 above), wildcard characters (* and ?) can be used in the **Note** field.

   The **…** buttons are present when Trading Partners are available for selection. See Managing Trading Partners on page 631. These buttons allow the user to display the Trading Partners and configured Interchange Identifiers/Qualifiers.

   If a Trading Partner Alias is selected along with **Use All Interchange Identifiers/Qualifiers**, then a trading partner alias variable will be used. This will match any of the Interchange Identifiers/Qualifiers configured for the Trading Partner. If **Use All Interchange Identifiers/Qualifiers** is not selected, then the user can select a specific Interchange Identifier/Qualifier pair to be used. Once the selections have been made and the **OK** button is selected, then the selection will be placed in the appropriate fields depending on which **…** button was selected.

   EDI-X12, UN/EDIFACT, and TRADACOMS file formats are recognized when routing by interchange sender and/or receiver, functional group application sender and/or receiver, and/or transaction type:

Criteria		**Corresponding EDI elements**		
		EDI-X12	**UN/EDIFACT**	**TRADACOMS**
Interchange	Sender	ISA06	UNB02:1	STX02:1
	Receiver	ISA08	UNB03:1	STX03:1
Functional Group	App Sender	GS02	UNG06:1	
	App Receiver	GS03	UNG07:1	
Transaction	Type(s)	ST01	UNH09:1	MHD02

An EDI file can potentially be split across multiple routes as long as each segment of the file has one and only one route defined. If there are undefined or doubly-defined segments in a file being routed, those segments will be rejected and filtered into the system reject box (see Specifying default host directories on page 700). More than one transaction type can be listed separated by either a comma (,) or a semicolon (;).

7. A **To** mailbox must be selected and one or more Cc mailboxes can also be selected. Click in the cell and a pull-down list can be used to select the appropriate host\mailbox. When routing, a file is sent to each mailbox selected concurrently.

   You can specify sending parameters that override the default parameters in the mailbox's default `<send>` action (for example, `[Content-Type]=Binary or ReceiverId=CHASE`).

8. When a route first initiates, the file/subdirectory being routed is marked as read-only so that no further updates can be made to the file(s). Temporary send actions (named `<send%########## >`) are created and used during the routing process. While a route is active, the status of the route can be displayed. Right-click a routing rule and select **Status** or double-click the routing rule.

9. If the route attempt should fail, the status will reflect the result. Retries are automatically scheduled based on "Autosend Retry Attempts" and "Autosend Restart" (see Other system options on page 729). To force an immediate retry, right-click a file and select **Retry Now**. To cancel a routing, right-click a file and select **Cancel** or double-click the file.

   If the route file is being split across multiple routes, only the segments being routed to this mailbox based on this routing rule are canceled.

10. Once all the routes for a file/subdirectory are complete, the file/subdirectory is automatically deleted.

Chapter

8

Partners

Managing Trading Partners

Trading Partner Management is a privileged operation enabled within the Cleo VLNavigator software, providing a place within the product to store information about trading partners and a way to know which host-mailboxes combinations (also called *connections*) are associated with a particular trading partner.

Primary functions include:

- Storing and retrieving information about a trading partner such as:
  - Contact information for multiple people, including the type of contact
  - Interchange Identifier(s) and qualifier(s)
  - Macro Identifier (Used at mailbox/command level substituted for `%tp`)
  - Folders, hosts, and mailboxes that are associated with the trading partner
- Viewing transfer reports sorted by Trading Partner
- When viewing transfers through VLPortal, viewing transfers for all mailboxes associated with the trading partner
- Using the Trading Partner Interchange Identifiers selectively or collectively (through the Trading Partner alias) in the routing table and the `CHECK` command

About the Trading Partners table

The Trading Partners table displays aliases, contacts, and connections for each trading partner configured. Each row in the table contains information about a single trading partner.

To access the Trading Partners Table, do one of the following:

- In the web UI, click **Partners**.
- In the native UI, select **Tools** > **Trading Partners** in the menu bar.

You can sort the table by any of the columns. By default, the table is sorted by the **Trader Partner Alias** column. When you sort by **Contacts**, rows are sorted by the first e-mail address in the cell for each row. When you sort by **Connections**, rows are sorted based on first item in the connections list.

Within each **Contacts** cell, items are sorted by e-mail address. Within each **Connections** cell, the items are also sorted alphabetically. The **Trading Partner Type** column is only displayed if Trading Partner Types exist for you trading partners.

The table will only display information about the Trading Partners and connections for which the current user has viewing privileges. This is based on the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom folders to which the current user has privileges to see. If the Trading Partner has associated folders, hosts, and mailboxes but the current user does not have privileges to see them, the user will not see the trading partner information in the table. If there are

no connections associated with a trading partner, all users will be able to see that trading partner and the associated contacts.

If the host/mailbox is not associated with a Trading Partner and is not a Cleo test host or the Local Listener, it is shown in the table at the bottom of the list with one row per host/mailbox, and the Trading Partner alias, Trading Partner Type, and Contacts cells are empty. These items are shown with a darker background color to indicate which host/mailbox combinations are not associated with any trading partner.

Right-click a trading partner row to display a menu from which you can choose from the following operations:

- **Edit Trading Partner…** displays the **Edit Trading Partner** dialog box. Alternatively, you can also double-click a row to display the edit dialog box. See Adding or editing a Trading Partner on page 633.
- **Remove Trading Partner** deletes the selected Trading Partner(s).
- **Transfer Report…** displays the Transfer Report Filter dialog box for the selected Trading Partner(s). See Transfers on page 895.
- **Find** and **Find Next** allow the user to search the table for specific entries. See Searching the Trading Partner Table on page 632.

Right-click a non-trading partner row to display a menu from which you can choose from the following operations:

- **Transfer Report…** displays the **Transfer Report Filter** dialog box for the selected host/mailbox. See Transfers on page 895.
- **Associate to Trading Partner** displays the **Trading Partner Selection** dialog box, where you can create a new partner or select an existing one.

In addition, you can use the row of buttons at the bottom of the page.

- **Filter** - See Filtering the Trading Partner Table on page 632.
- **Find** - See Searching the Trading Partner Table on page 632.
- **Add Trading Partner** - See Adding or editing a Trading Partner on page 633.
- **Export** - See Exporting Contacts on page 635.
- **Import** - See Importing Contacts and EDI Parameters on page 635.

Filtering the Trading Partner Table

Click **Filter** on the Trading Partner Management table to display the **Trading Partners Filter** dialog box.

The **Trading Partners Filter** dialog box contains a list of trading partners and a list of connections. Each item has a check box you use to select one or more of each to reduce the number of items displayed. Choosing items from the trading partners list updates the items displayed in the table. There are also **Business Contact** and **Technical Contact** check boxes. At least one of these must be selected.

Searching the Trading Partner Table

Click **Find** on the Trading Partner Management table to display Find Trading Partner dialog box, where you can specify a search for a specific trading partner alias, email address, name, or connection.

Select a specific radio button to choose the criterion you want to search on. Then enter a string into the enabled field(s). The search is case insensitive. It will stop when the string entered matches any part of the selected field(s). The search starts on the selected row. If no rows are selected, then the search starts at the top of the list. `F3` will perform a `Find Next`. If no matches are found from the starting point to the end of the list, the user will be asked if they want to continue searching from the top. The labels for the three Custom Fields at the bottom will be displayed using the user customizable labels configured in the **Trading Partner General** tab. See Trading Partner: General Tab on page 633.

Adding or editing a Trading Partner

1. Click **Add Trading Partner** on the Trading Partner Management table page to configure a new trading partner.
   The Trading Partner Alias input dialog box appears.
2. Enter trading partner alias and click **OK**.
   The Add Trading Partner dialog box appears.
3. Enter information on each of the following tabs as required.
   - General tab - see Trading Partner: General Tab on page 633.
   - Contacts tab - see Trading Partner: Contacts Tab on page 633.
   - Identifiers tab - see Trading Partner: Identifiers Tab on page 634.
   - Connections - see Trading Partner: Connections Tab on page 634.
   - Notes - see Trading Partner: Notes Tab on page 635.
4. Click **OK** when you are finished entering information about your trading partner.
   Your trading partner information is saved.

Trading Partner: General Tab

The **General** tab contains the Trading Partner address type and address as well as other general information including the Partner Type, Macro Value, and three custom fields. All fields are optional. The Macro Value is used with the `%tp` keyword referenced in HTTP hosts. The **Change…** button allows the user to change the alias of the Trading Partner to another non-existent alias. The **Edit Types…** button after the **Address Type** field allows the user to configure user-defined address types (see Edit Address Types on page 633). The **Edit Types…** button after the **Partner Type** field allows the user to configure user-defined partner types (see Edit Partner Types on page 633).

The **Edit Label…** buttons allow the user to label the three custom data fields. These three fields can be used to store information such as a division name or the file transfer product being used by the trading partner.

Edit Partner Types

The **Edit Partner Types** dialog box allows you to add new partner types and edit existing ones.

Click **New…** to create a new partner type.

Double-click a row to edit the partner type. When you modify a partner type, the modification is propagated to all Trading Partners of this type.

Right-click a row to display a menu from which you can edit the partner type or remove it.

Edit Address Types

The **Edit Address Types** dialog box allows you to add new address types and edit existing ones.

Click **New…** to create a new address type.

Double-click a row to edit the address type. When you modify an address type, the modification is propagated to all Trading Partners that have this address type.

Right-click a row to display a menu from which you can edit the address type or remove it.

Trading Partner: Contacts Tab

The **Contacts** tab displays the contacts associated with a trading partner.

The only required information for a contact is the email address and the contact type.

Click **Add Contact** to add a contact to the list of contacts for this trading partner. When adding a contact, you are prompted to provide an email address, which is checked to make sure it is valid. If not, you are prompted to provide

a valid email address. If the email address is already associated with a trading partner, you choose to use that contact information.

Double-click a row to edit the contact information.

Right-click a row to display a menu from which you can choose to edit the contact or remove it.

Note: Editing the contact information for an Email address associated with a Trading Partner modifies the data for this contact for all associated Trading Partners.

Contact: Contact Tab

The **Contact** tab for a contact contains information including contact name, title, phone numbers, and time zone, and whether the contact is a business contact, a technical contact or both. At least one of the contact types must be selected. Click **Change** to modify the contact's email address.

Contact: Address Tab

The **Address** tab for a contact contains the contact's address information. By default, the address is the same as the trading partner and the data entry fields are disabled. Select the **Different from General Address** check box to enable the data entry fields on the screen.

Contact: Trading Partners Tab

The **Trading Partners** tab for a contact contains a list of associated trading partners. This list is display only. The Trading Partner being edited is denoted by an asterisk (*) after the alias.

Contact: Notes Tab

The **Notes** tab for a contact contains any text you might want to save regarding this contact.

Trading Partner: Identifiers Tab

The **Identifiers** tab contains a list of interchange identifiers and qualifiers associated with a trading partner. These interchange identifiers/qualifiers can be used in the Routing and Transfer Reporting features.

Double-click on a row to display a dialog box where you can edit an existing interchange identifier/qualifier.

The user may also right-click and select **Edit Interchange Identifier…** to edit the row or **Remove Interchange Identifier…** to remove the row(s).

Trading Partner: Connections Tab

The **Connections** tab contains a list of connections (folders, hosts, mailboxes) associated with this Trading Partner.

The **Assigned Connections** list shows which connections are associated with this trading partner. If a folder is listed alone, then all folders, hosts, and mailboxes in that folder are considered as belonging to this trading partner. Likewise, if a host is listed alone, then all mailboxes of that host are considered as belonging to this trading partner. To remove items from this list, select one or more items from the list and click the **Remove Connection(s)** button.

The **Available Connections** list shows all folders, hosts, and mailboxes not associated with this trading partner even though they may be associated with another trading partner. This is because connections can belong to more than one trading partner. Select items from the **Available Connections** list and click the **Add Connections** button to associate the connection(s) to the trading partner. The connections will be added to the **Assigned Connections** with **Production** set to `False`.

Selecting one or more mailbox items from the Assigned Connections and right-clicking gives a menu with two choices:

- `Set Production to True`
- `Set Production to False`

These set the Production flag to `True` or `False` for the selected mailbox(es).

Trading Partner: Notes Tab

The **Notes** tab contains any user-entered notes for a Trading Partner.

Exporting Contacts

Click **Export** on the Trading Partner Management table to display the **Trading Partner Contact Export** dialog box, where you can export the currently displayed contacts and their EDI parameters to a comma-separated values (.csv) file. The data exported depends on the current filter.

Specify whether or not a header row should be output using the **Output header row** switch. You can also select the character used as the value separator. You can select comma, semicolon, or tab, or another character you specify. When you click **Export**, you are prompted for a file name and location.

The following columns are output in the following order:

- Trading Partner Alias
- First Name
- Last Name
- Email
- Title
- Department
- Work Phone
- Work Phone Extension
- Cell Phone
- Address 1
- Address 2
- City
- State/Province
- Zip
- Country
- Business (“True” or “False” specifying whether this is a Business contact)
- Technical (“True” or “False” specifying whether this is a Technical contact)
- Address Type
- Interchange Identifier
- Qualifier

Importing Contacts and EDI Parameters

Click **Import** on the Trading Partner Management table to display the **Trading Partner Contact Import** dialog box. Use this dialog box to import contacts from a comma-separated values (.csv) file into the Trading Partners table. The user is first prompted to select the CSV file to import. Once the file is selected, the Cleo Harmony application will attempt to automatically determine the Column Separator (if it is Comma, Semicolon, or Tab).

Specify whether the file contains a header row and select a column separator (if needed). When you click **Import**, the contacts and EDI parameters are imported. If a contact (Email address) already exists, the user will be prompted whether or not they want to overwrite the existing contact information. If an Interchange identifier already exists for that trading partner then it will be overridden.

If an invalid line is encountered, the import is aborted and all invalid lines are displayed in a dialog box.

The following columns in the following order are expected in the input file.

- Trading Partner Alias
- First Name
- Last Name
- Email
- Title
- Department
- Work Phone
- Work Phone Extension
- Cell Phone
- Address 1
- Address 2
- City
- State/Province
- Zip
- Country
- Business (“True” or “False” specifying whether this is a Business contact)
- Technical (“True” or “False” specifying whether this is a Technical contact)
- Address Type
- Interchange Identifier
- Qualifier

The required columns are the Trading Partner Alias and at least one of the following:

- An Interchange Identifier
- A Contact Email Address marked as a Business or Technical Contact

Chapter

9

Transfers

Viewing transfer status

Transfer logs contain information about the transfer of individual files; they are not action logs reporting the status of actions. When processing multiple files, each file transfer is logged individually when the actual file transfer begins. The log record is updated when the transfer is completed. If other action commands fail before the file transfer begins, the file transfer is not logged.

Use the **Transfer Report** to view the status of transfers that have already occurred.

1. To view the **Transfer Report**, do one of the following:
   a) In the web UI, click **Transfers**. In the native UI, select **Tools** > **Transfer Report** or click **Transfers** in the toolbar.

      Note: In the web UI, if you click the **Transfers** button, by default, the web UI displays the entire transfer report without displaying the filtering criteria dialog box. To display the filtering criteria in the web UI, click **Filter**.

   b) Right-click a folder, host, and mailbox and then select **Transfer Report** from the context menu. If you use this method, the folder, host or mailbox you right-click will be preseleted as part of your filtering criteria.

   The **Transfer Report Filter** dialog box is displayed.
2. Specify criteria for the transfers you want to display. See Transfer Status Filter on page 637.

   Alternatively, click **Open** to choose a previously saved filter criteria file to populate the fields in the dialog box.
3. Select a format for the report. Choose either **Table** or **Report**. If you choose **Report**, you can select **Include details** to populate the report with detailed information about the transfers.
4. Optionally, click **Save As** to save any filter criteria you specified to an XML file.

   You can use this XML file to later recall these settings using **Open…** or with the `VLStatc -f` command-line option to use the filter for reports generated to a file or to an email address.
5. Click **Continue** to display the report.

Note: In the web UI, if you click the **Transfers** button, by default, the web UI displays the entire transfer report without displaying the filtering criteria dialog box. To display the filtering criteria in the web UI, click **Filter**.

Transfer Status Filter

Use the **Transfer Status Filter** panel to select the items you want to view. By default, it displays the current day's transfers.

Specify values in the **From** and **To** fields to select the range of times. You can either use the menus, or manually enter dates (`YYYY/MM/DD`) and times (`HH:MM`) into the fields. There are four possible tabs that can be present on this panel: **General**, **Tracking**, **VersaLexes**, and **Advanced**.

Filters can be saved and cleared as needed.

Transfer Status Filter - General Tab

Use the General tab to specify filter criteria based on specific trading partner connections, folder names, and hosts \mailboxes.

Include Trading Partner(s)

Select the check boxes for all the trading partners you want to include in the report.

Click **All** to select all the trading partners in the list.

Click **None** to clear all selected trading partners.

Include Folder(s)

Select the check boxes for all the folders you want to include in the report.

Click **All** to select all the folders in the list.

Click **None** to clear all selected folders.

Include Host(s)

Select the check boxes for all the hosts you want to include in the report.

Select the **Show Mailboxes** check box to include mailboxes within each of the hosts in the list.

Note: Transfers associated with host-based actions are displayed only if **Show Mailboxes** is unchecked and the associated host is selected.

Click **All** to select all the hosts in the list.

Click **None** to clear all selected hosts.

The **Username(s)** filter is shown if you have configured and enabled an LDAP server. You can enter a comma or semi-colon separated list of LDAP usernames. If you set this field, all but local FTP, HTTP, and SSH FTP LDAP mailboxes are excluded and only transfers for the specified users are included.

Transfer Status Filter - Tracking Tab

In addition to specifying a date range, and any filter selections made on the other tabs, if one of the file tracking features is enabled (see Transfers on page 895), you can also filter based on certain tracking criteria. You have the option to filter by either EDI, XML or text data. For the **Reference 1** and **Reference 2** filters, you can use the special % character at the beginning and/or end of the search value to perform wild-carded searches. When fields on the tracking tab are dimmed, it could indicate that the either the feature is not licensed or it is not enabled.

The […] buttons are present when Trading Partners are available for selection. These buttons allow the user to display the Trading Partners and configured Interchange Identifiers/Qualifiers. See Managing Trading Partners on page 631.

If you select a Trading Partner Alias along with **Use All Interchange Identifiers/Qualifiers**, a trading partner alias variable is used. This matches any of the Interchange Identifiers/Qualifiers configured for the Trading Partner. If you select **Use All Interchange Identifiers/Qualifiers**, you can select a specific Interchange Identifier/Qualifier pair to use. Once you have made your selections and click **OK**, the selection is placed in the appropriate fields depending on which button was selected.

Transfer Status Filter - VersaLexes Tab

You can filter by specifying a date range or any filter selections on the other tabs. If logging transfers to a database and synchronizing hosts across multiple instances of Cleo Harmony, Cleo VLTrader, or Cleo LexiCom software, you can also filter based on which instance performed the transfer. By default, all synchronizing instances of the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application are included. Also, if you specify numbers in the **Options** > **Transfers** > **Additional Serial Numbers** field, those numbers are displayed. See Transfers on page 895. The **All**

and **None** buttons allow you to select all or none of the instances of Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application.

Transfer Status Filter - Advanced Tab

You can filter based on transport, status, direction, and run type, in addition to specifying a date range and any filter selections made on the other tabs. The **All** and **None** buttons allow you to select all/none of the criteria for the particular section for which the button applies.

Transfer Table Standard View

The **Transfer Report** panel shows the status of the items that match the filter selected. The **File Type** column is displayed only if file tracking is enabled. This column displays `EDI` (EDI-X12, EDIFACT, or TRADACOMS), `XML` or `Text`, depending on the file tracking options and the file transferred. The **Run Type** column is only available when database transfer logging is being used. If are employing Cleo VLNavigator user groups, you can add columns, remove columns, and set the order of the columns per user group. See User Group File Transfer Report Tab on page 930.

Initially, the table is sorted by the **Start Time** of the transfer. Click any of the column headers to sort the table in ascending or descending order based on the contents of the selected column.

Note: A transfer could have a status of `Delete Error` or `Delete Resolved`. These are special statuses associated with a monitoring feature of the Cleo Harmony application. See Monitoring source deletion on page 54 for more information.

Click the buttons at the bottom of the table to change filter settings and refresh the table, find entries in the table, refresh the table with the current filter, generate an HTML report, and export the table to a CSV file.

Tool-tip snapshots

Tool-tip snapshots are only available under the following conditions:

- **Configure** > **Options** > **Transfers** > **Transfer Logging** is set to **Database**.
- For remote hosts, the `sentbox` and `receivedbox` are configured.
- For local users hosts, the archive `sentbox` and `receivedbox` are configured.
- **Configure** > **Options** > **Other** > **Disable Date/Time Portion of Filenames in Sent/Received Box** is unchecked (off).

To get a small snapshot of a file's contents, hold your mouse over the cell of the filename. The beginning of the file (up to 250 characters) will be displayed within the tool-tip help. If the file's contents cannot be displayed for any reason (for example, the file contains binary data), the tool-tip text will indicate the reason for non-display. Unlike other tool-tip help where the text is displayed for a maximum time period (usually a few seconds), this particular help is displayed as long as your mouse is over the filename.

You can select a range of rows, or multiple ranges, using the **Shift** and **Ctrl** keys. When selecting multiple rows, hold down the **Shift**/**Ctrl** key while right-clicking to display the menu. Release the **Shift**/**Ctrl** keys prior to clicking a specific menu selection.

Note: For the web UI, it is particularly important to release the **Shift** and **Ctrl** keys prior to making the menu selection, as leaving either depressed could bring up another browser tab.

Right-click menu options

Right-clicking on a row (or rows) displays a menu. The menu selections vary based on the characteristics of the selected rows.

You can select a range of rows, or multiple ranges, using the **Shift** and **Ctrl** keys. When selecting multiple rows, hold down the **Shift** or **Ctrl** key while right-clicking to obtain the menu. Then, release the **Shift** and **Ctrl** keys prior to clicking a specific menu selection.

Note: For the web UI, it is particularly important to release the **Shift** and **Ctrl** keys prior to making the menu selection, as leaving either depressed could bring up another browser tab.

Viewing detailed information

If any single transfer (row) is selected, then **View Information...** is available. A shortcut to this option is to double-click or right-click the row. When selecting **View Information...** or double-clicking, the transfer details will be displayed as shown in the dialog below. If the file type is EDI, the extracted EDI headers will be included at the bottom of the display. Furthermore, if EDI functional acknowledgments are being tracked, a **Show Acknowledgment(s)** button allows the corresponding functional acknowledgment transfer information and EDI headers to be added to the bottom of the display.

Viewing a copy

View Copy... is only available under the following conditions:

- **Configure** > **Options** > **TransfersTransfer Logging** is set to **Database**.
- For remote hosts, the sentbox and receivedbox are configured.
- For local users hosts, the archive sentbox and receivedbox are configured.
- **Configure** > **Options** > **Other** > **Disable Date/Time Portion of Filenames in Sent/Received Box** is unchecked (off).

For any single transfer, when **View Copy...** is selected, a dialog box appears and displays the file's contents. By default, the character representation of the file is displayed. It is also possible to display the file in various dump representations such as hexadecimal or octal. This allows the display of binary data -- a useful tool when looking for specific control characters. It is not possible to change the file's contents; this display is view-only.

Viewing Resend/Rereceive Chain

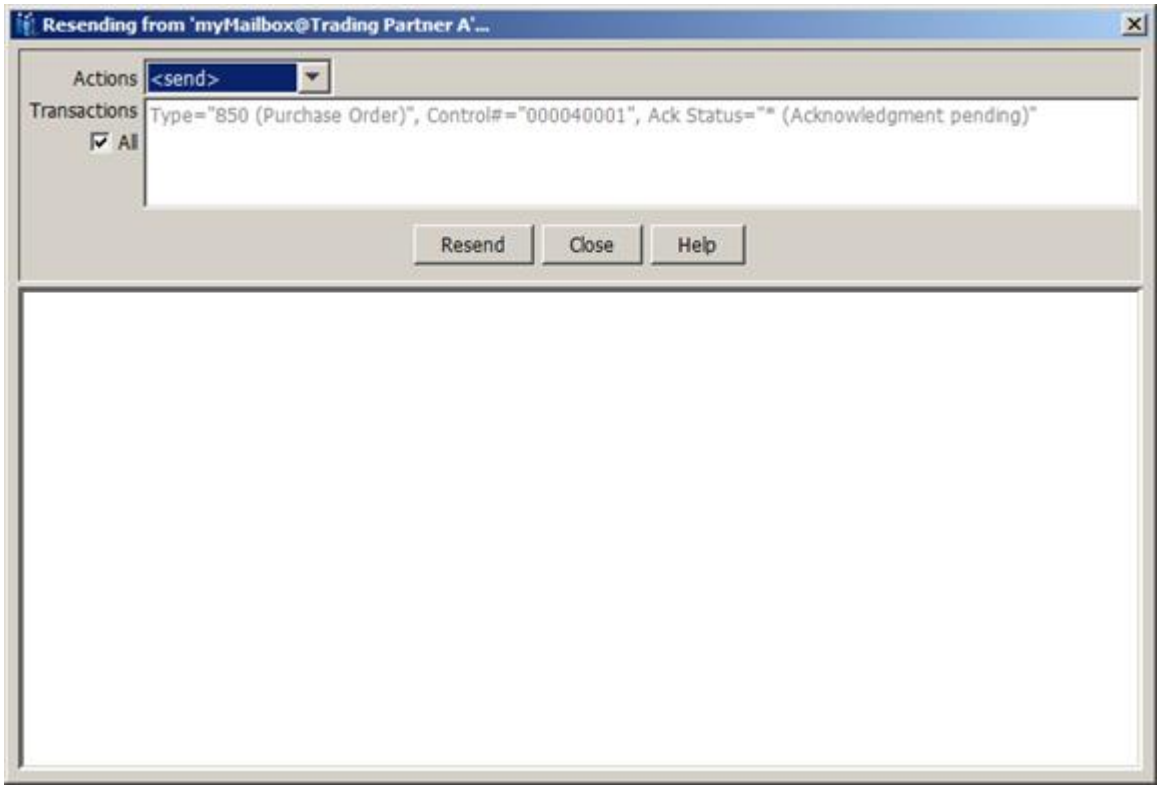
If the transfer has already been resent or rereceived, the chain of transfers can be viewed. The date/time, transfer ID and status of each transfer are shown in a hierarchical display. The pointer indicates the currently selected transfer.

Resending and rereceiving

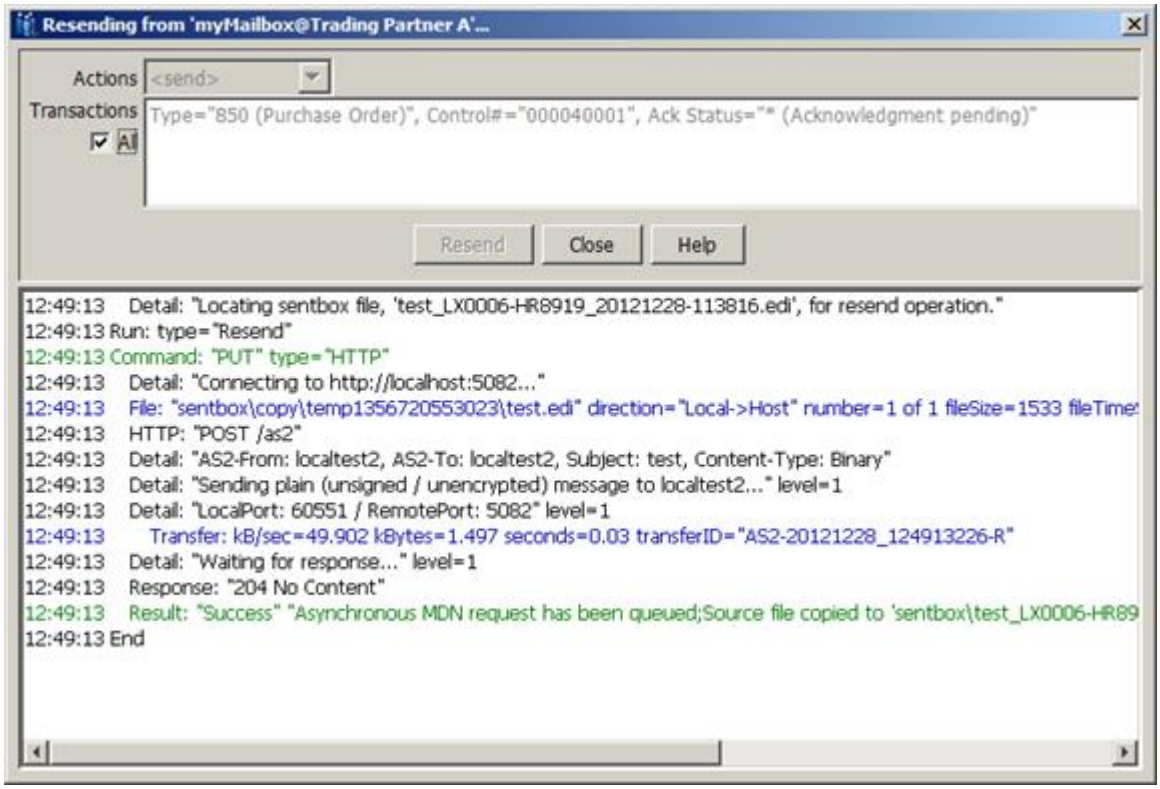
Resend and **Rereceive** are only available under the following conditions:

- **Configure** > **Options** > **Transfers** > **Transfer Logging** is set to `Database`.
- The `sentbox` or `receivedbox` is configured.
- **Configure** > **Options** > **Other** > **Disable Date/Time Portion of Filenames in Sent/Received Box** is unchecked (off).
- The send or receive applies to a remote host.

For one or more transfers, when you select **Resend** or **Rereceive**, the **Resend** or **Rerecieve** dialog box appears.



The **Actions** drop-down list provides the list of all actions within the mailbox. If all selected transfers belong to the same action, then that specific action will be pre-selected for you. If EDI file tracking is enabled, a list of **Transactions** is also displayed and a subset of transactions can be selected for resend or rereceive. After selecting the desired action and optionally transactions, click **Resend** or **Rereceive** to initiate the new transfer operation. The selected files will be located within the sentbox or receivedbox and run through the specified action. In the case of rereceive, an actual protocol transfer does not occur, but the file is re-streamed into the appropriate inbox directory and any execute/email on properties are invoked. The progress of the repeat operation is displayed within the dialog as shown below:

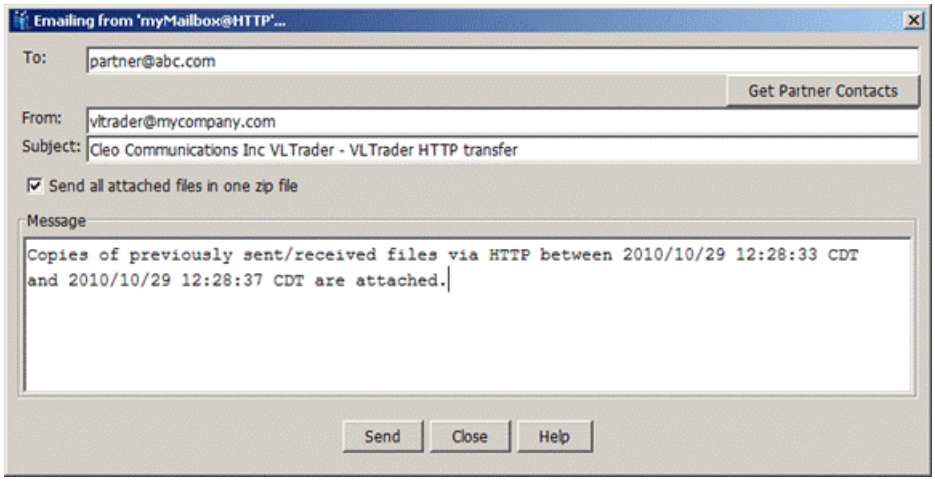


Emailing a Copy

Note: Email Copy is only available under the following conditions:

- **Configure** > **Options** > **Transfers** > **Transfer Logging** is set to **Database**.
- For remote hosts, the sentbox and receivedbox are configured.
- For local users hosts, the archive sentbox and receivedbox are configured.
- **Configure** > **Options** > **Other** > **Disable Date/Time Portion of Filenames in Sent/Received Box** is unchecked (off).

For one or more send or receive transfers, when **Email Copy...** is selected, the following dialog will be displayed.



Complete the following information on the screen:

1. In the **To:** field enter the email address of your trading partner. If the associated host is associated with a Trading Partner (see Managing Trading Partners on page 631) and the Trading Partner has Technical contacts, then a **Get Partner Contacts** button will be displayed. Selecting this button will fill the **To:** field with all the associated Technical contacts. Multiple valid email addresses may be specified, separated by colons, semi-colons, or commas.
2. The **From:** field's default value is taken from the 'System Administrator Email Address' defined in the **Other** tab of **Configure System Options**. If this field contains multiple email addresses, only the first address is used. See System on page 722.
3. Update the **Subject:** field as needed. It defaults to a string consisting of the license owner, product, and transport.
4. Choose the **Send all attached files in one zip file** option if you wish to compress the size of the data emailed or if your trading partner's email client has difficulty receiving your files due to certain file extensions.
5. Update the **Message** area as needed. It defaults to a descriptive message identifying the transport and time-date range.
6. After entering the needed information, click **Send**. The selected files will be located within the sentbox/receivedbox, optionally zipped into an archive, and then emailed. After the email has been successfully sent, you a dialog indicating success is displayed.

If there were any warnings or errors that were identified during emailing, you will receive notification of this as well.

Rerunning a Failed Action

If a single, failed send is selected, **Run Action** will be available. If **Run Action** is selected, the file size and modification time are compared against those from the original transfer. If the size and/or times are different, a dialog box describing the differences is displayed.

If the file has not been modified, a dialog box appears to verify the action to be run.

Note: Use extreme caution when using **Run Action** for the following reasons:

- The action may have already been run either by the scheduler, a translator, from command line, or interactively.
- The action may send other files besides the intended file.
- The action may be performing other operations (copying, deleting, and so on) besides the transfer of the intended file.
- The action may contain receive commands, in which case files will be retrieved from the trading partner.

The filter for the table can be modified again by clicking **Filter**. The **Refresh** button is used to update the table display in the case of new item availability. The refresh re-reads the data based on the current filter and re-displays the table. If the **Generate Report** button is clicked, the filter dialog is displayed allowing the user to select the report filter criterion.

Transfer Report Generation

Clicking **Generate Report** displays the report generation filter. This is the same dialog as above with the added **Include details** check box. If **Include details** is selected, every transfer matching the filter is displayed in the report. If **Include details** is not selected, only the totals are displayed. After selecting the criteria, click **Generate** to generate the report.

The **Include EDI** option is available only if EDI logging is enabled.

The report is sorted in order of Host\Mailbox followed by the transfer time. It contains the time span of the transfer, direction, status, bytes transferred, actual transfer time, and file name. The summaries contain a total of the number

of files based on the status and direction of the transfer. They also contain the number of bytes transferred and total transfer time.

Transfer EDI Table View

The EDI Transfer Report panel shows the interchanges that match the filter selected. Initially this is sorted by the Start Time of the transfer. By clicking on the column headers, the table can be sorted in ascending or descending order. If you select a row, the interchanges functional groups and/or transaction sets are then listed. If you double-click on a row in any of the tables, it will display the detailed transfer information regarding that interchange.

Right-clicking on a row will display a menu where you can choose from several actions.

If transaction rows are selected and functional acknowledgment tracking is enabled (refer to **Transfers EDI Logging under Configure System Options**) and the acknowledgment is still pending, then both **View Information...** and **Manual Acknowledgment...** will be available. **View Information...** gives the same information as double-clicking on the row. If **Manual Acknowledgment...** is selected and confirmed, the Ack Status is changed from pending (denoted by *) to manually acknowledged (denoted by @). Manual acknowledgment is useful for clearing pending acknowledgments that will never be received; however, a manually acknowledged transaction's Ack Status is still updated if a functional acknowledgment is later received. Also, right-clicking a manually acknowledged transaction will offer a menu containing **Undo Manual Acknowledgment…**, which allows resetting of the Ack Status back to pending.

Transfer Entries for CHECK Commands

The `CHECK` command is used to track certain events related to the transfer of data into and out of the Cleo Harmony environment. See CHECK command on page 943 for more information.

If the **ConditionsMet** parameter is specified on `CHECK` command, the results of the `CHECK` command are logged as a "quasi-transfer" and can subsequently be reported through transfer reports. Each `CHECK`'s quasi-transfer is given an ID, similar to a transfer ID on actual transfers. This ID is unique and starts with the word `CHECK`. The **Transport/Check** column of the transfer table will classify checks as either `CHECK FILE/DIR` or `CHECK TRANSFER`, based on the settings of the associated command. The only right-click menu item available for `CHECK` entries is **View Information...**. When **View Information...** is selected, a dialog such as the following will be displayed. Notice the **Command:** data item in this dialog. This item, which is only available if database transfer logging is enabled, is provided because the `CHECK` command can become quite complex if many parameters are specified.

Viewing transfer status - Web UI

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

The transfers page provides a tabular report of the transfers of individual files, reporting transfers sent/received due to a client action and transfers sent/received through server operations. When processing multiple files, each file transfer is recorded individually when the actual file transfer begins. The transfer status is updated when the transfer is completed.

To access transfers in the web UI, click **Transfers** in the top menu bar.

1. The transfer status page displays the following columns of information: **Start Time**, **Status**, **Node**, **Folder**, **Host**, **Mailbox**, **Direction**, **File**, **Protocol**, and **Run Type**. These columns are resizable and reorderable. To resize, click and drag the column separator. To reorder, click and drag the column headers. Table columns are also sortable by clicking on the column headers. This column configuration will autosave after you make your changes.
2. You can search or filter within these tables using the drop-down menus or search fields at the top of each column.

Resending and re-receiving - Web UI

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

If you wish to resend or re-receive a tranfer file, right-click on the row of the transfer in the table and select the option in the context menu. If the resend or re-receive option is available, it will appear in the right-click menu. Additionally, when a transfer is selected, the corresponding button for resend or re-receive will be enabled if the option is available. The resend and re-receive operations will run as a new transfer as a background operation. In order to see updated information on the resent or re-received file, refresh the data by clicking the refresh link at the bottom of the table. The **Run Type** column of the transfers table will display whether transfers have been resent or rereceived.

Transfer Report generation - Web UI

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

To generate a transfer report and export as an `.xlsx` file, click the icon in the lower right corner of the screen. A transfer report will generate a document with the applied filters, sort, and column order.

View Information - Web UI

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

If any single transfer is selected, the **View Information** button is available. A shortcut to this option is to double-click or right-click the row and select the option in the context menu. Note that viewing information will be unavailable when a transfer is in progress.

The **View Information** panel has two tabs. One displays general information about the transfer, and the other displays log events related to the transfer. Within this panel, you can always view the data in a new tab or to download it in a `.html` format. These buttons are located in the top right corner of the **View Information** panel.

View Information - Info tab

The **Info** tab displays the details of the specific transfer.

View Information - Events tab

The **Events** tab displays the events related to a transfer.

- The **Transfer Events** check box shows all of the log events related to the selected transfer.
- The **Other Events** check box shows all of the log events unrelated to the selected transfer. The other events will range from two minutes before the start time and two minutes after the stop time of the selected transfer.

View File - Web UI

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

For any single transfer, when the **View File** option is selected, a dialog box appears and displays the file's contents. By default, the character representation of the file is displayed. It is also possible to display the file in a hexadecimal dump representation. This allows the display of binary data, a useful tool when looking for specific control characters. It is not possible to change the file's contents; this display is view-only.

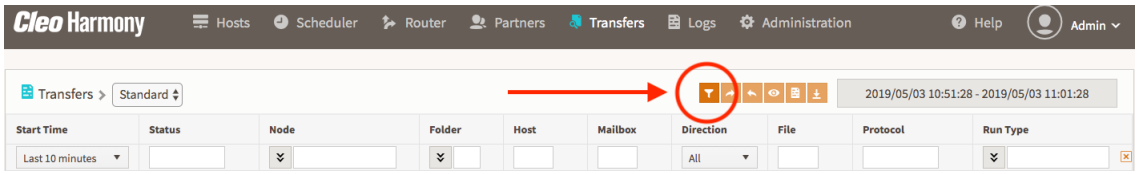
Download File - Web UI

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

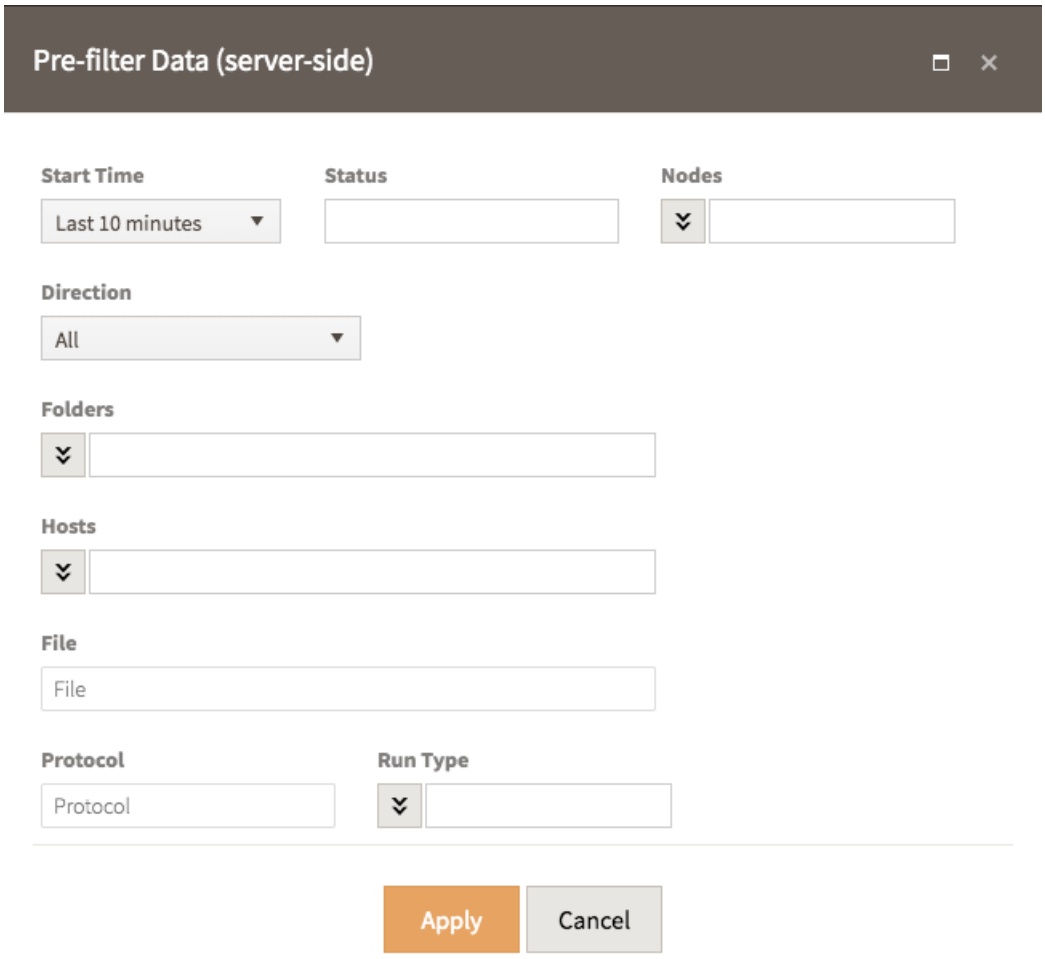
If any single transfer is selected, the **Download File** button is available. A shortcut to this option is to right-click the row and select the **Download File** option from the context menu. Note that a file cannot be downloaded if the size exceeds 2GB.

Advanced filtering options for Transfers

Advanced filtering options are used to pre-filter data from the server side before it reaches your **Transfers** page. To access these options, click the **Pre-Filter (Server-Side)** button in the button row:



The **Pre-filter Data (server-side)** dialog box appears:



Use this dialog box to control settings for pre-filtering data before it appears on your **Transfers** page.

Start Time

Use the **Start Time** drop-down menu to choose a start time for pre-filtering. The start time is bound to the full Transfers list start time.

Status

Use the **Status** field to filter by status. Select from **In Progress**, **Successes**, **Errors**, **Warnings**, and **None**.

Nodes

Use the **Nodes** option to filter by specific nodes. You can toggle this from a drop-down menu to a text field by clicking the down arrow button. Click the field to open the drop-down menu or, when toggled to text, enter text.

Note: Some users will not be able to see all **Nodes**. This will depend on specific system privileges. **Nodes** are live and if a node is offline, it will not appear in the drop-down menu and must be manually entered in the text field.

Direction

Use the **Direction** drop-down menu to filter by **Incoming**, **Outgoing**, or **All** transfers.

Folders

Use the **Folders** option to filter by specific folders. You can toggle this from a drop-down menu to a text field by clicking the down arrow button. Click the field to open the drop-down menu or, when toggled to text, enter text.

Hosts

Use the **Hosts** option to filter by specific hosts. You can toggle this from a drop-down menu to a text field by clicking the down arrow button. Click the field to open the drop-down menu or, when toggled to text, enter text.

File

Use the **File** field to enter a file name to filter by.

Protocol

Use the **Protocol** field to enter a protocol to filter by.

Run Type

Use the **Run Type** option to filter by specific run types. You can toggle this from a drop-down menu to a text field by clicking the down arrow button. Click the field to open the drop-down menu or, when toggled to text, enter text.

When you have finished making changes to your settings, click **Apply** to apply the settings and close the dialog box. Click **View** to see all the filters selected.

Chapter

10

Logs

Viewing log files

The system log file is a repository for ALL runtime messages. The existence of a log file and the level of messages stored in the log file can be configured. See Specifying default host directories on page 700 .

The entire log file can be viewed or the log file can be viewed relative to a particular tree branch.

Note: By default, when the system log file reaches five megabytes, the Cleo Harmony application automatically archives and restarts the log file.

1. To initiate viewing of the entire log file (that is, for `*`):
   - In the native UI:
     - Select **View** > **Log** in the menu bar
     - Click **Log** in the toolbar
     - Right-click in empty space in the tree pane and select **Log**
     - Right-click in the messages pane and select **Log**
   - In the web UI:
     - Select **Logs** from the menu bar
2. To initiate viewing of the log file relative to a tree branch in the native and classic web UI (that is, for <*action* > *mailbox@host*), right-click a *host*, *mailbox*, *action* or *local host* in the tree pane and select **Log**.
3. Further refine the criteria of the log file view:
   a) By default, the log file's entire date/time range (From and To) is viewed. Adjust as desired for viewing; pull-down lists provide common date and time values.
   b) The selected relative tree branch (For) can be modified or reselected via a pull-down list.
   c) By default, the active log file (File) is viewed. Browse for an archived log file.
   d) By default, all message types (`Run`, `Detail`, `Command`, `Result`, `File`, `Transfer`, `Request`, and `Response`) are viewed. For a description of the message types, see Screen layout on page 15. Click off any undesired message types.
   e) Manipulate as desired and click **OK**.

   All messages matching the specified criteria are listed in the upper portion of the window. The lower portion of the window contains summary statistics for the messages listed.
4. Right-click in the messages area.
5. Select **Find** to enter or recall a search string and find the first occurrence in the message list. Select **Find Next** to find the next occurrence.
6. Select **Copy** to copy all the selected messages (as text) to the system clipboard. Click on a message to select it. Multiple messages can be selected by holding the Shift or Ctrl key while clicking.

7. Select **Select All** to select all the messages at once.
8. Select **P Color** to remove coloring in the messages, if you prefer. Any **red** error conditions will appear **bolded** instead.
9. By default, the messages are sorted chronologically. Select **Sort** > **For** to sort the messages alphabetically by tree branch. Select **Sort** > **Message type** to sort the messages alphabetically by type.
10. Right-click in the summary area.
11. Select **Copy** to copy the summary (as text) to the system clipboard.
12. Additionally, since it is an XML file (and it is always well-formed), the log file can also be viewed through a browser at any time, potentially with an XSL style sheet applied. See XML file formats on page 969 for information about the layout of the log XML file.

Viewing the event log - Web UI

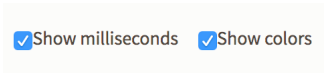
Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

The Cleo Harmony and Cleo VLTrader built-in NoSQL database in the web UI is used as a repository for all runtime messages and log files. The level of messages logged can be configured; by default, the last ten minutes of the event log is shown.

To view logged events in the web UI, click **Logs** in the top menu bar.

1.

   Using the drop-down menu at the top of the table, you can switch the logs table to display the **Event Log**, **Debug Log**, **Certificate Log**, and **System Counters**. Select **Event Log**.

   a) 

   Choose **Show milliseconds** to display or hide the milliseconds of the logs. Choose **Show colors** to view the line-based error and warning colors.

   b)
   Use the **View Thread Events** button by selecting a message row in the log table and clicking the **View Thread Events** icon. The event thread will appear in a tab below the log table. This tab is resizeable; click and drag the grey bar separating the table and the tab to change the size. Each time you click **View Thread Events**, the selected thread will open in a new tab.

   c)
   Use the **Pre-filter (Server-side)** button to pre-filter data before it reaches your **Logs** page. See Advanced filtering options for Logs on page 651 for detailed information.

   d) You can also double-click a specific message to view its thread events. The selected thread will open in a new tab.

2. To filter event logs, use the inline filtering options at the top of the log table. Available filtering options are **Date**, **Node**, **Source**, **Event Type**, and **Event Details**.

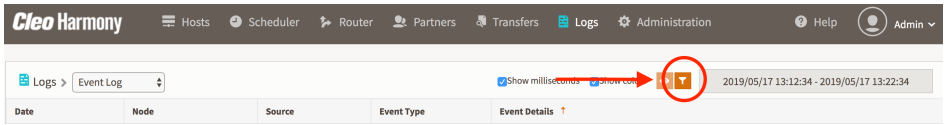
   a) Use **Date** to filter by date and time. Using the drop-down menu, choose from **Last 10 minutes**, **Last hour**, **Last 4 hours**, **Last 12 hours**, **Today**, **Yesterday**, and **Custom**. If you choose **Custom**, a **Date and Time** dialog box will appear. You can choose a custom date and time range in this dialog box. Click **Apply** to save your changes. Note that the read-only date range that is displayed in the upper corner of the page reflects your selection. Relative time selections are updated during any page refresh or by clicking the refresh button in the page footer. Custom selections are persistent until changed.

b) To filter by **Node**, click the **Node** menu which contains a list of all configured nodes in the cluster. Select the desired node(s).
c) To filter by **Source**, click the **Source** menu which contains a list of all sources represented by the current dataset. Select the desired source(s).
d) To filter by **Event Type**, click the **Event Type** drop-down menu. You can select **Errors**, **Warnings**, **Errors and Warnings**, and **Advanced**. Clicking **Advanced** opens a dialog box where you can choose the types of events by which to filter.
e) To filter by **Event Details**, click the **Event Details** menu and type a text string by which to filter.

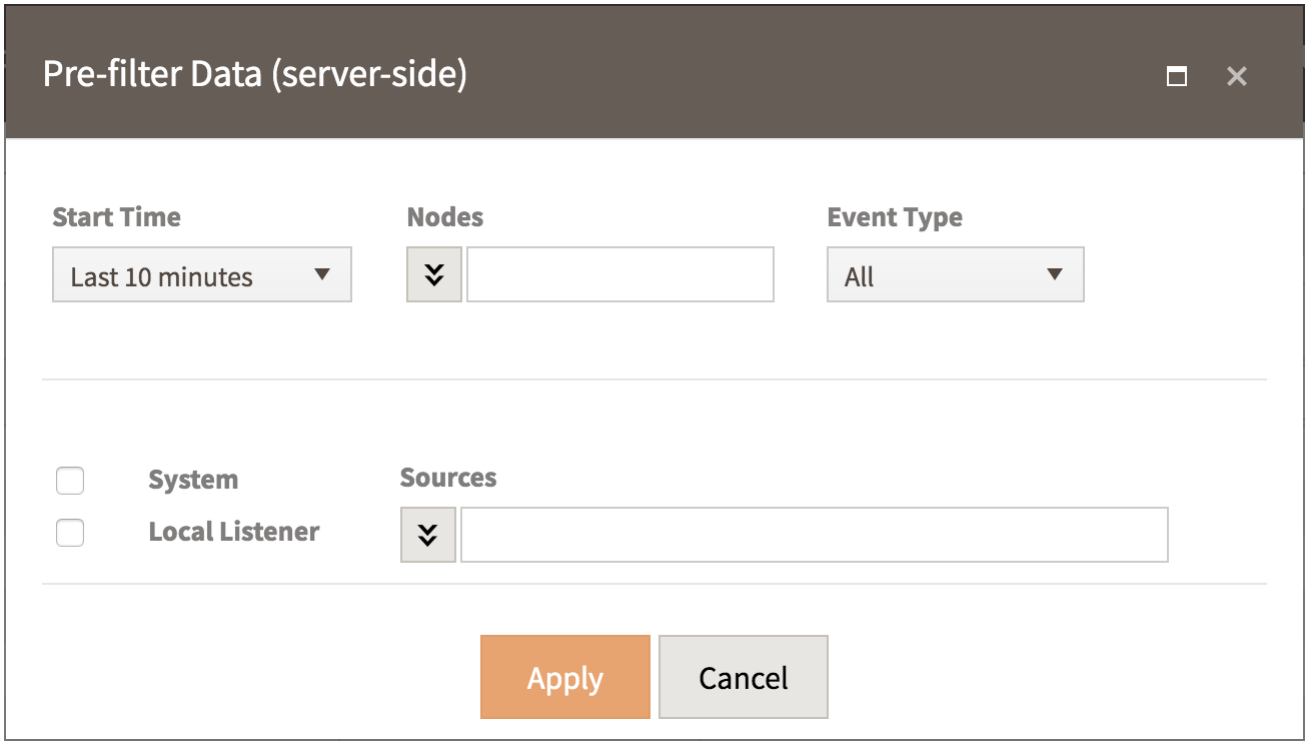
3. You can export the log threads. Click the tab of the event thread to be exported. Two orange buttons appear to the right of the tab:
a) **Open thread**: Opens the thread in a new browser window.
b) **Download thread**: Downloads the thread as an `.html` file.

Advanced filtering options for Logs

Advanced filtering options are used to pre-filter data from the server side before it reaches your **Logs** page. To access these options, click the **Pre-Filter (Server-Side)** button in the button row:



The **Pre-filter Data (server-side)** dialog box appears:



Use this dialog box to control settings for pre-filtering data before it appears on your **Logs** page.

Start Time

Use the **Start Time** drop-down menu to choose a start time for pre-filtering. The start time is bound to the full Logs list start time.

Nodes

Use the **Nodes** option to filter by specific nodes. You can toggle this from a drop-down menu to a text field by clicking the down arrow button. Click the field to open the drop-down menu or, when toggled to text, enter text. **Nodes** are live data. **Nodes** that are online are available for you to select from the drop-down menu. Offline **Nodes** must be typed into the text field.

Note: The **Nodes** visible to a given user depend on the user's specific system privileges.

Event Type

Use the **Event Type** drop-down menu to choose a type of event to filter. Select from **All**, **Errors**, **Warnings**, and **Errors and Warnings**.

Sources

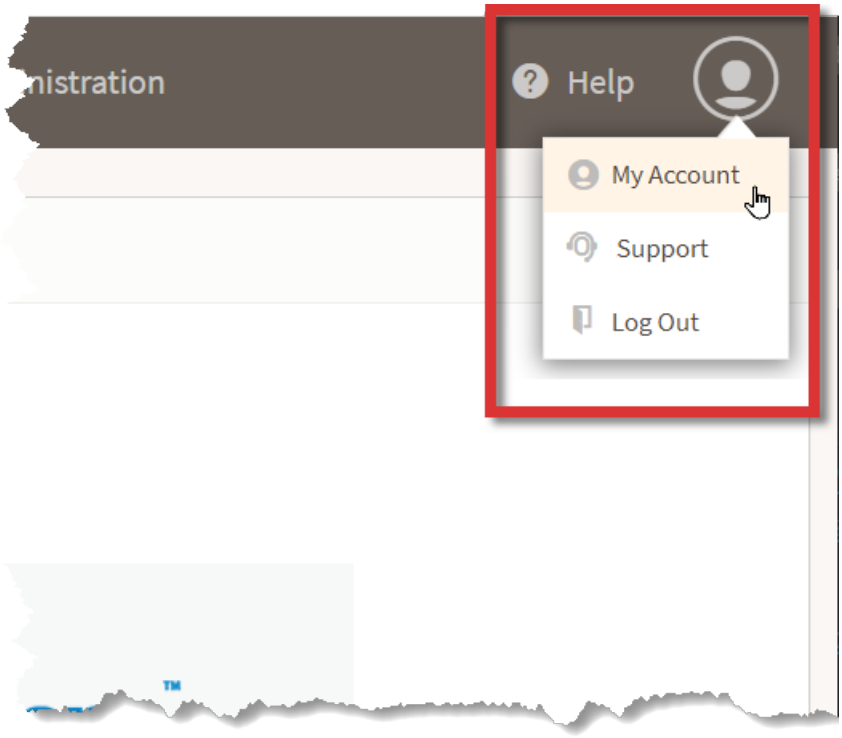
Use the **System** and **Local Listener** options to pre-filter data from the **System**, **Local Listener**, or both.

Use the **Sources** option to filter by a specific source. You can toggle this from a drop-down menu to a text field by clicking the down arrow button. Click the field to open the drop-down menu or, when toggled to text, enter text.

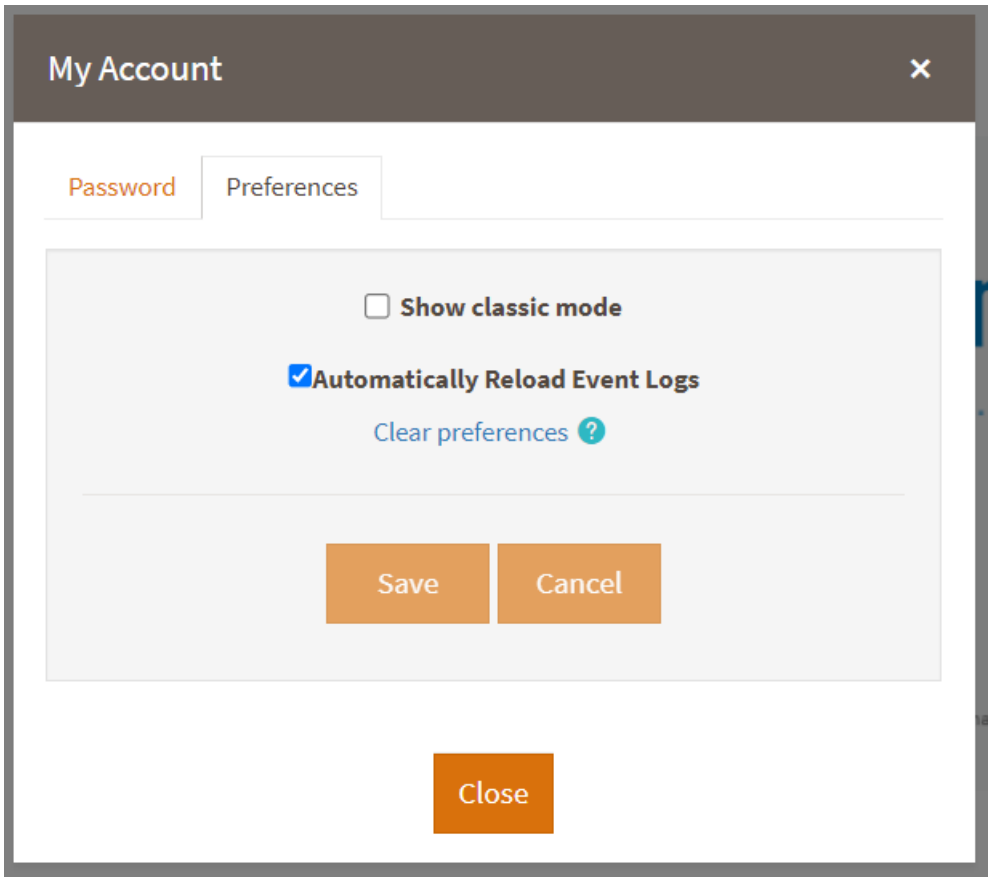
Controlling Event Log Loading

By default, when the Logs page is loaded, events are automatically loaded with the previously set filter. You can prevent event logs from being loaded automatically by deselecting the **Automatically Reload Event Logs** attribute as follows:

1. Click on the person icon in the top menu bar to display a drop-down menu, and select My Account.



2. In the My Account dialog box, select the Preferences tab.



3. Uncheck **Automatically Reload Event Logs** and click **Close**.

Chapter

11

Administration

License and registration

Licensing and registration functions allow you to request a permanent license, register your serial number and update your software.

About your license

Your Cleo Harmony license reflects the capabilities and restrictions of your installation. Understanding this information can help you track your capacity and plan for future growth.

You use the **License View** dialog box to review information about your license.

Viewing your license

You can use the **License** panel to review information about your Cleo Harmony license.

- In the web UI, go to **Administration** > **License**. In the native UI, go to **Tools** > **License**.

  The **License** panel displays.

License content

The top of the **License** panel displays your serial number, Host ID, and license owner name. The rest of the panel displays information about host and mailbox limits, and product features governed by your license and if or when it expires.

Limits

 # Hosts

Indicates the maximum number of hosts allowed by your license and the number you currently have.

 # Mailboxes

Indicates the number of mailboxes allowed by your license.

For the Cleo Harmony or Cleo VLTrader application, the maximum number of mailboxes allowed and the number you currently have.

For the Cleo LexiCom application, the number of mailboxes allowed per host.

Specific limits

Indicates the maximum number of mailboxes allowed per protocol and the number you currently have. Mailboxes for all protocols are available up to the `# Mailboxes` limit when no protocol-specific limits are present. The HSP protocol must be specifically licensed for Cleo Jetsonic to be available in the Cleo Harmony or Cleo VLTrader application.

Features and applications

Platform

- `Windows`
- `Unix` - Includes Linux and Solaris
- `Any`

The platforms for which the product is licensed.

Integration

`Yes` or `No`

Indicates that translator integration scripts can be generated.

Default value is `Yes` for the Cleo Harmony and Cleo VLTrader applications, and `No` for the Cleo LexiCom application.

VLProxy

`Yes` or `No`

Indicates whether Cleo VLProxy software is licensed. Requires separate installation.

Web Browser Interface

`Yes` or `No`

Web browser interface is licensed.

Default value is `Yes` for the Cleo Harmony and Cleo VLTrader applications, and `No` for the Cleo LexiCom application.

File Tracker

- `Off`
- `EDI`
- `All`

Indicates, along with transfer logging, whether EDI/XML/TEXT transfer file content can be detected and extracted.

Large File Applet

`Yes` or `No`

Indicates whether the Large File Applet is available with Cleo VLPortal.

Default value is `Yes` for the Cleo Harmony application, and `No` for the Cleo VLTrader application. Feature is not available in the Cleo LexiCom application.

High Availability Backup

`Yes` or `No`

Indicates whether this VersaLex application can only be used as a passive instance in a clustered VersaLex pool.

API

`Yes` or `No`

The Java API is licensed.

Default value is `Yes` for the Cleo Harmony and Cleo VLTrader applications, and `No` for the Cleo LexiCom application.

System Monitor

`Yes` or `No`

Cleo System Monitor software is licensed. Requires separate installation.

Default value is `Yes` for the Cleo Harmony application, and `No` for the Cleo VLTrader application. Feature is not available in the Cleo LexiCom application.

SNMP Agent

`Yes` or `No`

SNMP Agent functionality is licensed.

Default value is `Yes` for the Cleo Harmony application, and `No` for the Cleo VLTrader application. Feature is not available in the Cleo LexiCom application.

IP Filter

`Yes` or `No`

IP filtering is licensed.

Default value is `Yes` for the Cleo Harmony application, and `No` for the Cleo VLTrader application. Feature is not available in the Cleo LexiCom application.

JavaScript Actions

`Yes` or `No`

JavaScript actions are licensed.

Default value is `Yes` for the Cleo Harmony application, and `No` for the Cleo VLTrader application. Feature is not available in the Cleo LexiCom application.

Trigger Pool Size

Specific quantity or `Unlimited`

Maximum event trigger thread pool size per product instance.

Default value is `Unlimited` for the Cleo Harmony application, and `15` for the Cleo VLTrader application. Feature is not available in the Cleo LexiComapplication.

FIPS Mode

`Yes` or `No`

FIPS mode is licensed. Only available on Windows.

Default value is `No` for the Cleo Harmony and Cleo VLTrader applications. Feature is not available in the Cleo LexiComapplication.

Support

Indicates whether support is included and when it expires.

Requesting a permanent license

1. In the web UI, go to **Administration** > **License**. In the native UI, go to **Tools** > **License**.
2. Click **Request Permanent License**. **Request Permanent License** is also available from the license warning and expired windows that appear at product startup.
3. If you currently have a license, you must acknowledge that this is the final production destination for your product. Select **Cleo Harmony is installed into its final production destination**. Click **Continue**.

4. The contact information defaults to the registration. Modify it if necessary. If applicable, provide your EDI translator name and version and your firewall/proxy server and version; otherwise enter **None**.
5. If you do not have Internet access, press **Cancel** in the request permanent license dialog and then select **Send Email Request** to request a license file. A `license_key.txt` file will be emailed back to you. Either drop the file into the Cleo Harmony installed directory and restart the Cleo Harmony application or click **Browse** in the registration dialog and select the license file.
6. If you do have Internet access, modify the connection, if necessary. Click **Check for License**.
7. The differences between the active license and the available, permanent license are shown. Any major discrepancies are highlighted in red; otherwise differences are highlighted in orange. If you have any questions about your purchase order, contact your Cleo Sales Representative. Otherwise, click **OK** to continue.

After the initial permanent license, **Request Permanent License** can be re-used to update the license when a support subscription is renewed or more hosts are purchased.

Registering your serial number

In order for your Cleo product to be fully operational, you must first register your serial number.

1. When you invoke the application for the first time, it automatically prompts for registration.
2. If the product is being connected to a Cleo Harmony or Cleo VLTrader trading partner, the system administrator might have provided a network deployment URL. This deployment URL points to a zip file at a web location (possibly the Cleo VLTrader or Cleo Harmony application itself). If entered here, the zip file will be downloaded and imported after product registration is complete. The deployment URL can also be entered under **File** > **Import**.
3. If you do not have Internet access, you can click **Cancel** in the registration dialog and then select **Send Email Request** to request a license file. A `license_key.txt` file will be emailed back to you. Either drop the file into the installed directory and restart the product or click **Browse** in the registration dialog and select the license file.
4. If you use a proxy for Internet access, click **Set Proxy**. See Configuring for a proxy on page 881. If you use dial-up for Internet access, change the **Connection Type** to `Dial-Up Connection`, clear the **System Default** check box, and **Select** a phonebook entry. If you still have connectivity problems during the following steps, see Troubleshooting on page 965.
5. To continue registration, enter your serial number and click **Check Registration**.
6. Update the primary contact information, if necessary, and click **Register**.
7. If the registration is successful, a 30-day product key is activated.
8. After the initial registration, you can use **Tools > Register** to update the primary contact or company information, when necessary.

Updating your software

If you currently have a support contract, you might want to periodically check if new Cleo Harmony software is available for download or have the Cleo Harmony application notify you via email alerts when new software is available. Cleo Technical Support may also request that you download new software.

Software Update Contact Information

1. In the web UI, go to **Administration** > **License & Registration** > **Software Updates**. In the native UI, select **Tools** > **Software Update** from the menu bar.
2. The contact information defaults to the registration; change if necessary. Modify the connection type, if necessary.
3. Optional. Specify AS/400 Options.

a) If you are running the product on or interfaced to an AS/400 machine, click **Update Options**.

4. Choose from the following options:

   - **Cleo LexiCom application only**: If you are running on an AS/400, select **Download and unzip** AS/400 native software file.
   - If you are running on or interfaced to an AS/400, select **Download AS/400 network access software file**.
   - If this is the first time you are obtaining these files, select **Still download event if already at current release/ patch level**.

5. If you are not at the current release, you will need to install the current release before the AS/400 can be downloaded. If you are at the current release, the AS/400 files will be downloaded with a patch or by themselves. Click **OK**.

6. Optional. Receiving Software Update Email Alerts — You can configure your system to send email alerts to your registered email address when a software update is available. This feature may be enabled in either of the following ways:

   a) Each time **Check for Update** is clicked and the software update email alerts have not already been enabled, a dialog box is displays a message asking if you would like to be notified of software updates in the future.
   b) Click **Yes** to enable software update email alerts. If you do not want to receive these email alerts, you may suppress future displays of this dialog by clicking **No** and selecting **Don't ask me again** at the bottom of this panel.
   c) Click **Update Options** and select the **Send email when updates are available** check box.
   d) Click **OK**.

   Note: Future software update email alerts may be disabled at any time by deselecting this setting.

7. Manual Patch File Install

   a) If you are unable to access the Cleo website from the computer where the Cleo software is installed and a patch file has been emailed to you, click **Update Options**.

   b) Click **...** and after selecting the zip file, screens similar to the ones below will walk you through installation of the patch.
   c) Click **Check for Update**. The Cleo web site is queried and the notes relative to the release or release and patch are displayed.

   Note: If the active license is a permanent license, the Cleo web site also returns license information. If any discrepancies are found, software update is interrupted.

   d) If you are not at the current release, click **Continue** to start the download of the install. You will be prompted to select the temporary location for the install file. Remember this location as you may want/need to run the install manually. The install file is then downloaded.

8. Once the download is complete, you have the option of either starting the install immediately or waiting until later. If you are running as a Windows service or Unix daemon, be sure to stop the service/daemon before the install and restart the service/daemon after the install.

   If you are updating from one patch level to the current patch level, the changes between the two patches are highlighted with bold text when displayed or with a "+" when saved or printed.

9. If you are at the current release but not at the current patch level, click **Continue** to start the download of the patch file.

10. Once the download is complete, you are ready to install the patch. Click **OK**.

    The product will then do the following:

- wait for any currently running actions,
- backup any files that will be overwritten
- apply the patch files, and
- exit.

If you are running as a Windows service or Unix daemon, be sure to restart the service/daemon.

Unregistering a license

A given Cleo Harmony serial number can only be permanently licensed to one location. If it becomes necessary to move your installed location after you have already permanently licensed the product, first install the Cleo Harmony application at the new location.

An expiring license can also be unregistered, when necessary.

1. Select **Tools** > **License** from the menu bar.
2. If you are moving the Cleo Harmony application to another location, click **Unregister**. Before unregistering, you might first want to export user files. See Exporting user files on page 726.
   a) The contact information defaults to the registration; change this information and modify the connection type if necessary.
   b) Click **Request Unregister**. If the active license is a permanent license, the Cleo website is first queried for license information and any discrepancies are shown.
   c) If an expiring license is being unregistered, the Cleo Harmony application does not need to interact with the Cleo website.
   d) If the unregister is successful, the Cleo Harmony application shuts down. Register your serial number at the new location and import user files. Confirm that the new installation is operational, then uninstall at the old location.

Applications

The **Applications** tree branch contains information about the configurable applications. The applications listed under this branch include those configured for the Applications tree privilege under the **VLNavigator Privileges** tab for the user group associated with the current user. See User Group Tab on page 929.

When you select the **Applications** tree branch, the **Settings** tab appears.

The **Database** drop-down displays the list of databases that have been configured. See Databases on page 722. For any of the applications to be operational, a database must be configured. When the **Database** selection is cleared, the Application Settings dialog box appears, informing you that the applications will be disabled.

Test Database Connection can be used to test the connection to database. After the connection is tested, success or failure conditions will be reported.

Export Database Definition can be used to export the SQL statements that VLNavigator uses to create the database tables relative to the VLNavigator operations.

The exported file will contain the following types of DDL statements: CREATE TABLE, ALTER TABLE, and CREATE INDEX. These statements can be modified (e.g., to use a specific table space), but the table and column names must be unaltered. The modified script can then be used to create a modified database; however, if VLNavigator has already created the tables, DROP statements will need to be added to the beginning of the script.

After selecting the desired database and testing the connection, click **Apply**.

Certificate management

VersaLex provides functionality for managing digital certificates and private keys. It facilitates:

- generating self-signed user certificates and certificate signing requests (CSRs)
- importing/exporting user certificates/private keys
- importing/exporting certificate authority (CA) certificates
- marking CA certificates as either trusted or pending

When invoked through VersaLex during SSL negotiation, it also is used to:

- provide the set of trusted CA root certificates
- provide a selected user certificate chain

An X.509 certificate is equivalent to an ID card. It identifies a subject (entity) and an issuer (signer). If the subject and issuer are the same, the certificate is said to be self-signed.

The certificate infrastructure includes a public/private key pair for **encryption**. The public key is encapsulated in the digital certificate and is shared with trading partners. The private key is kept secret. Only the private key can be used to decrypt what has been encrypted by trading partners using the public key. A certificate and its public/private key pair can also be used as a **digital signature**.

Certificates are grouped into three categories:

- **User certificate**: Identifies a person (client) or a computer (server). User certificates, when first generated using Certificate Manager, are self-signed. If desired, they can be submitted to a certificate authority (CA) for signing. The CA-signed certificate then replaces the original self-signed certificate.
- **Intermediate CA certificate**: Identifies a trusted certificate authority (CA) whose certificate is signed by another intermediate CA or a root CA.
- **Root CA certificate**: Identifies a trusted certificate authority (CA) whose certificate is self-signed. A certificate "chain" is a series of CA-signed certificates terminated by a root CA certificate. A certificate chain consists of:
  - One CA-signed user certificate
  - Any intermediate CA certificates
  - One root CA certificate (sometimes referred to as the top level certificate)

Connecting a certificate's issuer CA to the next certificate's subject CA forms the chain. If a certificate's issuer CA cannot be found, the chain is incomplete. If a host requests the user certificate during SSL negotiation prior to a file transfer, the certificate chain, whether complete or not, is built and sent. Depending on the host, an incomplete chain may or may not affect the success of transfers.

For your convenience, VersaLex comes installed with an assortment of trusted VeriSign intermediate and root CA certificates and a trusted RSA root CA certificate.

All the certificates currently stored in Certificate Manager are listed directly under each store type (with a certificate icon). Certificate Manager builds and displays certificate chains starting in the users and trusted intermediate CA certificate stores trees. The certificates listed in these chains (with no icon) are references to a stored intermediate or root CA certificate.

If a chain is incomplete, the chain terminates with a `? Not Found` and the certificates in the chain are colored orange. If the issuer CA certificate is found but the signature is not valid, the chain is also considered incomplete. If signature verification is not an issue, it can be turned off by selecting **Configure** > **Options** and clearing **Check Certificate Issuer's CA Signature**.

If a certificate is not yet valid or is expired, the certificate is colored red. If validity is not an issue, it can be turned off by selecting **Configure** > **Options** and clearing **Check Certificate Validity Period**. When a certificate or a certificate chain is colored red, orange or is marked with a , additional tool-tip information is also provided.

The action items available at any given time from **Certificates** in the menu bar, the toolbar, and the right-click menus are dependent on the current selection in the tree pane.

Action items for adding a new certificate (e.g. generate user certificate, import) are enabled depending on the store type selected.

Action items for manipulating an existing certificate (e.g. generate CSR, replace, export, remove) are enabled depending on the certificate selected.

Note: The step-by-step instructions in the following sections describe the use of right-click menus. In all cases, Certificates in the menu bar provides the same selections. The toolbar provides most of the same selections.

Generating self-signed user certificates

To acquire a CA-signed certificate, you must first generate a self-signed user certificate. This will implicitly generate or import a public-private key pair.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click the **Users** store in the tree pane and select **Generate** > **Self-signed User Certificate**.

   The **Generate Certificate** dialog box appears.
3. Enter information about the certificate you want to generate.

   See User certificate reference on page 663 for information about the fields in the dialog box.
4. After you finish entering required information, click **OK**.

   After the key-pair and certificate are created, the certificate is added under **Users** in the tree pane.

   Note: Because generating a self-signed certificate might take some time because it could involve public-private key pair generation.

Generating a new self-signed user certificate based on an existing certificate

You can use the Certificate Manager to generate a new self-signed certificate based on the contents of an existing certificate. This is useful in situations where a self-signed certificate has expired and needs to be regenerated, or you want to generate a new self-signed certificate using the same information as an existing certificate.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click the existing certificate in the **Users** store and select **Generate** > **New Self-signed User Certificate**.
3. A new **Generate User X.509 Certificate** dialog is displayed with all the information from the original certificate except the **User Alias** and **Private Key Password**.
4. Enter new values in the **User Alias**, **Private Key Password** and **Confirm Password** fields, and then click **OK**.

   For information about these fields, see User certificate reference on page 663.
5. The new self-signed certificate is created and added to the **Users** store.

User certificate reference

User Information and Usage Information

User Alias

An arbitrary name for the certificate (for example, `CLEO`)

Common Name

A user name for client-style certificates; a fully qualified computer name (or registered IP address) for server-style certificates (for example, `cleo.com`). This field may be completed when importing OpenPGP or SSH FTP keys.

Email

Administrator email address, for example, `user@cleo.com`. This field may be completed when importing OpenPGP or SSH FTP keys.

Organization Unit

This could be a company department (for example, `Cleo Engineering`, or `Cleo Production`)

Organization

Official company name (for example, `Cleo Communications, Inc.`)

City

Complete city name (for example, `Loves Park`)

State

State name (for example, `Illinois`)

Country

Two characters (for example, `US`). Select from pull-down menu.

Signature Algorithm

Either MD5, SHA-1, SHA-256, SHA-384, or SHA-512.

SHA-256 is recommended for RSA certificates.

SHA-1 is the only valid signature algorithm for DSA certificates.

The appropriate algorithm is configured and this is field is disabled after importing OpenPGP or SSH FTP keys.

DigitalSignature

Set if certificate is to be used for SSL client or signing. **This field should generally be checked for AS2, AS3, or ebMS.**

KeyEncipherment

Set if certificate is to be used for SSL server or encryption. **This field should generally be checked for AS2, AS3, or ebMS.**

clientAuth

Set if certificate is to be used for TLS client. **Not applicable to AS2, AS3, or ebMS.**

serverAuth

Set if certificate is to be used for TLS server. **Not applicable to AS2, AS3, or ebMS.**

Subject Key Identifier

Set if the Subject Key Identifier extension is to be generated. This extension is used as a means of identifying the particular public key being used.

Valid For

The number of months that this certificate will be valid. By default, it is set to 24 months, but may be increased up to 96 months.

Generate Private

Used to generate a new public/private key pair.

Private Key Size

512, 1024, 2048, 3072 or 4096 for RSA certificates.

512 or 1024 for DSA certificates.

The larger the key size, the stronger the encryption; however, depending on your platform and/or CPU speed, generating certificates with private key sizes greater than 2048 bits may take several minutes. (2048 is the default for RSA certificates. 1024 is the default for DSA certificates.)

Algorithm

Defaults to RSA, which is the de facto standard. DSA is also available.

Private Key Password

This is an arbitrary password. This password can be any combination of letters, numbers, or special characters, but cannot start with an asterisk (*).

Confirm Password

Re-enter the private key password.

Encryption Sub-key Size

1024, 2048, or 4096-bit OpenPGP encryption sub-key size. Enabled when the Generate OpenPGP checkbox is selected. This is only necessary if you wish to generate a certificate to be used for OpenPGP encryption and an encryption sub-key is required.

OpenPGP Key Does Not Expire

When selected, the generated OpenPGP key will never expire. Otherwise, the OpenPGP key will expire when the User Certificate expires. Enabled when the Generate OpenPGP checkbox is selected.

Import OpenPGP

Used for OpenPGP encryption for an existing key.

OpenPGP Key

OpenPGP secret key. Browse/type for the OpenPGP filename.

Private Key Password

This must be the same password as the existing key.

SSH FTP Key

SSH FTP Key - to use an existing key for SSH FTP authentication. Enter the following information and click **Import** to read the key information. The Common Name and Email fields will be completed using the key information.

SSH FTP Key

SSH FTP private key. Browse/type for the SSH filename.

Private Key Password

This must be the same password as the existing key.

Generating PEM-formatted certificate signing requests

Once the self-signed user certificate has been generated, create and copy a PEM (Privacy Enhanced Mail)-formatted Certificate Signing Request (CSR) and paste it onto a web form on a Certificate Authority (CA) website. The CSR contains the public key of the key pair generated with the user certificate.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click a user certificate in the tree pane and select **Generate** > **PEM-formatted Certificate Signing Request**.

   The **CSR Generation** dialog box appears.

   Note: Certificate Manager will only allow a CSR to be generated for a self-signed certificate.
3. Enter the private key password and click **OK**. Use the same password that was used to generate the self-signed user certificate.
4. In the web UI, the CSR is downloaded. In the native UI, the CSR is displayed in a dialog box and you must click **Copy** to copy the CSR into the clipboard.
5. Paste the CSR into the CA's web form.

Generating trusted CA certificates from OpenPGP or SSH FTP keys

An OpenPGP public key contains a master key and one or more subkeys. You can create a Trusted CA Certificate from the public key information and use it to verify OpenPGP signatures and encrypt data before it is sent to your trading partner. You can use a SSH FTP public key for public key authentication with the SSH FTP server (Cleo VLTrader and Cleo Harmony only).

To import an OpenPGP or SSH FTP public key and generate a Trusted CA certificate:

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Import a key. Use one of the following methods.
   - **Choose an OpenPGP Public Key file** - Right-click the **Trusted CAs** store and select **Generate** > **Trusted CA Certificate from OpenPGP Key**.
   - **Choose an SSH FTP Public Key file** - Right-click the **Trusted CAs** store and select **Generate** > **Trusted CA Certificate from SSH FTP Key**.
3. Enter the name of or navigate to the public key file and click **Open**.

   The **Generate Certificate** dialog box appears.
4. Enter the required information. See User certificate reference on page 663 for information about the fields.

   User Alias

   An arbitrary name for the certificate (for example, `ACME`)

   Common Name

   This value might be provided when importing the public key. Alternatively, enter a user name for client-style certificates or a fully qualified computer name (or registered IP address) for server-style certificates (for example, `acme.com`).

   Email

   This value might be provided when importing the public key. Otherwise, enter the trading partner administrator email address (for example, `user@acme.com`).

   Organization Unit

   This could be a company department (for example, `Acme Purchasing` or `Acme Production`)

   Organization

   Official company name (for example, `Acme, Inc.`)

   City

   Complete city name (for example, `Loves Park`)

State

State name (for example, `IL`)

Country

Two characters only (for example, `US`). (This is available through a pull down menu.)

Valid For

If the chosen key does not have an expiration date, enter the number of months (1-96) the certificate should be valid for. If the chosen key has an expiration date this field is not configurable.

5. After all the required information is entered, click **OK**. After the certificate is created, the certificate is added under **Trusted CAs** in the tree pane.
6. For OpenPGP, you can view the embedded OpenPGP key fingerprint and usage in the **Certificate Manager** (using the right and/or bottom scroll bars, if necessary). Confirm the fingerprint shown matches the fingerprint provided by your trading partner. This ensures the public key has not been altered and the encrypted data you send can only be decrypted by your trading partner.

Replacing a user certificate with a CA-signed certificate (server ID)

After you submit a CSR to a Certificate Authority (CA) and receive the CA-signed certificate back, you must replace the user certificate previously generated in Certificate Manager.

If the CA-signed certificate is sent embedded in an email, cut and paste the certificate into a certificate file. This involves copying from the `-----BEGIN CERTIFICATE-----` marker to the `-----END CERTIFICATE-----` marker (inclusive) into a text editor. The extension you give the certificate file does not really matter. Certificate Manager will automatically determine whether just one certificate (CER/DER) or a certificate chain (P7B) is included. If a certificate chain is found, this means intermediate and/or root CA certificates have been included. These are imported, along with the CA-signed user certificate, into the proper stores.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click the user certificate in the tree pane and select **Replace** > **User Certificate**
3. Enter the private key password. Use the same password that was used to generate the self-signed user certificate.
4. Enter or browse for the certificate filename.

   Note: In the web UI, you must click **Import** to display a dialog box where you can enter or browse for a certificate filename, select a file, and then click **Open**.
5. Click **Import** to replace the user certificate with the CA-signed certificate.

   Note: You can repeat this process if a replacement CA-signed certificate is received at a later time.

Importing certificates

In addition to generating self-signed user certificates and replacing these with CA-signed user certificates, you can import user and CA certificates from scratch.

User certificates must always have an associated private key. When importing a user certificate, a private key must also be supplied. This is not the case with CA certificates. The Certificate Authority keeps its own private keys.

Importing user certificates and private keys (one PKCS12 file)

You can import a user certificate and private key together. A PKCS#12 file is password encrypted and contains both a certificate/certificate chain and the corresponding private key.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click the **Users** store in the tree pane and select **Import** > **User Certificate and Private Key...**
3. Type a new user alias.
4. Enter the password of the private key being imported. If the private key is unprotected (that is, it does not have a password), enter a password and select **Add password to unprotected key**.
5. Select **Personal Information Exchange-PKCS #12** (.P12).
6. Enter or browse for the PKCS12 filename. The PKCS12 file extension does not matter, as long as it is a valid PKCS12 file.
7. Click **Import** to import the user certificate (possibly with chain) and the private key.

Importing user certificates with private keys (two files)

You can import a user certificate and private key separately.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click the **Users** store in the tree pane and select **Import** > **User Certificate and Private Key...**
3. Enter a new user alias.
4. Enter the password of the private key being imported. If the private key is unprotected (does not have a password), enter the desired password and select **Add password to unprotected key**.
5. Select **Certificate file and Private Key file**.
6. Enter or browse for the certificate filename and the private key filename. The certificate file extension does not matter. The Certificate Manager will determine automatically whether just one certificate (CER/DER) or a certificate chain (P7B) is included.
7. Click **Import** to import the user certificate (possibly with chain) and the private key.

Importing CA certificates

You can import a CA certificate.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate ManagerTools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Do one of the following:
   - Right-click the **Trusted CAs** store and select **Import** > **Trusted CA Certificate**
   - or the **Pending CAs** store in the tree pane and select **Import** > **Pending CA Certificate**.

   Certificate Manager will automatically detect whether a certificate being imported is an intermediate or root CA.
3. Right-click the **Trusted CAs** store and select **Import** > **Trusted CA Certificate** or the **Pending CAs** store in the tree pane and select **Import** > **Pending CA Certificate**. Certificate Manager will automatically detect whether a certificate being imported is an intermediate or root CA.
4. Type or browse for the CA certificate filename. The certificate file extension does not matter. The Certificate Manager will automatically determine whether just one certificate (CER/DER) or a certificate chain (P7B) is included.
5. Click **Import** to import the CA certificate/certificate chain.

Exporting certificates

Any certificate or certificate chain in the certificate management database can be exported to a file to be archived or to be moved to another system.

For user certificates, this can include exporting the private key. This does not compromise the private key, because its password must be known both when exporting and importing.

Exporting user certificates

You can export user certificates.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Under **Users**, right-click the user certificate you want to export and select **Export** > **User Certificate**.
3. Select the file format: `DER`, `Base64 (CER)`, or `P7B`. If you selected to export the certificate chain, `P7B` is automatically selected for you.
4. Enter a filename for your certificate. When the certificate is exported, the correct file extension will automatically be added to the filename you enter if you don't provide it. By default the certificate will be stored in the home directory. You can choose to store your certificate file in another directory by first clicking **Browse…** and choosing a new directory before entering your certificate name.
5. Click **Export** to export the user certificate (possibly with the chain).

Exporting private keys

The following describes how to export a user certificate's private key.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click the user certificate in the tree pane and select **Export** > **Private Key**.
3. Select the file format - either `DER (P8)` or `Base64 (PEM)`.
4. Enter the password of the private key being exported.
5. Type or browse for the private key filename.
6. Click **Export** to export the private key.

Exporting both user certificates and private keys (one PKCS12 file)

The following describes how to export a user certificate and private key together.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click the user certificate in the tree pane and select **Export** > **User Certificate and Private Key**.
3. If a certificate chain exists, indicate whether the certificate chain should be included in the export.
4. Enter the password of the private key being exported.
5. Enter an optional friendly name. This value will appear in other Certificate systems, such as Microsoft® Internet Explorer.
6. Enter or browse for the PKCS12 filename.
7. Click **Export** to export the user certificate (possibly with chain) and the private key.

Exporting OpenPGP or SSH FTP keys

The following describes how to export an OpenPGP or SSH FTP keys.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click the user certificate in the tree pane and select **Export>OpenPGP or SSH FTP Keys...**
3. Choose the file format from the following:

   - `OpenPGP Public`
   - `OpenPGP Public/Private`
   - `OpenSSH FTP Public`
   - `SSH FTP Public (IETF format)`
   - `SSH FTP Private`

   Neither the OpenPGP Public/Private Keypair or SSH Private Key should be selected for export and sent to a trading partner. Instead, select the appropriate public key format if you wish to export for sending to a trading partner.
4. When either the **OpenPGP Public Key (.ASC)** or **OpenPGP Public/Private Keypair (.ASC)** options are selected, the **Preferred PGP Algorithms** panel is enabled, allowing selection of the preferred **cipher**, **digest** and **compression** algorithms to be used when exporting the public key or public/private keypair in `.asc` format. The preferred algorithm selection values are:

   - **Cipher**: TripleDES (default), Blowfish, CAST5, DES, AES-128, AES-192, AES-256, Twofish
   - **Digest**: MD2, MD5, RIPE-MD-160, SHA-1, SHA-256 (default), SHA-384, SHA-512
   - **Compression**: ZIP (default), ZLIB
5. Enter the **Private key password**. This field is not necessary when either the OpenSSH or SSH FTP format is selected and is disabled.
6. Enter or browse for the key filename. The appropriate extension will be appended to the filename.
7. Click **Export** to export the key.

Exporting CA certificates

The following describes how to export a CA certificate.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click the trusted intermediate CA certificate or root CA certificate in the tree pane and select **Export** > **Trusted CA Certificate**; or right-click the pending intermediate CA certificate or root CA certificate in the tree pane and select **Export** > **Pending CA Certificate**.
3. If a certificate chain exists, indicate whether the certificate chain should be included in the export.
4. Select the file format: `DER`, `Base64 (CER)`, or `P7B`. If you selected to export the certificate chain, P7B is automatically selected for you.
5. Enter or browse for the certificate filename.
6. Click **Export** to export the CA certificate (possibly with chain).

Replacing trusted CA certificates

When a trusted CA certificate has been updated by a trading partner, you can replace it in the certificate store while retaining the original file name so the partner's certificate defined in your host configurations does not need to be updated.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. In the tree pane, right-click the intermediate CA certificate or root CA certificate that you wish to replace and select **Replace** > **Trusted CA Certificate**.
3. Enter or **Browse** to the path of the new partner certificate that will be replacing the existing certificate and click **Replace**.

   Note: The extension of the new file must match the extension of the original file and the certificates must be of the same type. For example, you should not attempt to overwrite the contents of a `.p7b` file with the contents of a `.cer` file.
4. A dialog appears showing the content of the new and original certificates and asking for confirmation of the certificate replacement. By default, the original certificate file will be archived in the certs\archive directory and the archived file name will be appended with the current date/time stamp. If you do not want to archive the certificate, clear the **Archive original file before replacing it with the new content** check box.
5. Click **OK**.

Moving certificates

You can move a certificate from pending to trusted or from trusted to pending.

CA certificates can be either trusted or pending. Only trusted CA certificates are used during SSL negotiations.

Moving a pending CA certificate to trusted CA certificate

1. In the web UI, go to **Administration** > **Certificates** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click the pending intermediate CA certificate or root CA certificate in the tree pane and select **Move** > **Pending** > **Trusted CA Certificate**.
3. Click **Yes**.
   The CA certificate is moved into the trusted store.

Moving a trusted CA certificate to pending CA certificate

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click the trusted intermediate CA certificate or root CA certificate in the tree pane and select **Move** > **Trusted** > **Pending CA Certificate**.
3. Click **Yes**.
   The CA certificate is moved into the pending store.

Removing certificates

Exercise care when you remove a certificate. Once deleted, you cannot get it back.

Some user certificates are purchased items and might not be easily replaced. CA certificates, however, are readily available from the certificate authority.

Removing user certificates

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. In the tree pane, right-click the user certificate you want to remove and select **Remove** > **User Certificate and Private Key**.

3. Click **Yes**.
4. Click **Yes**.
5. If the certificate had a certificate chain, click **Yes** if those certificates should also be removed (if they are unreferenced by other chains).

Removing CA certificates

The following describes how to remove a CA certificate.

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.
2. Right-click the intermediate CA certificate or root CA certificate in the tree pane and select **Remove** > **CA Certificate**.
3. Click **Yes**.
4. If the certificate had a certificate chain, click **Yes** if those certificates should also be removed (if they are not referenced by any other chains).

Configuring certificate management options including CRL and TSL

The following describes how to configure certificate manager options, including how you want to work with certificate revocation lists (CRLs) and trusted service lists (TSLs)..

1. In the web UI, go to **Administration** > **Certificate Management** > **Options**. In the native UI, open the **Certificate Manager Options** dialog box – go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar and then select **Configure** > **Options**.
2. Select options from the **Acceptance Criteria** section.
   - **Check certificate validity period** – display certificates that are expired or within the warning period (15 days) in red and orange, respectively.
   - **Check certificate issuer's CA signature** – verify the issuer's signature when building the certificate chain.
   - **Check certificate verification** – check the validity of the certificate's signature algorithm and that it can be used within the current environment. When in FIPS mode, this setting is on by default and cannot be disabled. When not in FIPS mode, this setting defaults to off. If a certificate fails the verification check, it is marked with ⃠.
3. In the **Revoked Certificates** section, select **Check Revoked Certificates** to check the revoked status for each user and CA certificate and specify a value in the **every [n] hours** to control how often the check occurs. by using either the certificate's OCSP (Online Certificate Status Protocol) URL or CRL (Certificate Revocation List) URL. If a revoked certificate is found, it is marked with ⃠ and cannot be used during file transfers, whether as a server or client certificate, for signing or encryption, and so on. If it is a CA certificate, its issued certificates also cannot be used. In addition to checking CRLs actually contained within the certificates in the store, you can specify **additional CRL** URLs provided by certificate authorities can be configured and checked, if necessary.
4. Optional. Click **View Last Results…** to see the status of the certificate revocation checks.

   Each OCSP and CRL URL is listed along with the status result. Possible results are:

   - `No revoked certificates found`
   - `Revoked certificate(s) found`
   - `Check error: …`

   A `check error` can occur for varying reasons such as the URL being unreachable or the site returning an HTTP error code. Click **Check Now** to cause a new check to start in the background. Click **Refresh** to update the display if a check has just finished in the background.

5. In the Trusted Service List seciton, select the **Import Trusted Service (Status) List** check box to download and import the configured **TSL** URLs **every [n] hours**. A TSL contains a set of CA certificates to be automatically trusted. Whether a CA certificate is added or removed from the TSL, it is likewise added or removed from the local certificate store. Click **Import Now** to start a new import in the background.
6. In the **Logging** section, select the **Enabled** check box and then select a log level. A **High** log level is recommended while debugging a problem. You can find the debug log file can be found under the home directory at `logs\CertMgrLogfile.txt`. It contains information relative to security providers, certificate parsing, chaining, and usage, and UI invocation. Because the debug file will continue to grow, you should only enable certificate debug logging while you are investigating an issue, and you should disable it once the investigation is complete.
7. Click **View Last Results…** to see the status of the certificate revocation checks.

   Each OCSP and CRL URL is listed along with the status result. Possible results are:

   - `No revoked certificates found`
   - `Revoked certificate(s) found`
   - `Check error: …`

   A `check error` can occur for varying reasons such as the URL being unreachable or the site returning an HTTP error code. Click **Check Now** to cause a new check to start in the background. Click **Refresh** to update the display if a check has just finished in the background.
8. Click **Save** (web UI) or **OK** (native UI).

Viewing user and CA certificate usage

1. In the web UI, go to **Administration** > **Certificate Management** > **Certificates**. In the native UI, go to **Tools** > **Certificate Manager** or click the **Certificates** button in the tool bar.

   Each user and trusted CA certificate is listed by either alias (user certificate) or filename (CA certificate). Supplemental information includes the certificate expiration date and specific active host usage. A certificate is repeated in the list if it has multiple uses.
2. Double-click a certificate to display a detailed description.
3. For distribution, click **Save As...** to save the report as HTML.

Exchanging certificates with your trading partner

There are several methods to exchange certificates with trading partners, including email and EDIINT Certificate Exchange Messaging (CEM).

CEM was developed through a Drummond Group initiative to automate the secure exchange of public-key certificates between trading partners over the internet. Since the structure of a CEM is of a specific format (currently only supported in AS2), CEMs should only be sent to trading partners capable of receiving and processing them. The Cleo Harmony, Cleo VLTrader, and Cleo LexiCom applications are CEM-capable and can successfully process properly formed messages. CEMs should only be used to update existing certificates in an established trading partner relationship. The initial exchange of certificates for new trading partner relationships should be done out-of-band, for example, through the Email Profile Utility - see Emailing a profile to your trading partner on page 87.

Displaying the certificate exchange dialog box

There are several ways to launch the Certificate Exchange dialog box:

- From the **Certificate Manager** window, choose the **Tools** > **Exchange Certificates** option.
- From the host tree, select a mailbox, right-click and select **Exchange Certificates**
- From the **Certificates** panel, click **Exchange Certificates**.

Additional certificate filtering

Independent of the current **Protocol** and **Status** filter settings, you can filter records containing specified certificates by clicking **More Filters...**

Each certificate field in the pull-down list contains all the certificates (for that field's type) that are currently defined in the table.

Selecting a certificate for one or more certificate fields and clicking **OK** will cause records containing only the specified certificate(s) to be displayed.

To disable filtering on the previously selected certificate(s), click **More Filters...** again and then click **Clear**.

To hide all 'Disabled' and/or 'Undefined' status entries in the table view, check the appropriate selection.

After clicking **OK**, all entries with a status of 'Disabled' or 'Undefined' will no longer be displayed.

Sending certificate exchange messages

To send new certificates to your trading partner(s) via EDIINT Certificate Exchange Messaging, the following pre-requisites must be satisfied:

- The trading partner relationships must already exist. EDIINT Certificate Exchange Messaging may only be used to upgrade certificates in established trading relationships.
- Your trading partner(s) must be capable of sending and receiving EDIINT Certificate Exchange Messages (that is, for **AS2-CEM** protocols only).

If either of these pre-requisites has not been satisfied, you can still use the Certificate Exchange dialog boxes, but the certificates are sent using **Email** instead. See Exchanging certificates with your trading partner on page 672. See Non-CEM capable trading partners on page 676 for further information.

1. Open the Certificate Exchange dialog box. In the web UI, go to **Administration** > **Cerfiticate Management** > **Certificate Exchange**. In the native UI, click **Certificates** in the menu bar to display the **Certificate Manager**, and then in the **Certificate Manager**, go to **Tools** > **Exchange Certificates**.

   The **My Certs** tab appears.
2. In the **My Certs** tab, select the AS2-CEM trading partner(s) you want to exchange with.
3. In the Command menu, select **Send New Certificates**, and then click **Proceed**.

   The **Send Local Certificates** dialog box appears, allowing you to select certificates for this trading relationship.
4. Select certificates.
   a) Before you enter information to select certificates, you might have to enable fields, except for the Signing Certificate fields, which are always enabled.

      To enable the **Encryption Certificate Alias** fields, clear the **Use Signing Certificate** check box. Clearing this check box means you choose to use separate certificates for signing and encryption. If you leave this check box selected, the certificate you select as the signing certificate is also used for encryption.

      To enable the **SSL Client Certificate Alias** fields, select the **Send SSL Client Certificate** check box.

      To enable the **SSL Serer Certificate Alias** fields, select the **Send SSL Server Certificate** check box.

      If a certificate is already pending from a previous certificate exchange, the fields and the **Browse** button for that certificate are not enabled.
   b) For each certificate you want to send, type a certificate alias name in the **Alias** field or click **Browse** to navigate to a certificate and select it.
5. The **Send** button is enabled only if previous messages from the trading partner have included a specific header indicating that the partner is CEM-capable. You can verify this capability by ensuring that the **Partner Is CEM-Capable** setting in the **Host** > **AS2** panel is set to `True`.

If the partner has specifically requested the exchange of new certificates using EDIINT Certificate Exchange Messaging but **Send** is not enabled, select the **Partner Is CEM-Capable** option to force sending of the new certificates via EDIINT Certificate Exchange Messaging.

6. Click **Send**, click it to send the Certificate Request message.

   A confirmation dialog box appears.

7. Click **Yes** to verify the certificates you selected are the ones you want to send.

   If any of the specified certificates are already active (that is, installed) for this trading relationship, an additional confirmation dialog box appears asking if you want to send the installed certificates.

8. Click **Yes** to send all new and previously installed certificates to your trading parter.

   Click **No** to send only the newly selected certificates to your trading partner.

   If all the selected certificates are already installed, clicking **No** returns you to the previous **Send Local Certificates** panel allowing you to either choose new certificates to send to your trading partner or to cancel the send operation altogether.

9. The **My Certs** tab appears and, if the Certificate Request is successfully sent, its status is set to `Pending`.

   If an error occurred, you can correct any issues, select the partner entry, and click **Retry**.

10. Click **Close**.

    The status of the Certificate Request is set to **Pending** if it was successfully sent. (If an error occurred, the Certificate Request message can be re-sent after correcting the problem, if possible, by selecting the partner entry and invoking **Retry**.)

    The new certificates are displayed in the panel with the current certificates and are be editable until after certificate acceptance and your trading partner begins encrypting with the new encryption certificate.

    If a new SSL Server certificate was sent, the new certificate is displayed in the Local Listener's HTTP panel with the current certificate. **Certificate Alias** is read-only until all HTTP partners have received and accepted the new certificate. Once this has occurred, the new SSL Server certificate is automatically installed (normally within five-minutes).

    Since only one HTTP SSL Server certificate can be active at any time, the new SSL Server certificate is the only certificate that can sent for all subsequent Certificate Exchange Messages.

Receiving inbound EDIINT CEM responses

When a response to the Certificate Request message has been received and the partner has accepted all the new certificates, an email notification will is sent to the email addresses specified in the **Admin Email Address** field on the **Other** tab in **Configure System Options** panel, the status of the partner record is set to **Active** and the appropriate statuses of the certificates can be viewed using the tool tips (by using the cursor to mouse-over the desired certificates). See Other system options on page 729.

The new SSL certificate remains in an "accepted/pending" state until it has been exchanged with and accepted by all trading partners using HTTP/s.

Note: Your trading partner should respond to the Certificate Request within *the Maximum Allowed CEM Response Days* specified in the **Local Listener Advanced Panel**. See Specifying Local Listener advanced properties on page 759. If this time period is exceeded without a response, an email notification will be sent to the email address(es) specified in the **Admin Email Address** field on the Other tab in Configure System Options panel , and the status will be set to Expired. See Other system options on page 729. Since it is possible that your trading partner may not be able to respond to your CEM requests, you should contact him to determine why a timely response has not been received. You may need to resend your CEM request or distribute your new certificate(s) through another method. Once your trading partner has verified that

he has installed your new certificates, you should then manually switch this trading relationship to the new certificates using the 'Set As Active' command in the Certificate Exchange dialog.

Using the local encryption certificate for the first time

Since the partner might not always begin using the newly-accepted certificate immediately, messages received by the trading partner might be decrypted with either the old certificate (CLEO-ENCRYPT) or the newly accepted certificate (CLEO). Once an encrypted message is received from the trading partner using the new certificate (referred to as "first-usage"), it is automatically installed as the active certificate in the panel.

Receiving inbound EDIINT CEM requests

When you receive an inbound Certificate Request message from your trading partner:

1. An email notification of the inbound Certificate Request (CEM) message is sent to the email addresses specified in the **Admin Email Address** field on the **Other tab in Configure System Options** panel with information about the received certificates and the "Respond By" date by which a response should be sent. See Other system options on page 729
2. The received certificates are stored in the certs\pending folder until they are either accepted or rejected; or manually installed by you when it is deemed necessary.
3. The status of the partner record in the **Trading Partner Certs** panel is set to `Pending`.
4. The **Signing Certificate** field is updated to indicate that there is a new pending certificate, although it is not used to validate signed messages until after it has been accepted. Likewise, the encryption field is not updated until after the new encryption certificate is accepted.

Auto-accepting inbound EDIINT CEM requests

You can choose to auto-accept inbound Certificate Request messages from any or all of your trading partners by selecting the **Auto Accept Received Certificate (CEM)** Advanced property in the Local Listener panel. This system-wide setting can be overridden at the host level by selecting the **Override Listener CEM Auto Accept** setting, allowing you to limit auto-accepting to only the desired trading partners.

Responding to inbound EDIINT CEM requests

After a new Certificate Request has been received by your trading partner and auto-accept has not been enabled (see Auto-accepting inbound EDIINT CEM requests on page 675), the pending certificates can be viewed by either right-clicking on the individual partner's record and choosing the **Display** option, or by double-clicking on the partner record. A panel showing all active and pending certificates is displayed.

After viewing the newly-received certificates, you can choose to either Accept or Reject any or all the received certificates by selecting the partner record in the **Trading Partner Certs** panel, invoking the desired command option and then clicking **Proceed...**:

If you choose **Accept**, you will be given the option to accept any or all of the pending certificates. (Likewise, if you choose **Reject**, you will be given the option to reject any or all of the received pending certificates.)

If the certificates are accepted, the old encryption, SSL client and SSL server certificates (if applicable) will be archived in the certs\archive directory and the newly received certificates will be installed and activated and the status of the partner record will be set to **Active**.

Using the partner's signing certificate for the first time

Since the partner might not always immediately begin signing with the newly-accepted signing certificate, the signatures of the messages received by the trading partner can be verified with either the original or newly-accepted partner signing certificates. Once a message received from the trading partner has been signed with the newly-

accepted signing certificate (referred to as “first-usage”), it is automatically installed as the active certificate in the panel and the original signing certificate is archived in the certs\archive directory.

CEM-specific email alerts

The following email alerts are generated and sent to the email addresses specified in the **Admin Email Address** field (see System on page 722) on the **Other** tab in **Configure System Options** panel when the following events occur:

1. An inbound CEM Request message is received by a trading partner and auto-accept has not been enabled. (See Auto-accepting inbound EDIINT CEM requests on page 675.)
2. An inbound CEM Response message is received by a trading partner.
3. An inbound CEM Response message has not been received by the trading partner in response to a previously pending CEM Request before the locally specified 'Respond By' date (from the originally received CEM Request message). **Daily email alerts will continue to be sent until the response is received or some other manual intervention is taken.**
4. An outbound CEM Response message has not been sent in response to a trading partner's previously pending CEM Request before the trading partner's specified 'Respond By' date. **Daily email alerts will continue to be sent until the response is sent or some other manual intervention is taken.**

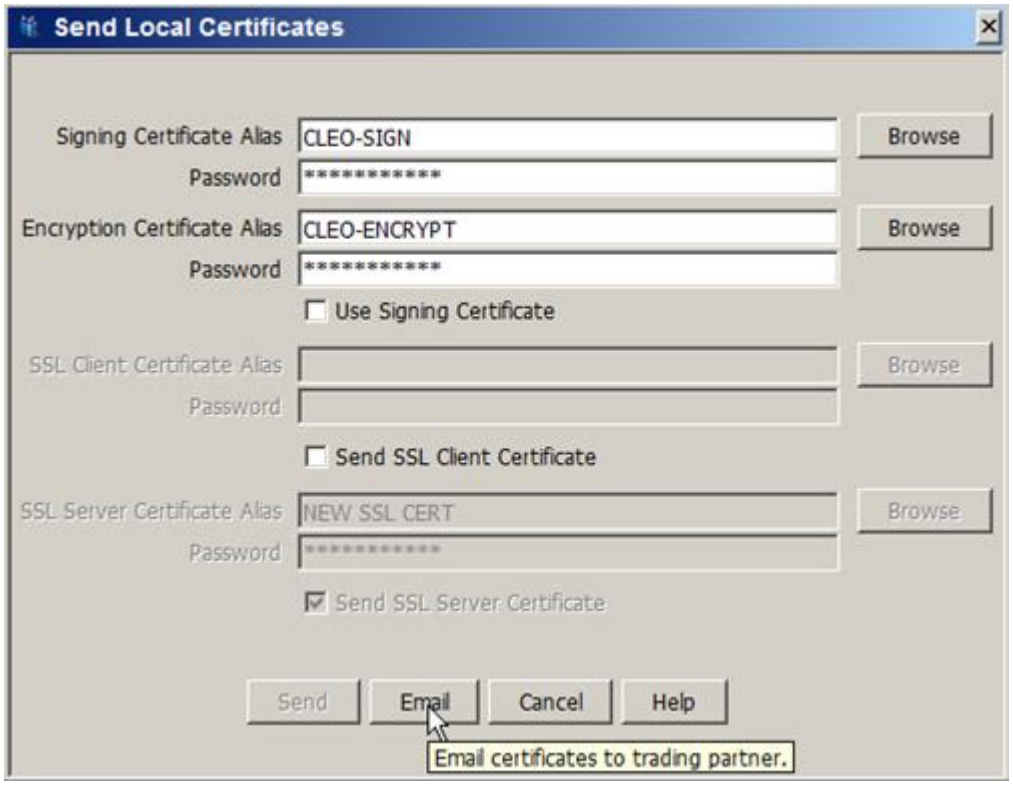
Additionally, daily email alerts are sent for the following scenarios:

1. An inbound CEM Request message has been received by a trading partner and still requires a response and it is still before the trading partner's specified 'Respond By' date.
2. The pending SSL Server Certificate still needs to be sent and/or accepted by some of your trading partners. Since only one SSL Server Certificate may be active, the pending certificate cannot be installed until all trading partners using the current SSL certificate have received and have accepted the pending SSL certificate. Once this has occurred, the Local Listener will automatically install (normally within five minutes) and begin using the pending SSL certificate.
3. One or more of your trading partners has rejected the pending SSL Server Certificate. Since the new SSL Server Certificate cannot be activated in the Local Listener while it has a **Rejected** status for any trading partner relationships, you should contact these trading partners to resolve any issues and then manually set the status to **Active** by selecting the **Set As Active** command option in the **My Certs** panel and then click **Proceed...**
4. More than one unique SSL Server Certificate has been accepted by your trading partners. Only one SSL Server Certificate can be defined in the Local Listener for HTTP/s or FTP/s (Cleo Harmony and Cleo VLTrader only), however different SSL Server Certificates can be specified for the HTTP/s and FTP/s protocols.

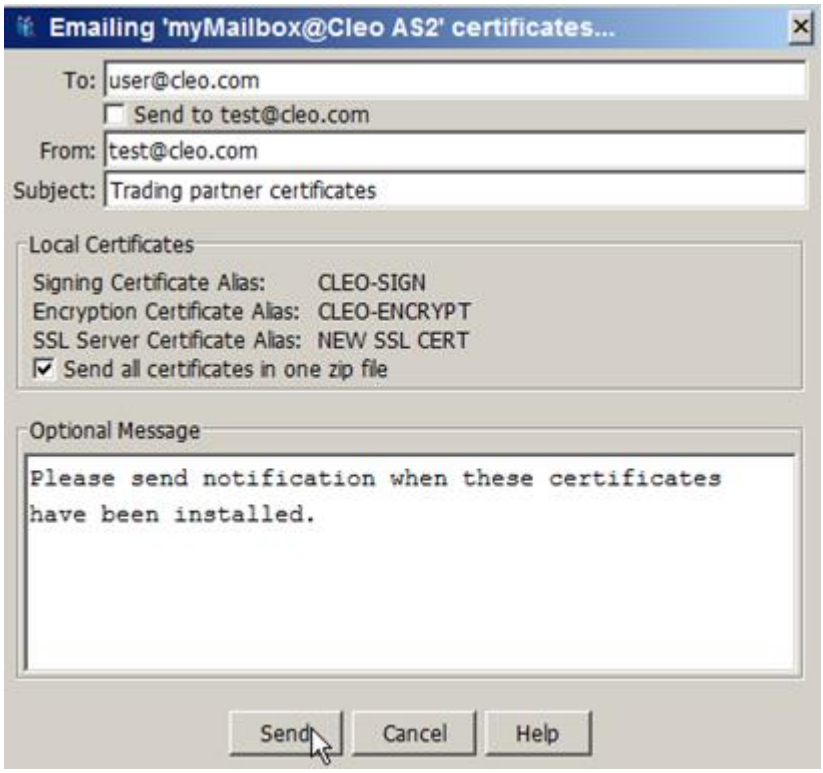
Non-CEM capable trading partners

The Certificate Exchange Dialog can be used to exchange certificates with non-CEM capable trading partners (that is, for protocols other than **AS2-CEM**) or when setting up initial trading partner relationships by sending the certificates via email.

Select the appropriate certificates to send to your trading partner just as you would do when sending certificates to your CEM-capable trading partners, but click **Email** instead of **Send**.

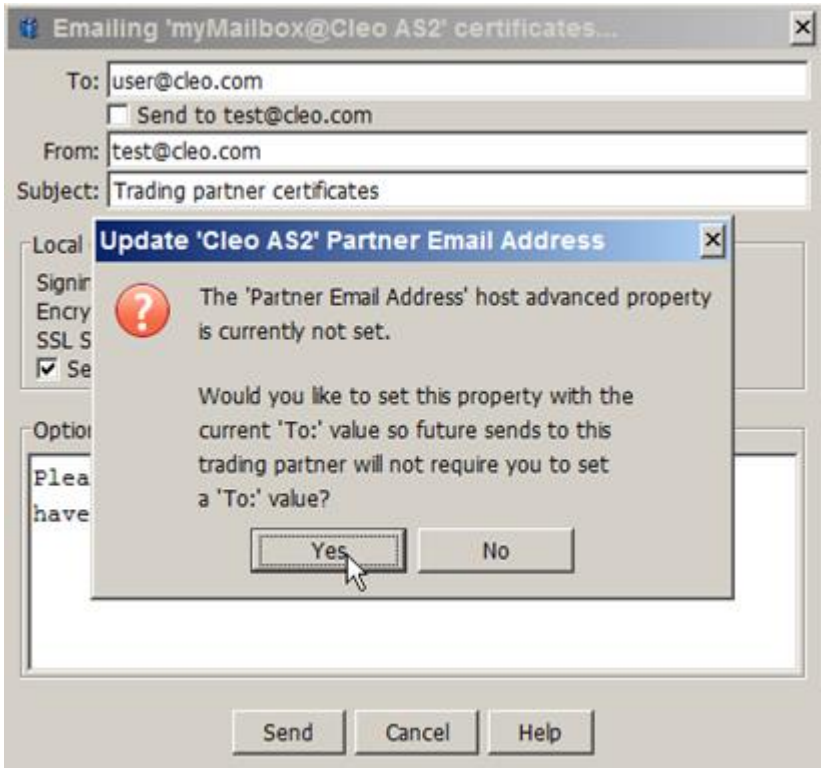


The following dialog is displayed. See Emailing a profile to your trading partner on page 87 for more information.

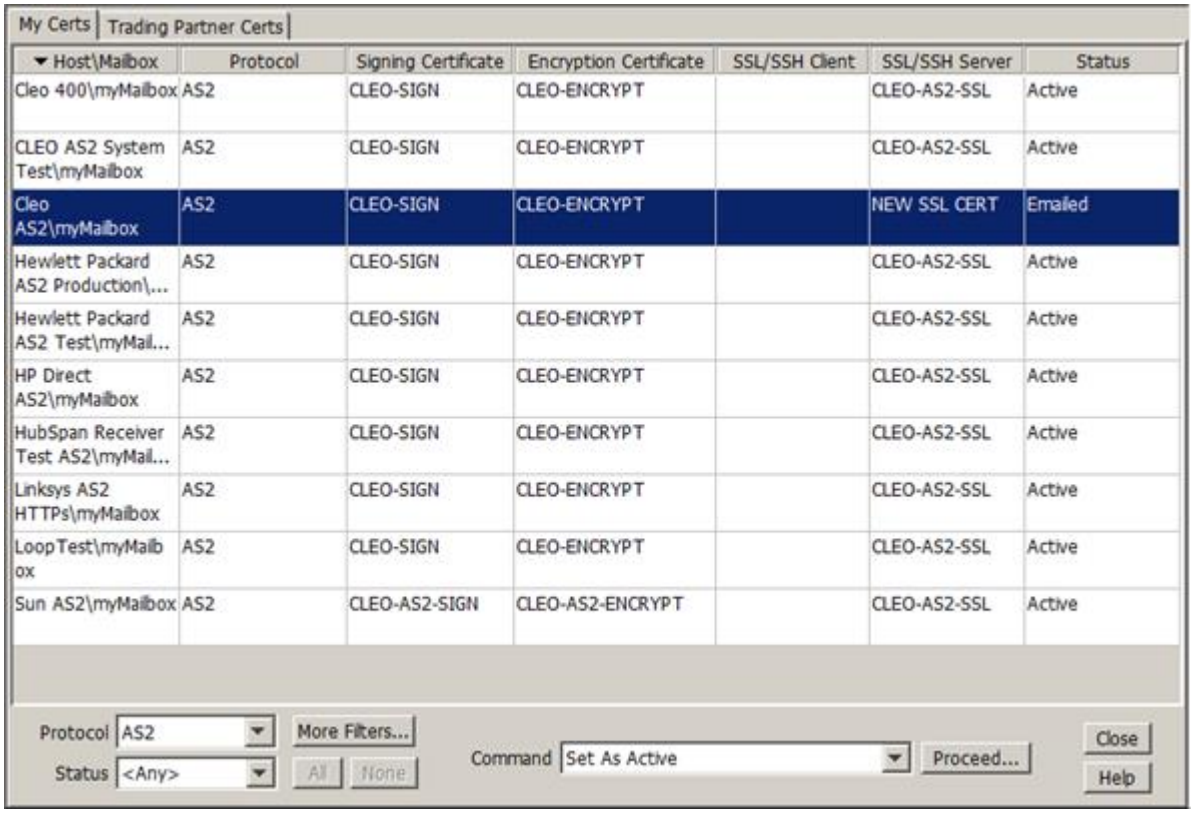


When you click **Send**, the following confirmation dialog box is displayed allowing verification of the new certificates before sending them to your trading partner:

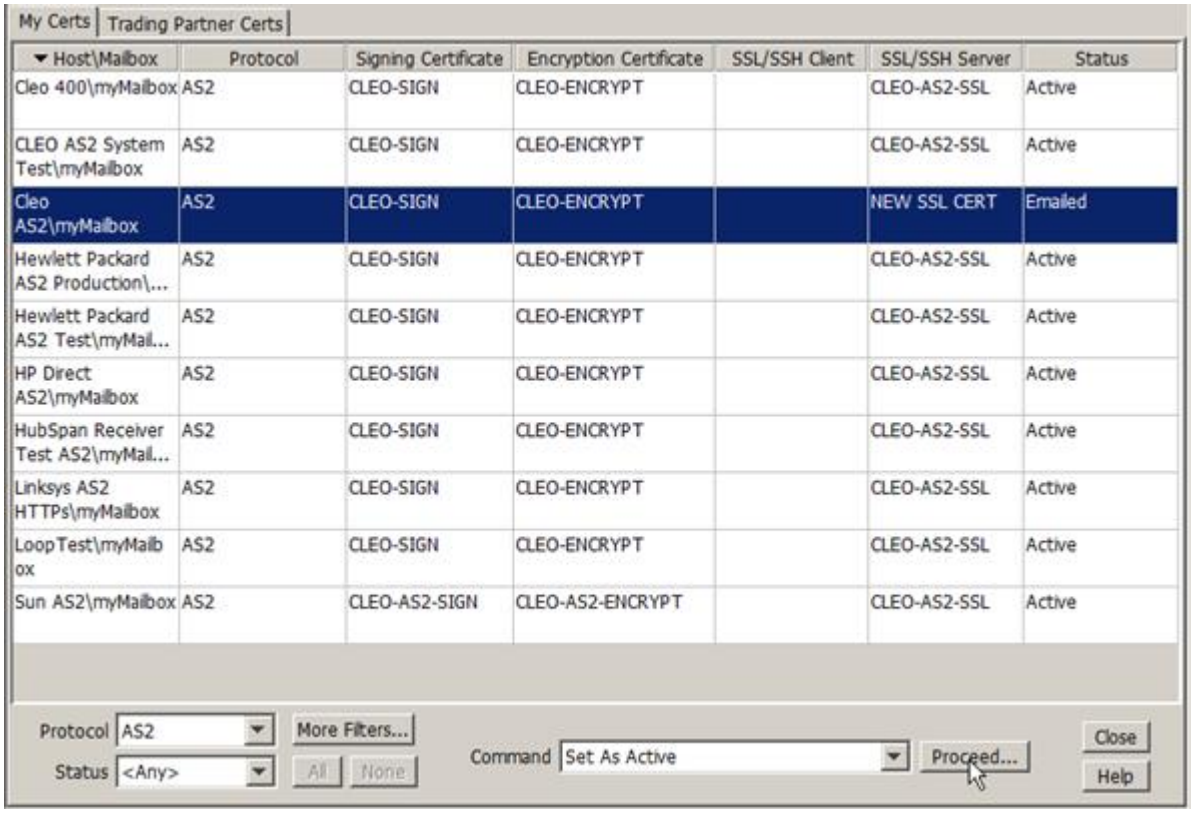
Additionally, if the Partner's Email Address is not currently set in the Host's Advanced Panel, the following prompt is displayed, allowing you to update that property with the currently defined 'To:' email address:



Once the certificates have been successfully sent, the status of certificates in the **My Certs** panel is set to `Emailed`.



After you have received notification that your trading partner has verified and installed your new certificates, they should manually be activated by selecting the trading partner's record in the **My Certs** panel, choosing the **Set As Active** command option and then clicking **Proceed...**:



About the Certificate Exchange dialog box

The **Certificate Exchange** dialog box displays all active and, if applicable, pending or rejected certificates for each trading partner relationship.

Features of this dialog box include:

- Sorting and filtering of records by protocol and current status
- Additional filtering of records by certificate selection - see Exchanging certificates with your trading partner on page 672 .
- The ability to hide all records with a status of ‘Disabled’ and/or ‘Undefined’
- Simultaneous selection of multiple records that are currently filtered by the same protocol and status
- Command options available for any/all selected records based on the current filter settings
- The ability to optionally send new certificates to your trading partner through EDIINT Certificate Exchange Messaging (CEM) - if your trading partner is CEM-capable; or through email if your trading partner is not CEM-capable; or if you are setting up the initial trading partner relationship and have never previously exchanged certificates with a trading partner
- The ability to have certificates be activated for use at a scheduled time. See Scheduling certificates for future use on page 681 for detailed information.
- Certificates for individually selected records may be viewed by either right-clicking on that record and choosing **Display** or by double-clicking on a specific record. (Viewing of certificates when more than one record is selected is not supported.)

The local certificates (for example, your self-signed or CA certificates that are sent to your trading partners) are viewable from the **My Certs** tabbed panel.

The certificates that are received from your trading partners are viewable from the **Trading Partner Certs** tabbed panel.

Note: In either the **My Certs** or the **Trading Partner Certs** panels, initially the **Protocol** and **Status** filters are set to **<Any>** when the Certificate Exchange dialog is launched from either the Local Listener or from the **Tools>Exchange Certificates** menu in the Certificate Manager.

Whenever the **Protocol** or **Status** filter settings are set to **<Any>**, selecting an individual record on the panel displays a dialog box that prompts you to filter on the specified record's protocol and status.

Click **Yes** to filter on the specified protocol and status; to allow selection of multiple records; and to enable the commands relevant to this protocol and status.

Note: Multiple records may be selected/deselected by clicking **All** or **None**; or by simultaneously pressing the **<Ctrl>/<Shift>** key and the desired records.

Click **No** in response to the filtering prompt to operate only on the selected record. Filtering will not be done and only one record may be selected at a time. Commands only relevant to the protocol and status of the selected record may be invoked.

Select **Don't ask me again during this session** to disable the filtering prompt. The last selected option will be used as you move from record to record. This prompt will not be displayed again until the next time the Certificate Exchange dialog is launched.

Note: Commands will only be enabled when at least one record is selected.

When the Certificate Exchange dialog box is launched from a mailbox, that mailbox is initially selected and the records are pre-filtered for the current protocol and status of that mailbox. Additionally, the ability to filter on any other protocol or status is disabled.

Multiple record selection (by clicking **All** or **None**; or by simultaneously pressing the <Ctrl>/<Shift> key and the desired records); filtering on desired certificates by clicking **More Filters...**; and executing commands by clicking **Proceed...** is done in the same way as when the Certificate Exchange dialog is not launched through a mailbox.

Scheduling certificates for future use

Your Cleo product provides the ability to select local or partner certificates on a per trading partner basis that can be activated for use immediately or at a scheduled time in the future.

In addition, trading partners using non CEM-capable AS2 or AS3 protocols will automatically be able to take advantage of the "first-usage" features for scheduled local encryption certificates and scheduled partner signing certificates. See Exchanging certificates with your trading partner on page 672.

To schedule new certificates for future use for one or more trading partners:

1. Go to the **My Certs** or the **Trading Partner Certs** panel.
2. Select the certificate you want to schedule for future use.
3. Select the **Schedule Certificates For Future Use** command option and click **Proceed...**
   The **Schedule Local Certificates** dialog box displays.
4. Select one or more new certificates. You can browse to a new certificate or specify a certificate explicitly for the following:
   - **Signing Certificate Alias**
   - **Encryption Certificate Alias**
   - **SSL Client Certificate Alias**
   - **SSL Server Certificate Alias**
5. Add the correct private key password to the appropriate **Password** field.

6. Select the appropriate options:
   - Select **Use Signing Certificate** to choose the same certificate for Signing and Encryption or deselect this option to use different certificates for Signing and Encryption.
   - The **SSL Client Certificate Alias** and **Password** fields will only be enabled if an SSL Client certificate had been previously selected for the trading relationship. To override selection of these fields, **Schedule SSL Client Certificate** may be selected or deselected as desired.
   - The **SSL Server Certificate Alias** and **Password** fields will only be enabled if the associated secure port for this protocol (in this case HTTP/s) has been enabled in the Local Listener. To override selection of these fields, **Schedule SSL Server Certificate** may be selected or deselected as desired.
   - Select the desired **Activation Date** and **Time** from pull-down lists or specify your own date (in the form: 'yyyy/mm/dd') and time (in the form: hh:mm or hh:mm:ss).
   - If you are scheduling a certificate for use with PGP partner packaging signing/encryption key, you can choose the **Allow Overlapping Key Usage** option. This option is useful when a new key has been scheduled but not yet activated and decryption of an inbound file fails using the installed key. Using this option allows your system to attempt decryption using the scheduled but not-yet-active key. Additionally, during this overlap period, outbound files are signed using both the installed and scheduled keys to avoid possible signature verification errors by the trading partner. By default, the **Allow Overlapping Key Usage** option is selected.

     Note: Only *partner* packaging certificates are used when scheduling for packaging certificates even though the UI displays *Local* in some dialog boxes.
7. Click **Schedule** to schedule the selected certificates for future use.
   A confirmation dialog box displays.
8. Click **Yes** to confirm that all selected certificates should be scheduled for installation and activation for the specified trading partners.
   Click **No** to return to the Schedule Local Certificates page, where you can choose other certificates and options.
9. If you confirmed certificates to be scheduled, you can choose to email the scheduled certificates to your trading partners.
10. The new certificates are displayed in the panel with the current certificates and are not editable until after the scheduled certificate activation date and time or, for AS2 and AS3, your trading partner begins encrypting with the new encryption certificate.
    When the activation date and time occurs, scheduled certificates are activated and an email notification is sent to the email address specified in the **Admin Email Address** field on the **Other tab in Configure System Options** panel. See Other system options on page 729.

    If you scheduled a new SSL or SSH Server certificate, the new certificate is displayed in the Local Listener's HTTP, FTP, OFTP or SSH FTP panel (depending on the specified protocol) along with the current certificate. The **Certificate Alias** is read-only until all partners using the same SSL/SSH protocol have scheduled the new certificate and that scheduled date has passed. Once this has occurred, the new SSL/SSH Server certificate will automatically be installed – typically, within about five minutes.

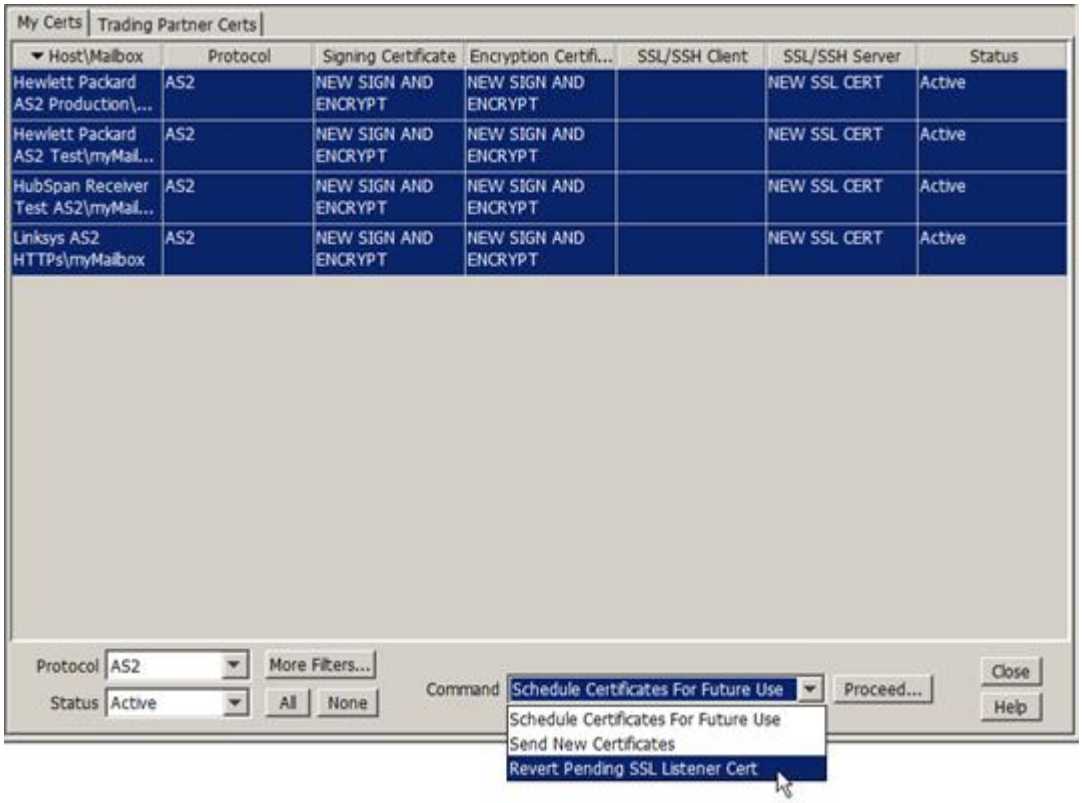
    Because only one HTTP, FTP, OFTP and SSH FTP server certificate can be active at any time, the new server certificate relevant to the specified protocol is the only certificate that can be scheduled for all subsequent schedule requests for any other protocols that use the same server certificate.

Reverting a certificate schedule

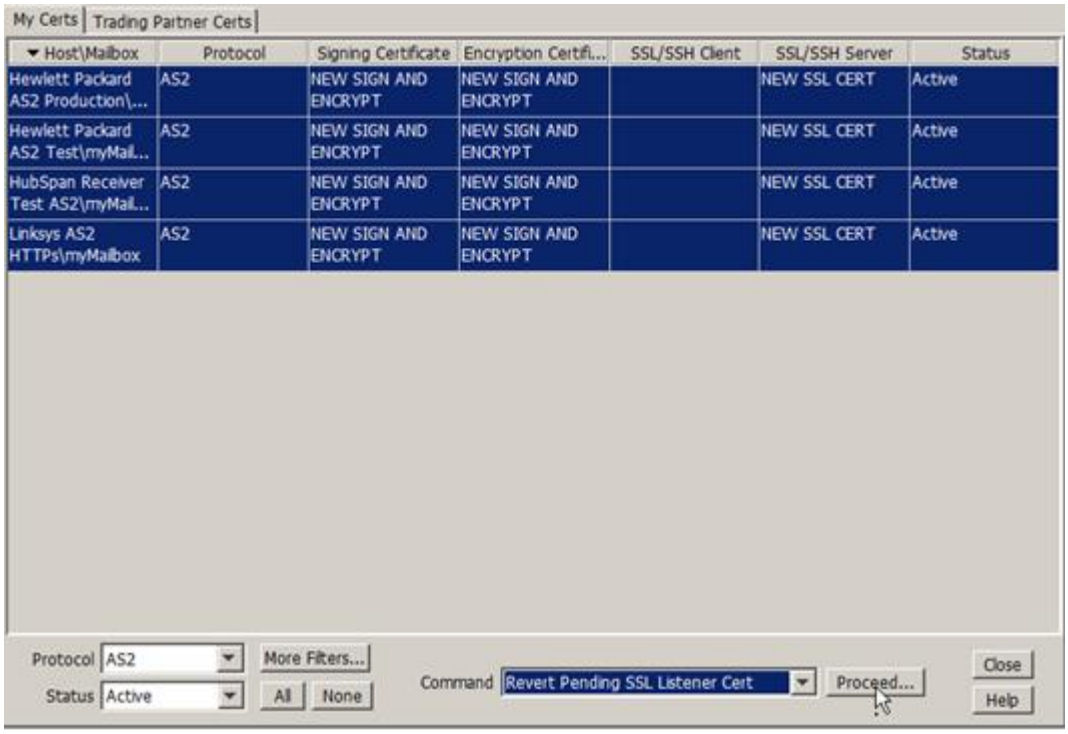
If the server certificate was incorrectly scheduled and currently is in a read-only state, it may be reverted by performing the following steps

1. Use **More Filters…** to quickly isolate all records using the pending server certificate and click **OK**:

2. Select those records and then choose **Revert Pending SSL Listener Cert**.

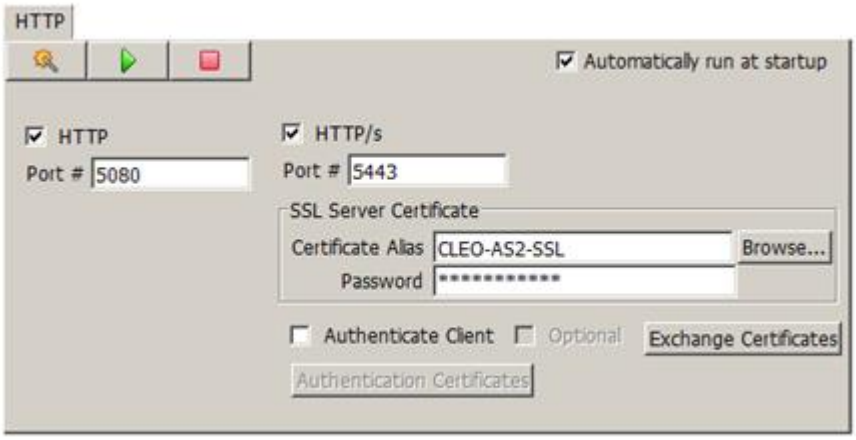


3. Click **Proceed…**



The following confirmation dialog will be displayed:

The HTTP/s panel certificate is now reverted back to its original state:



Allowing overlapping signing/encryption keys

When you have a local PGP partner packaging signing/encryption key scheduled for future use (using the **Certificate Exchange** dialog box via the **My Certs** tab), there might be a period of time where the new key has been scheduled but not yet activated. To prevent a situation where decryption of an inbound file fails using the installed key during this "overlap" period, you can configure your system to attempt decryption using the scheduled but not-yet-active key. Additionally, during this overlap period, outbound files are signed using both the installed and scheduled keys to avoid possible signature verification errors by the trading partner. By default, the **Allow Overlapping Key Usage** option is selected.

Handling expired certificates

Certificates created through the Cleo Harmony application have a default validity period of 24 months. This validity period can range from 1 to 96 months and can be lengthened or shortened as necessary when creating a new certificate. After that time, your certificate is no longer considered valid and you should generate a new certificate and distribute it to all your trading partners.

Beginning 30 days prior to a certificate's expiration date, the Cleo Harmony application logs warning notifications in its message log when any certificates used by the application (that is, either your user certificates or your trading partners' certificates) are about to expire or have already expired.

You can also set the **Email Local Certificate Expiration Notices** property in the **Local Listener: Advanced** tab to receive daily email notifications when any of your user certificates is within 30 days of expiration or have already expired. See Specifying Local Listener advanced properties on page 759. Otherwise, if the **Email Local Certificate Expiration Notices** property is not set and you have System Event logging configured for both errors and warnings (applies to the Cleo Harmony and Cleo VLTrader applications only), the daily certificate expiration notifications are logged in the System Event log/file instead. If the **Email Local Certificate Expiration Notices** property is not configured and System Event logging is not defined, a warning message is logged in the Cleo Harmony message log if it detects any local or partner certificates have expired or are about to expire. See Logs on page 892.

Although a 30-day warning should afford you ample time to either generate a new certificate and distribute it to all your trading partners or request and obtain a new certificate from your trading partner, you may change this default setting by changing the **Email Local And Partner Certificate Expiration Warning Days** property in the **Local Listener: Advanced Tab**. See Specifying Local Listener advanced properties on page 759.

Use the **View** button to review certificate expiration dates. See Viewing user and CA certificate usage on page 672.

User management

User Management allows you to configure and control settings that impact the users of your Cleo Harmony server. In this section, learn how to use the LDAP server to authenticate users and designate hosts, and configure your Cleo Harmony and Cleo VLTrader applications to support SAML to implement SSO and SLO for your users.

Users

The **Users** tree branch contains information about all configured user groups. Cleo VLNavigator supports authenticating users using its own database or using a directory service via LDAP. A non-LDAP user with administrative privileges, such as the default administrator user, should be defined in case the LDAP server is not functional.

Note: If you have an Administrator user configured in Cleo VLNavigator and a Users host user configured in Cleo Harmony or Cleo VLTrader with the same username, you might experience issues logging in to your system with the Adminstrator user. To resolve possible issues, you can rename or remove the Users host user or change the configuration of the Users host user to use VLNav Connector Host authentication.

Configuring the Cleo VLNavigator LDAP server

Use the **LDAP Server** tab in Cleo VLNavigator to configure the LDAP server to authenticate internal administrators and operators of the Cleo VLNavigator and Cleo Harmony applications.

1. In Cleo VLNavigator, click the **Users** node in the tree view.

   The **LDAP Server** tab appears.
2. Select the **Enabled** check box to enable the fields on the tab.

   If the LDAP server is disabled (the **Enabled** check box is cleared), any LDAP users and the Default LDAP group, if it exists, are displayed in yellow to indicate the LDAP server is currently disabled and, therefore, all LDAP accounts are currently not usable.
3. Specify values for the fields in the **Server Configuration** section.

   See Cleo VLNavigator LDAP server configuration reference on page 687.
4. Specify values for the fields in the **Domain Configuration** section.
   a) Add servers to the list of active LDAP servers. Either retrieve LDAP service records or add them manually.
      - To retrieve LDAP service records, select the **Lookup** check box, specify a value in the **Domain** field, and click **Refresh**. LDAP service records found in the domain you specify are displayed in a table.
      - To add LDAP service records manually, clear the **Lookup** check box, and click the **New** button to display a dialog box in which you can enter information for a new record. When you are finished entering the information, click **OK** to dismiss the dialog box and display the new record in the table.

        Click **New** to add more new records as necessary.

        While the **Lookup** check box is cleared, you can right-click service records to edit them or remove them from the list.

   b) Specify values for **Base DN**, **Search Filter** and **Username Attribute**.

      See Cleo VLNavigator LDAP domain configuration reference on page 687 for information about the fields in the **Domain Configuration** section.
   c) Optional. Click **Advanced** to specify password expiration settings. The **Advanced** button is enabled only when you select `Active Directory` from the **Directory Type** menu. See Cleo VLNavigator LDAP server configuration reference on page 687.

d) Click **Test** to test changes before they are applied. Enter an LDAP username and password. Changes to the **Server Configuration** panel are not applied until after a successful test login to the LDAP server.

5. Specify values for the fields in the **User Configuration** section.

   See Cleo VLNavigator LDAP user configuration reference on page 690.

Cleo VLNavigator LDAP server configuration reference

Enabled

Select the check box to enable LDAP connections to the configured server. Clear the check box to disable LDAP connections. When this check box is cleared, LDAP users are not able to log in.

Directory Type

The product used for the external LDAP directory service.

Possible values:

```
Active Directory
Apache Directory Services
Lotus Domino(IBM)
Novell eDirectory
DirX(Siemens)
```

Security Mode

If the directory server requires use SSL, specify a security mode. Otherwise, select `None`.

Possible values:

`None` - Information retrieved from the directory server will be clear-text.

`SSL` - Select when your servers support only SSL connections.

`StartTLS` - Select when your servers support SSL by use of the `StartTLS` command.

Cleo VLNavigator LDAP domain configuration reference

Lookup

Select the check box to use the value in the **Domain** field for retrieving SRV (Service) records for the LDAP service cluster.

Clear the check box to add records to the table manually.

Domain

The name of the domain from which you want to retrieve SRV records.

Click **Refresh** to refresh the information in the table using the value in the **Domain** field.

SRV record table

The SRV record table displays information about SRV records. Each row in the table represents one SRV record. Each row contains the following columns:

Enabled

Select this check box to use the record. Otherwise, the record is ignored.

Hostname

The target machine on which the LDAP service is running.

Port

The port used to connect to the LDAP service. Typically, the port `389` is used for non-secure (`None`) or StartTLS mode and `636` is used for SSL mode.

TTL

The `Time To Live` value defined as the time interval (in seconds) that the LDAP service record can be cached before the source of the information (for example, the domain) should again be consulted. A value of zero means that the LDAP record can only be used for the transaction in progress, and should not be cached. You can also use a value of zero for extremely volatile data.

Priority

The priority of the LDAP server. Attempts are made to contact LDAP servers with the lowest-numbered priority first. LDAP servers with the same priority are contacted in the order specified by the Weight field.

Possible values: `0-65535`

Weight

A server selection mechanism that specifies a relative weight for entries with the same priority. Larger weights are given a proportionately higher probability of being selected. Use a zero value when server selection is not required.

When there are records with weight values greater than zero, records weighted with a zero value will have a very small chance of being selected. When all priority and weight values are the same, the LDAP servers are selected in random order.

Possible values: `0-65535`

Base DN

The base organizational unit where the users are defined. Contact your directory administrator for the correct Base DN value. (The Base DN value entered here can be overridden in a local user host LDAP mailbox.)

The examples the table below show sample base organizational units for the supported directory types.

Directory Type	Example Base DN
Active Directory	`OU=Employees,DC=company,DC=com`
Apache Directory Services	`OU=Users,DC=example,DC=com`
Lotus Domino	`O=SCNotes`
Novell eDirectory	`O=Company Organization`
DirX	`ou=Users,o=Company`

Search filter

Optional. Used to limit the amount of information returned from the LDAP server when many users are defined. A more restrictive filter can be specified as a comma separated list. If necessary, contact your directory administrator to determine the appropriate attributes and values. You can override the value entered here in a local user host LDAP mailbox.

The following table contains example lists with sample attribute names and values.

Search Filter	Description
`department=EDI`	Limits the search to entries that have the attribute, `department`, with a value of `EDI`.
`department=EDI,group=administrators`	Limits the search to entries that must match two attributes. The user must be in the `EDI` department and in the `administrators` group.

Search Filter	Description
`department=EDI,telephoneNumber=800*`	Limits search to EDI department members with a telephone number starting with `800`.
`objectclass=person`	Limit the search to entries that are people if the Base DN contains other entries (for example, computers) and people.
`!(userAccountControl:1.2.840.113556.1.4.803:=2)`	Excludes disabled accounts - in Active Directory, if an account is disabled, bit `0x02` in the `userAccountControl` attribute value is on. `1.2.840.113556.1.4.803` is the rule object ID (ruleOID) for the LDAP bitwise `AND` operator.

If the value to search in has any of the following special characters, they must be substituted in the Search Filter with the corresponding escape sequence.

ASCII character	Escape Sequence Substitute
*	\2a
(	\28
)	\29
,	\2c
\	\5c
NUL	\00
/	\2f

Username Attribute

The **Username Attribute** is the directory attribute that matches the username entered when a login is required. The following table contains typical attribute names for the supported directory types.

Directory Type	Username Attribute
Active Directory	`sAMAccountName`
Apache Directory Services	`Uid`
Lotus Domino	`CN`
Novell eDirectory	`CN`
DirX	`cn`

LDAP Server Advanced Settings

The **LDAP Server Advanced Settings** dialog box displays when you click **Advanced** on the **LDAP Server** tab. Use this dialog box to specify values for password expiration checking.

Enable Password Expiration Checking

Select this check box to enable password expiration checking and the rest of the fields in the dialog box. Password expiration checking provides a daily email notification to the system administrator.

Warning Days Before Password Expiration

The range of days within which a notification is generated.

Daily Time Check

The time of day password expiration is checked.

To

The email address of the recipient of the daily password expiration check notification. You can specify multiple recipients. Separate email addresses by commas (,), semi-colons(;) or colons(:).

One or more individual users can also receive an email notification, if specified, when the **Security Mode** is not set to `None` and an email address is configured for the users (as part of his Active Directory settings). A Web Portal user whose password hasn't already expired is directed to the web link (see Providing access to the web portal on page 793) where they can change their password. Otherwise, they are directed to contact the system administrator for assistance in changing it.

Default value: The System Administrator email address defined in the **Options > Other** panel in the native UI or **Administration > System > Other** in the web UI.

From

The email address of the sender of the daily password expiration check notification. If this field contains multiple email addresses, only the first address is displayed.

Default value: The System Administrator email address defined in the **Options > Other** panel in the native UI or **Administration > System > Other** in the web UI.

Subject

String that appears in the Subject field of the daily password expiration check notification.

Cleo VLNavigator LDAP user configuration reference

Email Address Attribute

Required field. Attribute name for a user's email address.

Note: If you do not specify the **Email Address** attribute and you have LDAP users who try to reset a password via email, the Cleo Harmony application will not send password-reset emails.

Phone Attribute

First Name Attribute

Last Name Attribute

Full Name Attribute

Optional fields. Other options might depend on the values you specify for these fields.

User UID Attribute

Required field.

An additional distinguishing attribute in the user list.

LDAP Account for Extracting Users

Username

Password

Credentials used to login to extract LDAP user from the LDAP directory service to populate the optional default LDAP user group or when you browse for users on the **Cleo VLNavigator User** tab. In addition to

the **List** button here and in each of the local user host mailbox LDAP tabs, this account is used to periodically extract users in order to check mailbox license limits and to create user subdirectories.

Create/Maintain Default LDAP Group

Select the check box to create the optional Default LDAP user group. Clear the check box to remove the Default LDAP user group. See Default LDAP group on page 691.

Default LDAP group

On the LDAP Server tab (see Users LDAP Server), when an LDAP directory service is configured, the optional **Username** and **Password** fields are specified, **Create/Maintain Default LDAP Group** is selected, and **Apply** is clicked, a special user group called **Default LDAP** will appear under the **Users** tree. The **Default LDAP** group is a convenience group, provided as an easy way to add many users at one time. The users within this group will correspond to those shown when **List** is clicked (not including any users that already exist within other VLNavigator user groups).

Once created, the Default LDAP group can be disabled, refreshed, or removed by right-clicking the user group within the tree pane and selecting **Disable**, **Refresh**, or **Remove**. If **Remove** is selected, **Create/Maintain Default LDAP Group** cleared for you and the group is removed. Another way to remove the **Default LDAP** group is to clear **Create/Maintain Default LDAP Group** and click **Apply**.

The users within the **Default LDAP** group cannot be edited or disabled; however, they can be moved to another user group by right-clicking on the user within the tree pane and selecting **Move**.

LDAP server

Note: This feature is being deprecated. For similar functionality, use an LDAP host, which is a type of Connector host. See Connector Host on page 534 for more information.

Note: This section applies to the Cleo VLTrader and Cleo Harmony applications only.

Use the **LDAP Server** tab to configure the external LDAP directory service to be used for authenticating users. The LDAP service cluster can be obtained by specifying a single domain where the LDAP servers are located, or through manually configuring an LDAP service cluster that resides on a single domain. In either case, hosts can optionally be designated as primary servers and others as backups. If you are unsure of any of the required values, contact your directory administrator. LDAP user groups can then subsequently be configured as mailboxes in each of the local user hosts – FTP, HTTP, SSH FTP, and Users.

1. Open the LDAP tab.

   In the web UI, go to **Administration** > **User Management** > **LDAP Settings**.

   In the native UI, go to **Configure** > **Options** > **LDAP Server**.
2. Select the **Enabled** check box to enable the fields on the tab.
3. Specify values for the fields in the **Server Configuration** section.

   See Server configuration reference on page 692.
4. Specify values for the fields in the **Domain Configuration** section.
   a) Add servers to the list of active LDAP servers. Either retrieve LDAP service records or add them manually.

   - To retrieve LDAP service records, select the **Lookup** check box, specify a value in the **Domain** field, and click **Refresh**. LDAP service records found in the domain you specify are displayed in a table.
   - To add LDAP service records manually, clear the **Lookup** check box, and click the **New** button to display a dialog box in which you can enter information for a new record. When you are finished entering the information, click **OK** to dismiss the dialog box and display the new record in the table.

     Click **New** to add more new records as necessary.

While **Lookup** check box is cleared, you can right-click service records to edit them or remove them from the list.

b) Specify values for **Base DN**, **Search Filter** and **Username Attribute**.

See Domain configuration reference on page 692 for information about the fields in the **Domain Configuration** section.

c) Optional. Click **Advanced** to specify password expiration settings. The **Advanced** button is enabled only when you select `Active Directory` from the **Directory Type** menu. See Server configuration reference on page 692.

d) Click **Test** to test changes before they are applied. Enter an LDAP username and password. Changes to the **Server Configuration** panel are not applied until after a successful test login to the LDAP server.

5. Specify values for the fields in the **User Configuration** section.

See User configuration reference on page 695.

Server configuration reference

Enabled

Select the check box to enable LDAP connections to the configured server. Clear the check box to disable LDAP connections. When this check box is cleared, LDAP users are not able to log in.

Directory Type

The product used for the external LDAP directory service.

Possible values:

```
Active Directory
Apache Directory Services
Lotus Domino(IBM)
Novell eDirectory
DirX(Siemens)
```

Security Mode

If the directory server requires use SSL, specify a security mode. Otherwise, select `None`.

Possible values:

`None` - Information retrieved from the directory server will be clear-text.

`SSL` - Select when your servers support only SSL connections.

`StartTLS` - Select when your servers support SSL by use of the `StartTLS` command.

Domain configuration reference

Lookup

Select the check box to use the value in the **Domain** field for retrieving SRV (Service) records for the LDAP service cluster.

Clear the check box to add records to the table manually.

Domain

The name of the domain from which you want to retrieve SRV records.

Click **Refresh** to refresh the information in the table using the value in the **Domain** field.

SRV record table

The SRV record table displays information about SRV records. Each row in the table represents one SRV record. Each row contains the following columns:

Enabled

Select this check box to use the record. Otherwise, the record is ignored.

Hostname

The target machine on which the LDAP service is running.

Port

The port used to connect to the LDAP service. Typically, the port `389` is used for non-secure (`None`) or StartTLS mode and `636` is used for SSL mode.

TTL

The `Time To Live` value defined as the time interval (in seconds) that the LDAP service record can be cached before the source of the information (for example, the domain) should again be consulted. A value of zero means that the LDAP record can only be used for the transaction in progress, and should not be cached. You can also use a value of zero for extremely volatile data.

Priority

The priority of the LDAP server. Attempts are made to contact LDAP servers with the lowest-numbered priority first. LDAP servers with the same priority are contacted in the order specified by the Weight field.

Possible values: `0-65535`

Weight

A server selection mechanism that specifies a relative weight for entries with the same priority. Larger weights are given a proportionately higher probability of being selected. Use a zero value when server selection is not required.

When there are records with weight values greater than zero, records weighted with a zero value will have a very small chance of being selected. When all priority and weight values are the same, the LDAP servers are selected in random order.

Possible values: `0-65535`

Base DN

The base organizational unit where the users are defined. Contact your directory administrator for the correct Base DN value. (The Base DN value entered here can be overridden in a local user host LDAP mailbox.)

The examples the table below show sample base organizational units for the supported directory types.

Directory Type	Example Base DN
Active Directory	`OU=Employees,DC=company,DC=com`
Apache Directory Services	`OU=Users,DC=example,DC=com`
Lotus Domino	`O=SCNotes`
Novell eDirectory	`O=Company Organization`
DirX	`ou=Users,o=Company`

Search filter

Optional. Used to limit the amount of information returned from the LDAP server when many users are defined. A more restrictive filter can be specified as a comma separated list. If necessary, contact your directory administrator to determine the appropriate attributes and values. You can override the value entered here in a local user host LDAP mailbox.

The following table contains example lists with sample attribute names and values.

Search Filter	Description
`department=EDI`	Limits the search to entries that have the attribute, `department`, with a value of `EDI`.
`department=EDI,group=administrators`	Limits the search to entries that must match two attributes. The user must be in the `EDI` department and in the `administrators` group.
`department=EDI,telephoneNumber=800*`	Limits search to EDI department members with a telephone number starting with `800`.
`objectclass=person`	Limit the search to entries that are people if the Base DN contains other entries (for example, computers) and people.
`!(userAccountControl:1.2.840.113556.1.4.803:=2)`	Excludes disabled accounts - in Active Directory, if an account is disabled, bit `0x02` in the `userAccountControl` attribute value is on. `1.2.840.113556.1.4.803` is the rule object ID (ruleOID) for the LDAP bitwise `AND` operator.

If the value to search in has any of the following special characters, they must be substituted in the Search Filter with the corresponding escape sequence.

ASCII character	Escape Sequence Substitute
*	\2a
(	\28
)	\29
,	\2c
\	\5c
NUL	\00
/	\2f

Username Attribute

The **Username Attribute** is the directory attribute that matches the username entered when a login is required. The following table contains typical attribute names for the supported directory types.

Directory Type	Username Attribute
Active Directory	`sAMAccountName`

Directory Type	Username Attribute
Apache Directory Services	`Uid`
Lotus Domino	`CN`
Novell eDirectory	`CN`
DirX	`cn`

LDAP Server Advanced Settings

The **LDAP Server Advanced Settings** dialog box displays when you click **Advanced** on the **LDAP Server** tab. Use this dialog box to specify values for password expiration checking.

Password Expiration Checking

Enable Password Expiration Checking

Select this check box to enable password expiration checking and the rest of the fields in the dialog box. Password expiration checking provides a daily email notification to the system administrator.

Warning Days Before Password Expiration

The range of days within which a notification is generated.

Daily Time Check

The time of day password expiration is checked.

To

The email address of the recipient of the daily password expiration check notification. You can specify multiple recipients. Separate email addresses by commas (,), semi-colons(;) or colons(:).

One or more individual users can also receive an email notification, if specified, when the **Security Mode** is not set to `None` and an email address is configured for the users (as part of his Active Directory settings). A Web Portal user whose password hasn't already expired is directed to the web link (see Providing access to the web portal on page 793) where they can change their password. Otherwise, they are directed to contact the system administrator for assistance in changing it.

Default value: The System Administrator email address defined in the **Options > Other** panel in the native UI or **Administration > System > Other** in the web UI.

From

The email address of the sender of the daily password expiration check notification. If this field contains multiple email addresses, only the first address is displayed.

Default value: The System Administrator email address defined in the **Options > Other** panel in the native UI or **Administration > System > Other** in the web UI.

Subject

String that appears in the Subject field of the daily password expiration check notification.

Follow Referrals

Only applicable when connecting to Active Directory servers. Specifies whether referrals returned by the LDAP server are followed. When enabled, the system automatically follows a referral to another LDAP server to continue authentication or user lookup. When disabled, referrals are ignored, which might cause authentication or user lookup to fail if the requested information is not available on the initial LDAP server.

User configuration reference

Email Address Attribute

Full Name Attribute

Home Directory Attribute

Optional fields. Other options might depend on the values you specify for these fields. For example, if the LDAP server provides user home directory paths in addition to authentication, the **Home Directory** attribute is required.

Note: If you do not specify the **Email Address** attribute and you have LDAP users who try to reset a password via email, the Cleo Harmony application will not send password-reset emails.

User UID Attribute

Required field for user ID lookup.

If you are using SAML, this LDAP attribute value must match the SAML assertion `NameId` value passed by the IDP in order for a user to successfully login through SAML.

You should not use the **Email Address Attribute** as the **User UID Attribute**, as an email address for an individual can change.

LDAP Account for Extracting Users

Username

Password

Credentials to use to login to extract LDAP user from the LDAP directory service to populate the optional default LDAP user group or when you browse for users on the **Cleo VLNavigator User** tab. In addition to the **List** button here and in each of the local user host mailbox LDAP tabs, this account is used to periodically extract users in order to check mailbox license limits and to create user subdirectories.

SAML configuration

Note: SAML is a licensed capability available in Cleo Harmony.

You can configure the Cleo Harmony application to support Security Assertion Markup Language (SAML) to implement Single Sign On (SSO) and Single Logout (SLO) for Cleo Portal users or for Cleo Administration through the WebUI.

You provide information about the Service Provider (SP) and the Identify Provider (IDP), where the Cleo system acts as an SP. When the user attempts to sign in, the SP requests an identity assertion from the IDP and, based on that assertion, allows or denies the user access to the service requested. One IDP can provide SAML assertions to many SPs.

Note: Cleo Harmony requires signed assertions for authenticating users through SAML. Configure your IDP to send back signed assertions while using Cleo Harmony as Service Provider.

Configuring SAML

Provide information about the Service Provider and the Identity Provider.

Important: Before you enable SAML for Cleo Portal users, make sure you have imported your IDP settings and your IDP has your SP settings.

1. In the web UI, go to **Administration** > **User Management** > **SAML**. In the native UI, go to **Options** > **SAML**.
2. On the **Service Provider (SP)** tab, provide information about your system and, optionally, export SP information to a file you can share with your IDP. See Configuring and exporting SAML service provider information on page 697 and SAML service provider reference on page 698.
3. On the **Identity Provider (IDP)** tab, import information about your IDP.

See Importing SAML identity provider information on page 697 and SAML identity provider reference on page 700.

Once imported, you can view the raw IDP XML file. See Viewing an imported IDP file on page 697.

Configuring and exporting SAML service provider information

When you configure Service Provider information, you can export it to a file you can share with or import to your IDP.

1. In the web UI, go to **Administration > User Management > SAML**. In the native UI, go to **Options > SAML**.
2. Click the **Service Provider (SP)** tab.
3. If necessary, enter information about your SP.

   Note: You should not enable SAML for Cleo Portal users until you have imported your IDP settings and your IDP has imported your SP settings.

   See SAML service provider reference on page 698.
4. Save your updates.

   In the web UI, click **Save**.

   In the native UI, click **OK**.
5. (Optional) Click **Export**.

   In the web UI, updates to the SP information are saved when you click **Export**.

   In the native UI, clicking **Export** does not save any changes. You must click **OK** to save the SP information.

   For more information about service provider information, see SAML service provider reference on page 698.

Importing SAML identity provider information

You can import SAML configuration information from your IDP to your Cleo Harmony system.

1. In the web UI, go to **Administration > User Management > SAML**. In the native UI, go to **Options > SAML**.
2. Click the **Identity Provider (IDP)** tab.
3. Click **Import** to display the **Import IDP Settings** dialog box.
4. Specify or navigate to your IDP settings file, and then click **Import**.

   The imported IDP information populates the **Identity Provider (IDP)** tab. See SAML identity provider reference on page 700.

   In the web UI, updated IDP information is saved when you click **Import**.

   In the native UI, you must click **OK** to save the updated IDP information. In the native UI, clicking **OK** to save your IDP data also dismisses the **Options** dialog box.

   Once you have imported an IDP XML file, you can view the file's raw content. See Viewing an imported IDP file on page 697.

Viewing an imported IDP file

You can view the raw contents of an IDP file you imported into your Cleo Harmony system.

1. In the web UI, go to **Administration > User Management > SAML**. In the native UI, go to **Options > SAML**.
2. Click the **Identity Provider (IDP)** tab.
3. Click **View IDP file**.

   The IDP file is displayed in you default XML editor.

SAML service provider reference

Provide information about the Service Provider (SP).

Enable SAML for all Cleo Portal users

Select this check box to authenticate all Cleo Portal users via IDP using the SAML protocol. If you select only this option, your SAML login page is displayed when users invoke Cleo Portal.

Important: Before you select this check box, make sure you have imported your IDP information and your IDP has your SP information.

Enable SAML for Default/Native Users

Selecet this check box to allow users created in Cleo Harmony to log in using SAML.

Allow non-SAML login for Cleo Portal Users

Select this check box to allow Cleo Portal users to login using their local credentials. If you select only this option, the Cleo Portal login page is displayed when users invoke Cleo Portal.

Note: Selecting both **Enable SAML for all Cleo Portal users** and **Allow non-SAML login for Cleo Portal Users** enables *mixed mode authentication*, where Cleo Portal users can log in with either SAML or local credentials. The Cleo Portal log in page displays the **Use Company Login** check box. Clicking **Log In** with this check box enabled redirects the user to the SAML log in page. Otherwise, users can log in using local login credentials.

Enable SAML for WebAdmin

Select this check box to authenticate all Cleo WebAdmin users via IDP using the SAML protocol. If you select only this option, your SAML login page is displayed when users invoke the Cleo WebAdmin. The SAML assertion will be matched using the users configured in **User Management > Admin Users**. After this option is enabled users in the 'Administrators' group will still be able to log in by unchecking the **Use Company Login** checkbox. VLNavigator resource option is disabled in **Local Listener > Web Browser** after this option is enabled. All Admin User administration should be done through the Cleo WebAdmin.

Note: You cannot use **Enable SAML for all Cleo Portal users** and **Enable SAML for WebAdmin** at the same time. They can only be used one at a time.

Entity ID

Specify the value to be used as the `Issuer` in the `Authn` request. This value must be unique and it should conform to the URI pattern.

This value is used to publicly identify your deployment throughout your configuration and all of the other deployments that it interoperates with. This means that updating this value could affect many different systems and could take a long time to propagate. It is recommended that you *not* use a physical hostname, as such a value could change if you update your physical configuration. Instead, consider using a value that describes the service itself, as such a value could remain intact even through changes in physical configuration. One recommendation is to use your Assertion Consumer Service Endpoint value, as long as the domain is fully qualified.

Assertion Consumer Service Endpoint (HTTP-POST)

The URL to which the IDP posts assertions to your Cleo Harmony system.

`http://<domain>:<port>/<portal-resource>`

The value you should use for <*portal-resource*> is the same one you configure for the Local Listener Web Browser Service. See Local Listener Web Browser Service on page 781.

Single Logout Service Endpoint (HTTP – Redirect)

The URL from which the IDP sends logout requests to your Cleo Harmony system.

`http://<domain>:port</signout>`

This field is populated automatically based on the value provided in the **Assertion Consumer Service Endpoint** field and is read-only.

Enable Single Logout

Select this check box to enable single logout processing and populate the **Single Logout Service Endpoint (HTTP – Redirect)** field.

Signing & Encryption

Provide information to support signing authentication requests and encrypting assertions.

Sign Authentication Requests

Select the check box to enable fields where you specify a certificate and password to cause `Authn Requests` sent to the IDP to be signed.

Signing Certificate

Password

Algorithm

Alias, password and algorithm for the certificate to use to sign authentication requests. You can specify a certificate or browse for and select one.

`SHA-1` and `SHA-256` algorithms are supported.

Encryption Assertion

Encryption Certificate

Password

Optional - Certificate alias and password the IDP will use for encryption. You can specify a certificate or browse for and select one.

Select **Use same as Signing Certificate** to use the signing certificate for encryption.

Sign MetaData

Enables the fields where you select a certificate to use to sign SP metadata XML files generated during export.

Metadata Signing Certificate

Password

Certificate alias and password to use for signing SP metadata XML files generated during export. You can specify a certificate or browse for and select one.

Select **Use same as Signing Certificate** to use the signing certificate to sign metadata.

Organization and Contacts

Name

Display Name

Website

Information about the SP organization.

Technical - Name and Email

Support - Name and Email

Information about people at the SP who are available to be contacted.

SAML identity provider reference

Information from an Identity Provider (IDP) file you import.

Entity ID

The unique ID for the IDP imported from the IDP metadata file.

Single Sign On Service

The binding supported by Cleo Harmony for single sign on. Only `HTTP-Redirect` is supported.

There might be other values in the metadata, but only `HTTP-Redirect` is displayed.

Single Logout Service

The binding supported by the Cleo Harmony application for log out. Only `HTTP-Redirect` is supported.

There might be other values in the metadata, but only `HTTP-Redirect` is displayed.

wantAuthnRequestsSigned

Indicates the IDP expects a signed Authorization Request.

Organization and Contacts

Organization

Name

Display Name

Website

Information about the IDP organization.

Contacts

Technical - Name and Email

Support - Name and Email

Information about people at the IDP who are available to be contacted.

See Importing SAML identity provider information on page 697 for information about how to import IDP information.

File system

The directories in the **File System** menu allow you to specify default **Host Directories** in the web UI. **File System** also allows you to enable read and write access from Windows and Unix shares using the **CIFS Directories** tab in the Web UI and the **Windows/Unix Folders** tab in the native UI. Configuration of these settings is described in the following sections.

Specifying default host directories

1. In the web UI, go to **Administration** > **File System** > **Directories**. In the native UI, select **Configure** > **Options** in the menu bar or click **Options** in the toolbar, and click the **General** tab.
2. Specify values for the fields on the page and then click **Save**.

   For information about fields and possible values, see Default host directory Reference on page 700.

Default host directory Reference

Default Connection Type

Indicates whether a dial-up connection is first needed before trying to access a host. The dial-up connection option is only available on Windows platforms.

Possible values:

- `Direct Internet Access or VPN` - Default value
- `Dial-Up Connection`

Default Phonebook Entry

Indicates the default phonebook entry to use for dial-up connections. Only available on Windows platforms.

Possible values: Existing Windows dial-up connections

Default value: No default value.

Dial-Up Timeout

Indicates how long to wait for a dial-up connection before timing out.

Possible values: `# of seconds`

Default value: `120`.

Inbox

Default directory for incoming files.

Possible values: Any local or shared directory.

Default value: `inbox\`

Outbox

Default directory for outgoing files.

Possible values: Any local or shared directory.

Default value: `outbox\`

Sentbox

If specified, default directory for retaining sent files. Files are a copy of the original source file; any file manipulations performed as part of the send are not reflected in the sentbox copies.

Possible values: Any local or shared directory.

Default value: No default value.

Receivedbox

If specified, default directory for retaining received files. Files are a copy of the final destination file; any file manipulations performed as part of the receive are reflected in the receivedbox copies.

Possible values: Any local or shared directory.

Default value: No default value.

Rejectbox

Directory for files rejected by a host system.

Possible values: Any local or shared directory.

Default value: `rejectbox\`

Custom Directory Variables

If specified, contains a list of custom directory macro variable definitions. See Using macro variables on page 59 for information about using custom directory variables.

Variables are defined as `%name%=value` pairs. Each pair must be separated by one of the following characters:

`,` (comma)

`;` (semi-colon)

`\r` (carriage return)

`\n` (new line - linefeed)

Variable values can reference any local or shared directory.

Possible values: `%name1%=value1, %name2%=value2 … %nameN%=valueN...`

Default value: No default value.

CIFS directories

Note: This feature is being deprecated. For similar functionality, use an SMB host, which is a type of Connector host. See Connector Host on page 534 for more information.

Note: This section applies to Cleo VLTrader and Cleo Harmony applications only.

Windows has a built in capability to access Windows (CIFS) and Unix (SMB) shares. This is accomplished through the use of UNC paths or mounting the drive as a drive letter. The account the Cleo VLTrader or Cleo Harmony application is running as must have the credentials to access the files on the share. If the Cleo VLTrader or Cleo Harmony application is running as a user that has permission to access the desired shared paths, then configuring this feature is not necessary.

Windows/Unix Folder Access enables the Cleo VLTrader or Cleo Harmony application to read and write directly from Windows (CIFS) and Unix (SMB) shares from any platform. It allows different user credentials to be used on different shares. Access to these shares can be through a user other than the user running VersaLex. This allows the Cleo VLTrader or Cleo Harmony application to be running as a Windows Service under a **Local System Account**. On Unix platforms, it allows the Cleo VLTrader or Cleo Harmony application to access shares without the use of Samba.

Important: When running on certain operating systems, the operating system assumes it is the only software talking to the server. It will send a VC (Virtual Circuit) number of zero to the server. Many servers, by default, will reset all other CIFS/SMB connections to the same computer including the Windows/Unix Folder connection for the Cleo VLTrader or Cleo Harmony application.

For Samba servers, `reset on zero vc = no` can be configured in the `smb.conf` file.

For some Windows servers, `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters\SmbDeviceEnabled` can be added to the registry and set to `0`. This same setting can also be used on the client computer. See http://support.microsoft.com/kb/301673 for details.

Configuring Windows/Unix folder access

Follow the instructions below to configure access to files on Windows/Unix (CIFS/SMB) shares.

1. In the web UI, go to **File System** > **CIFS Directories**. In the native UI, select **Configure** > **Windows/Unix Folders** from the menu bar.

   The **CIFS Directories** page is displayed in the web UI. The **Windows/Unix Folder Configuration** dialog box is displayed in the native UI.
2. Click **New**.

   The **Windows/Unix Inbound/Outbound Folder** dialog box appears.
3. Enter values for the fields as needed.

   Domain

   The name of the Domain for the user. If this is not a domain login, then leave this field empty.

   User ID

   Password

   The credentials the product will use to connect to the share.

UNC Paths

A list of UNC-type paths (`\\servername\sharedfolder`) that can be accessed through this option. Enter one UNC path per line. VersaLex will perform a case-insensitive match against these paths to determine whether it should use this feature to access the Windows/Unix folder. The paths entered in other places (such as **Inbox**, **Outbox**, **Sentbox**, **Receivedbox**) will be compared against this list. If the complete folder name listed in **UNC Paths** matches the beginning folder in the **Inbox** field (as an example), then the folder will be accessed using the entered domain, username, and password.

4. Optional. Click **Validate** to verify the paths can be accessed using the entered user information. This button will only check read access on the UNC paths entered.
5. Once all the information has been entered click **OK**.
6. Repeat steps 1 through 5 for each Domain/User pair needed.
7. The updated **Windows/Unix Folder Configuration** panel is displayed. Enter any necessary JCIFS properties in the **Custom JCIFS Properties** field (one per line). These properties are described at the following website: http://jcifs.samba.org/src/docs/api/overview-summary.html#scp . On Unix platforms, we have seen increased performance if the following properties are set:

   ```
   jcifs.resolveOrder=DNS
   ```

   ```
   jcifs.smb.client.dfs.disabled=true
   ```
8. In addition to the properties described on the web page, there are some additional ones defined by Cleo. These should only be configured at the direction of Cleo Technical Support. The following are the default values:

   ```
   jcifs.cleo.debugOn=false
   ```

   ```
   jcifs.cleo.max.semaphores=-1
   ```

   ```
   jcifs.cleo.startOSSmbAccess=false
   ```
9. The **List by** choices at the top of the panel chose the display format for the Domain/User ID/Folder list. The **Domain/UserID** choice will order the list by Domain/User ID. The **Folder** choice will order the list by Windows/Unix Inbound/Outbound Folder name.
10. Create links for the Inbound and Outbound Files.

    The next step is to enter the UNC paths into the fields where they are required. The following is a list of the locations where the Windows/Unix Folders (UNC paths) are NOT supported:

    - **Configure** > **Options** > **Other** > **Autorun Directory**
    - **Tools** > **Router** > **Autoroute Directory**
    - **View** > **File**
    - Selection of the folder using the **File Chooser** anywhere in the product

AS/400 Setup and installation

Note: This section applies to Cleo LexiCom users only.

Use the following to install and configure the Cleo LexiCom software to run natively on the AS/400. If you are installing on a Windows PC and mapping to the AS/400 through a networked drive, see AS/400 Network Access Setup on page 980.

AS/400 Overview

Unlike typical AS/400 installations performed natively using the optical drive on the AS/400, this installation process is done from your PC via a network share that has been mapped to a directory created on the AS/400's Integrated File System (IFS).

Note: The AS/400 is an older reference and is now referred to as the “iSeries”, “System i” or "IBM i". Throughout this document it will continue to be referred to generically as the “AS/400” however “iSeries”, “System i” or "IBM i" may be used interchangeably.

AS/400 Process map

The following is a checklist of tasks for you to perform to successfully install LexiCom for the AS/400 and begin exchanging messages with your trading partner. Following this checklist are the detailed steps required to accomplish each of the tasks below.

- ☐ Getting Started
- ☐ **Determine if your system meets the minimum hardware requirements**
- ☐ **Determine if your operating system meets the minimum software requirements**
- ☐ **Obtain and install any missing software products**
- ☐ **Obtain and install all required cumulative and group PTFs**
- ☐ **Install LexiCom** : Follow this step-by-step procedure to map a shared IFS drive and install LexiCom on the AS/400.
- ☐ **Configure and Test** : This section describes how to configure hosts for sending and receiving files via a LexiCom AS/400 server. It also gives information on configuring the LexiCom Scheduler for sending and receiving files.
- ☐ **Starting and Stopping the LexiCom Server** : This section describes the commands used to start and stop the LexiCom server on the AS/400.

AS/400 Getting Started

AS/400 System Requirements

Please Note: Cleo LexiCom 5.8.1 requires Java 8 and support IBM i7.3, IBM i7.4, and IBM i7.5.

Visit Cleo LexiCom 5.8.1 System Requirements for current system requirements.

Determining Your Currently Licensed AS/400 Products

To display an inventory of the software that is installed on your system, type the command: **DSPSFWRSC**

Verify that **Java SE 8 64-bit (Option 17, Feature 5117)** is installed on the AS/400. *If it is not present, it must be downloaded from the IBM web site and installed before proceeding any further.* Refer to http://www-01.ibm.com/support/docview.wss?uid=nas8N1020692 for further information.

To determine the Java Group PTF level on your system, type the following command:

For IBM i 7.3 V7R3:

```
WRKPTFGRP SF99727
```

For IBM i 7.4 V7R4:

```
WRKPTFGRP SF99737
```

For IBM i 7.5 V7R5:

```
WRKPTFGRP SF99957
```

Obtaining Program Temporary Fixes (PTFs) for Your AS/400

IBM recommends that you regularly apply updated PTFs to your system to maintain optimal system performance. To find information on downloading and ordering Program Temporary Fixes (PTFs), Group PTFs and a wealth of other information to help you manage your AS/400, visit the IBM Web site: https://www.ibm.com/support/pages/program-temporary-fix-download-and-installation

Installation and Operation Pre-requisites

Before you can successfully install and run LexiCom on the AS/400, you must verify that the following additional requirements are met:

1. TCP/IP must be properly configured on the AS/400 and connectivity between a client PC and the AS/400 must be established and working correctly.
2. The host and domain name must be correctly defined on the AS/400. To verify or configure the AS/400's host and domain name, type `GO CFGTCP` and choose option `12`. Enter your AS/400's values in the **Host name** and **Domain name** fields.
3. The DNS (Domain Name System) must be properly configured to successfully resolve host names. Without DNS configured properly, LexiCom will only be able to send messages to IP addresses. To configure DNS, type **GO CFGTCP**and choose option 12 and enter the IP address of your **Domain Name Server**.
4. Add a host table entry for the AS/400's IP address and host name by typing **GO CFGTCP**and choosing option 10 (Work with TCP/IP host table entries). You should also have a LOOPBACK entry that points to the LOCALHOST at 127.0.0.1.
5. The IBM i Net Server must be properly configured on the AS/400. Net Server allows support for Windows Network Neighborhood and allows you to map directories in the AS/400 file system to shared drives accessible through your Windows environment. If the NetServer has not already been started, the command **STRTCPSVR *NETSVR** should be entered to start this server.
6. Client Access Express for Windows (or its equivalent) and the latest Service Pack must be installed and configured on at least one PC in your Local Area Network. Once LexiCom is properly installed, any PC in the network (with the appropriate privileges and object authority) will be able to access the shared IFS drive and view the LexiCom UI.
7. The System i Navigator (or its equivalent) must be installed on at least one PC in your Local Area Network, and preferably on the PC where LexiCom will be installed. System i Navigator is only required for creating file shares (using IBM i Net Server) but is also useful for viewing System i functions with a graphical user interface. The examples in the following sections use System i Navigator for its illustrations; however you are under no obligation to use it if you prefer using comparable AS/400 native commands.
8. The QUTCOFFSET system value must be properly set for your time zone. This value is the offset from Greenwich Mean Time and is used to correctly display and log the local time of your AS/400. If not properly set, the times displayed in the LexiCom log will not reflect your current system time. To view this offset, type **DSPSYSVAL QUTCOFFSET**on the AS/400. If it is incorrect, verify the **QTIMZON** system value is set appropriately for your local time zone.

Obtaining Additional Information from IBM

Use the IBM i Support Portal as your starting point for looking up AS/400 technical information: https://www.ibm.com/support/home/

With your hardware order, you may have received digital media on a DVD labelled **System i Access for Windows** that contains the IBM i Access for Windows licensed program.

Use the Client Access Web site as a general source of information on Client Access: http://www-03.ibm.com/systems/power/software/i/access/windows/os.html

Use the IBM i Net Server web site for general information as well as links to installation and configuration information: http://www-01.ibm.com/support/docview.wss?uid=isg3T1026870

Installing Cleo LexiCom on AS/400

To install and run the AS/400 version of Cleo LexiCom software, a portion of the software will be installed using a Windows PC mapped to the Integrated File System (IFS) and then another portion will be installed in the AS/400 Native File System through command prompts. After all the requirements described in the previous section have been satisfied, use the following two sections to complete the installation to the Integrated and Native File Systems.

The following procedure should only be completed in its entirety the first time you install Cleo LexiCom. If you are upgrading to a new version of Cleo LexiCom software, first verify the product is not running on the AS/400 by either typing the `ENDLEXSVR` CL command at the command prompt or by selecting the **Stop AS/400** option from within the Cleo LexiCom software. Verify the `QJVACMDSRV` and `STRLEXSVR` processes are not running in the `QSYSWRK` subsystem by issuing a `WRKACTJOB` command at the command prompt.

Use the following links (replacing `SN=L#####-######` with your Cleo Serial Number) for New Installations or updating to the Latest patch.

- **LexiCom**. The file will be called `install.exe` and can be saved to the local file system. The link will be in the following form (all in one string):

  `http://download.cleo.com/download/LexiComDL.asp?OS=Windows(64-bit)&SN=L#####-######&PROD=LexiCom`
- **Latest patch.** The file will be called `#.zip` (where `#` is a number) and can be saved to the local filesystem. The link will be in the following form (all in one string):

  `http://download.cleo.com/download/LexiComDL.asp?SN=L#####-######&OS=Windows(64-bit)&PROD=LexiCom&PATCH=Y`
- **AS400 service module**. The file will be called `AS400.zip` and can be saved to the local file system. The link will be in the form of the following (all in one string): `http://download.cleo.com/download/LexiComDL.asp?SN=L#####-######&OS=Windows(64-bit)&PROD=LexiCom&EXTRA=AS400/AS400.zip`

If you are upgrading:

1. Export the LexiCom configuration via the UI for backup purposes.
2. Make sure LexiCom is not running. Do the following:
   a. Close the GUI.
   b. Issue `ENDLEXSVR` at the “green screen” command prompt.
   c. Make sure that LexiCom is NOT running as a Windows service and is NOT installed locally on Windows (on C: or other local drive).

Installing on an Integrated File System

This section will guide you through the procedure required to complete the **first-time installation** of Cleo LexiCom in the AS/400 Integrated File System. If you are upgrading 5.8.1.0 or later, use the local LexiCom install to upgrade and then skip to step 8.

1. **Create the IFS folder.**

   On a client PC within your Local Area Network that has the Client Access Express for Windows installed and running, use the System i Navigator to create a new folder named LexiCom under the AS/400's Root ('/ ') directory.

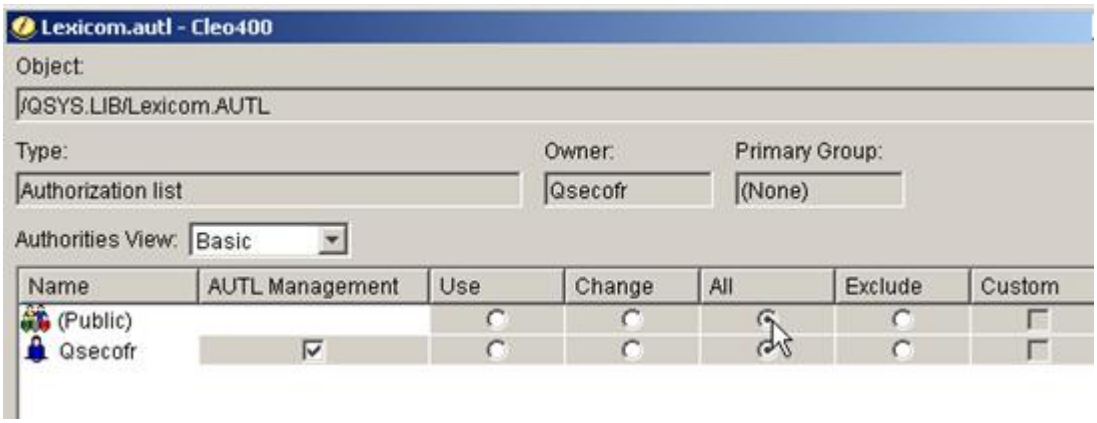
   Warning: You will not be able to run Cleo LexiCom software on the AS/400 if you name this folder anything other than LexiCom!

2. **Define the Authorization List for accessing the IFS Folder.**

   To allow multiple users to successfully run Cleo LexiCom and share access to all log and host files (even to those who did not originally create the files) without needing to give "All Object" access to any of these users, an Authorization List is used to assign Read, Write and Execute privilege to the /LexiCom folder and all of its subfolders. To do this, choose the Security icon in the System i Navigator, select Authorization Lists and choose New Authorization List.

   a. Create a LexiCom Authorization List and select All under Public authority.

   A screen similar to the following will be displayed. Verify that the All privilege is selected.



   b. Add the users who will be running Cleo LexiCom to the Authorization List and assign them the same All privilege.

   Note: The previous steps may also be performed using the CRTAUTL and ADDAUTLE (green screen) commands, if preferred.

   c. Next the /LexiCom folder and all its subfolders must be linked with the newly created Authorization List. Since the System i Navigator can only link the /LexiComfolder and none of its subfolders, it is necessary to open an AS/400 (iSeries/i) green screen as the owner of the /LexiCom folder or a user with either *ALLOBJ or *ALL access and enter the CHGAUT command as follows:

```
CHGAUT OBJ('/LexiCom')
                DTAAUT(*RWX) AUTL(LEXICOM) SUBTREE(*ALL)
```

   If desired, the System i Navigator may be used to verify that the Cleo LexiCom Authorization List has been properly assigned to the /LexiCom Object.

To do this, open the File Systems tree and expand the Integrated File System entry. Under the Root entry, right-click the /LexiCom folder and choosePermissions.

For additional information refer to the following IBM resources:

- Authorization lists concepts:

  https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_73/rzamv/rzamvauthlists.htm
- Authorization list security:

  https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_71/rzarl/rzarlauthsec.htm

3. **Create the Cleo LexiCom File Share.**

   Open IBM i Net Server and create a file share for the Cleo LexiCom folder that you created above. Make sure that the file share has Read/Write access.
4. **Map the File Share to a Network Drive.**

   Using Windows Explorer, map the new Cleo LexiCom file share to any available network drive.

   The contents of the shared IFS drive (which will be empty) should appear.

   Note: Due to IBM i compatibility issues, Cleo does not guarantee a desirable user experience while using Windows 10 mapped drives to display the LexiCom UI and therefore does not support mapping file shares on Windows 10 network drives.
5. **Installing the Integrated File System portion**

   a. Click on the **install.exe** file that you downloaded from the Cleo website.
   b. At the **Choose Install Folder** prompt, do not accept the default value of `C:\LexiCom`. You must either use the network drive (for example, `L:\`) or the network share (for example, \\cleo400\LexiCom) that you mapped in the previous step as the install target.
   c. At the **Where would you like to create product icons?** prompt, make sure to select **Don't create icons** and then click **Next**.
   d. At the **Install As A Service** prompt, make sure the **Start service automatically at system startup** checkbox is ***not*** selected and click **Next**.
   e. Review the **Pre-Installation Summary** window.
   f. Click the **Install** button.
   g. Click **Done** when installation is completed.
6. **Installing Cleo LexiCom on a local drive**

   a. Click on the same **install.exe** file again that you downloaded from the Cleo website.
   b. At the Choose Install Folder prompt, accept the default or some other location on the local drive(s).
   c. At the **Where would you like to create product icons?** prompt, this time do not select **Don't create icons** and then click **Next**.
   d. At the **Install As A Service** prompt, make sure the **Start service automatically at system startup** checkbox is again ***not*** selected and, even though the service won't be used, change the Service name to be different from the AS/400 install and then click **Next**.
   e. Review the **Pre-Installation Summary** window.
   f. Click the **Install** button.
   g. Click **Done** when installation is completed.
7. **Point the local LexiCom install at the AS/400 share install.**

   a. Start the local Cleo LexiCom (from either the Start menu or by double-clicking the LexiCom.exe application in the local install) from your PC.

b. Skip product registration at this point. To do this, click **Cancel** and then click **Continue** from the **Cleo LexiCom Product Registration** dialogs.

c. Now go to **Configure>Launcher**.

d. Starting with LexiCom v5.8.1, a **LexiCom AS/400 Install Share Directory** setting is available near the bottom of the **Cleo LexiCom Launcher Configuration** dialog box. Enter or select the AS/400 share install location. This can be either a mapped drive or a UNC path.

e. Click **Apply**, and then click **OK**.

f. Exit and restart the local Cleo LexiCom. On restart, the local Cleo LexiCom is pointed at the AS/400 share location.

Important: From this point on, only use the local LexiCom install to manage the product (i.e. licensing, configuration, operation, software updates, etc.). When applying a software update on the local install, it will also be applied on the AS/400 install at the same time. Even if you use the commandline LexiComc.exe, still use the local LexiCom's LexiComc.exe

8. **Installing the Native File System portion** - If this is the first time you have installed on the AS/400 or you are installing a release and not a patch, follow this procedure to complete the Cleo LexiCom NFS installation on the AS/400. If you are not installing a major release, you can skip this step.

a. Verify that the LexiCom.savf file has been copied (or unzipped from the AS400.zip file) to the /LexiCom folder in the IFS.

b. Sign on to the AS/400 Command Prompt as QSECOFR and type the following command:

```
CPYFRMSTMF FROMSTMF('/LexiCom/LEXICOM.savf')
                    TOMBR('/QSYS.LIB/QGPL.LIB/LEXICOM.file')
 CVTDTA(*NONE)
```

The message `Stream file copied to object` is displayed.

c. Restore all the objects required to complete the installation:

```
RSTOBJ OBJ(*ALL) SAVLIB(QGPL) DEV(*SAVF)
                    SAVF(QGPL/LEXICOM)
```

The message `7 objects restored from QGPL to QGPL` is displayed.

d. Type the following command to install all the necessary Cleo LexiCom commands and objects on the AS/400:

```
CALL INSTLEX
```

The message `LexiCom AS/400 Installation Complete` is displayed.

e. Save the downloaded jt400.jar file to the .../LexiCom/lib/ directory.

f. The installation is now complete. Run STRLEXSVR to begin operating Cleo LexiCom on the AS/400. To interact with the software, connect the Native UI to the service by running LexiCom.exe in the IFS installation path.

g. Verify the QJVACMDSRV and STRLEXSVR processes are running the QSYSWRK subsystem by issuing WRKACTJOB command on the AS/400 Command Prompt.

h. The AS/400 share portion of the install is done.

i. The reason for not creating icons during the AS/400 share install in the previous step is that using the AS/400 share to display the LexiCom application is not recommended and might not even be possible, depending on the networking between the Windows machine and the AS/400. Instead, starting with LexiCom v5.8.1, a second LexiCom can be installed locally and attached to the LexiCom installed on the AS/400 share. This local LexiCom can then be used to display the LexiCom application to manage the product.

9. **Register Cleo LexiCom**

Start the local Cleo LexiCom (from either the Start menu or by double-clicking the LexiCom.exe application in the local install) from your PC and register your serial number. See Registering your serial number on page 658.

Note: Once you have Cleo LexiCom installed into its final production destination, and before the end of your 30-day trial period, request your Permanent License. See Requesting a permanent license on page 657.

10. **If applicable, install the latest patch within the LexiCom application** (again using the local LexiCom install) by going to **Tools > Software Update > Update Options > Manual Patch File** Install. Navigate to the previously downloaded .zip file and follow the prompts to install. This will actually install the patch in both the local LexiCom install and the AS/400 share LexiCom install. If necessary, contact Cleo Support for assistance.

Configuring and testing on AS/400

Since the AS/400 does not have a graphical user interface and Cleo LexiCom is a graphical product, configuration of the hosts and the Local Listener is easily done using the Cleo LexiCom AS/400 UI. You will be configuring the hosts that are stored on the AS/400 IFS (in the /LexiCom folder) and therefore, you must invoke the *LexiCom* program icon linked to the shared drive that you mapped during the installation process.

The Cleo LexiCom AS/400 UI product is used to configure hosts and view status information in real-time. After you have started LexiCom on the AS/400, start the Cleo LexiCom application from the IFS mapped drive. After several seconds, Cleo LexiCom application will start and the UI will be displayed.

Once all your hosts and the Local Listener are configured to your satisfaction and optionally, the scheduler is correctly set up, you should verify that you can properly exchange messages with all your trading partners by sending and receiving test messages.

AS/400 Configure Content-Type Inboxing for the Native File System (AS2 only)

The **Add Content-Type Directory to Inbox** check box allows for sorting of incoming messages based on the content-type of the message to a subdirectory (under the *Inbox* specified on the General tab for the Host). You specify each of the content-types that you want directed to specified subdirectories by entering a name in the **Directory** field. Directory entries may be made for content-types of: EDIFACT, X12, XML, Binary, Plain Text, and Other (a default catch-all for messages with all other content-types you may receive.) The same subdirectory may be used for multiple content-types. You may also leave 'Directory' entries blank that will cause any received messages of that 'Content-Type' to be stored in the Inbox specified on the General tab.

Note: If you use this feature, incoming messages will be placed in the specified folder based on the content type specified in the HTTP header of the message. LexiCom does not check the actual content of the message to determine its content type.

Note: If you are integrated with a translator, you should not add entries for the X12 or EDIFACT directories. These directories must remain blank for translator integration to work properly.

By default, the Content-Type directories are preconfigured for windows or IFS based folders. To use this feature on the AS/400 Native File System, modifications must be made to all directories that will be used so that the settings have the correct AS/400 syntax, that is, each setting must be in the form `DIRECTORY.FILE`.

On the 'General' tab, specify just the library for the "Inbox" value where the "Content-Type" files will be created.

Now verify that all the "directories" that you have specified, i.e., files in the form DIRECTORY.FILE, have a matching physical file. In the example above, the files EDIFACT.FILE, X12.FILE and XML.FILE under the /

QSYS.LIB/LEXICOM.LIB library are being used. If these files don't already exist, create a physical file for each of the files you have specified as follows:

```
CRTPF FILE(LEXICOM/EDIFACT) RCDLEN(132) MAXMBRS(*NOMAX )    SIZE(*NOMAX)
```

```
CRTPF FILE(LEXICOM/X12) RCDLEN(132) MAXMBRS(*NOMAX ) SIZE(*NOMAX)
```

```
CRTPF FILE(LEXICOM/XML) RCDLEN(132) MAXMBRS(*NOMAX ) SIZE(*NOMAX)
```

As a final step, verify that the **Add Mailbox Alias Directory To Inbox** setting on the Advanced panel is not selected.

Configuring the Scheduler for the AS/400

Since the Cleo LexiCom AS/400 server does not have a UI to allow the user to manually send and receive files from trading partners, and typical AS/400 users will be integrating Cleo LexiCom software with an EDI translator, the Scheduler is a convenient way to invoke the <send> and <receive> actions that you have configured for your hosts.

See Scheduling actions - Native and Classic Web UI on page 611 for information.

Configuring for AS/400 Native or Integrated File System access

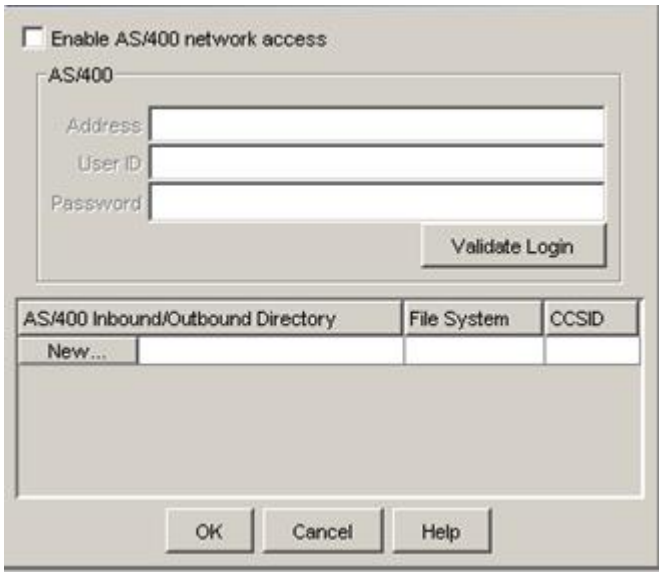
Cleo LexiCom provides a means for reading and writing from the AS/400 (QSYS.LIB) file system, which allows for seamless conversion of the data between EBCDIC and ASCII formats. Reading and writing into the Integrated File System where Cleo LexiCom software is installed may also be done, if desired.

Configuring directories for AS/400

Follow the instructions below to configure the Cleo LexiCom system to access files on the AS/400.

1. On the Cleo LexiCom menu bar, select **Configure** > **AS/400**.

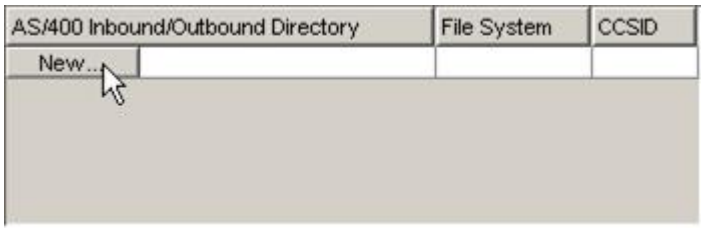
   The following panel will appear:



   If you will only be starting the Cleo LexiCom application interactively (from the AS/400 "green screen" command line), you will not need to enable AS/400 network access and the top portion of the panel may be left blank. This

portion of this panel is for running from a PC and accessing the AS/400 via the network. (See to AS/400 Network Access Setup on page 980 for additional information.)

2. Now click the **New…** button on this panel, as shown:

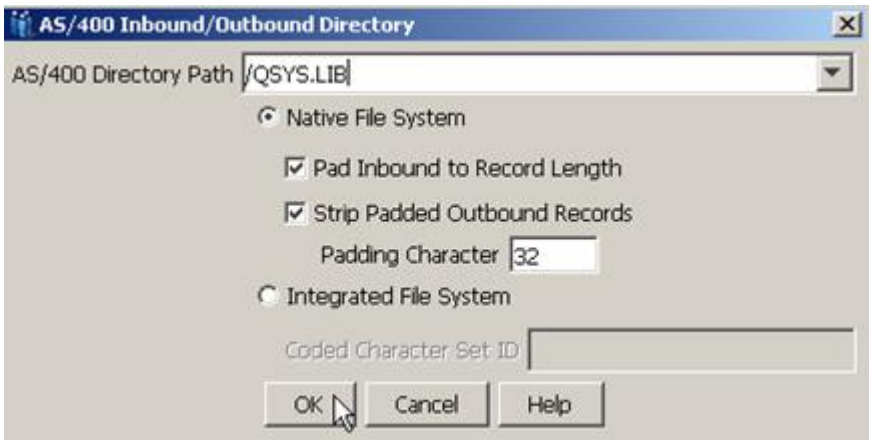


Selecting a file system type for AS/400

Follow the instructions below to tell the Cleo LexiCom application whether your files will be located on the AS/400 native file system (QSYS.LIB) or the integrated file system (IFS).

A display similar to the following will appear. Update the form as shown below:

For Native File Systems

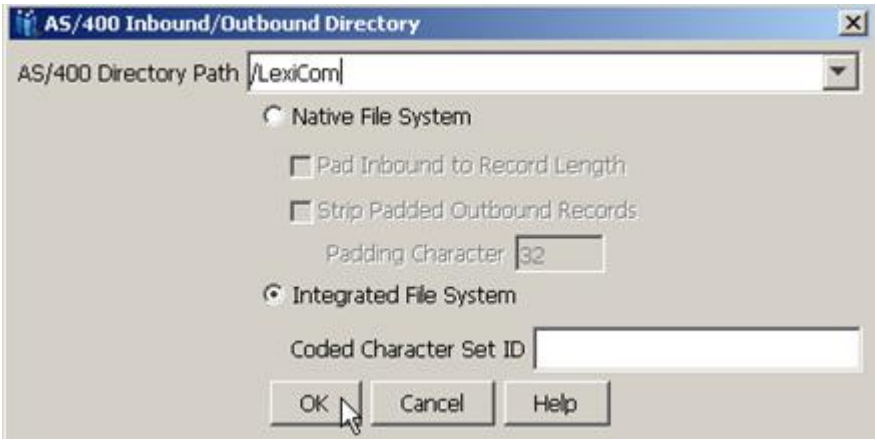


- In the **AS/400 Directory Path** field, enter /QSYS.LIB. This entry allows the Cleo LexiCom product to correctly do the EDCDIC / ASCII format conversion for any file that begins with the /QSYS.LIB path specifier.
- Select the **Native File System** option.
- Select the **Pad Inbound to Record Length** option if inbound files will consist of variable length records. When this option is selected, all records are transformed to a fixed-length format as they are stored in the AS/400 NFS file member. End of line terminators (i.e., CR, LF or CRLF) are stripped from the record and the remainder of the record will be padded with blanks. The record length is determined from the AS/400 NFS target file. If the inbound file contains a record larger than the AS/400 target file, an error will be logged and the file will not be stored. When this option is not selected, the inbound file will be assumed to already be fixed-length and will be streamed, i.e., no padding will be done to the records as the they are written to the AS400 NFS file member and end of line terminators will not be stripped from the file.
- Select the **Strip Padded Outbound Records** option if outbound records are a fixed record length and are padded with the specified **Padding Character**. The record length is determined from the AS/400 NFS target file. When this option is selected, padding characters (if present) after the terminator (CR, LF or CRLF) will be removed.
- The **Padding Character** is the decimal value of the character used in AS/400 target file for padding outbound records. By default, this value is set to 32 (the ASCII representation of a space). Any ASCII value between 0 – 127 may be used.

- The **Coded Character Set ID** field is only used when accessing the Integrated File System and is not accessible for the Native File System.

Note: For the Cleo LexiCom product to be able to determine that source and destination paths are part of the AS/400 native file system, the paths that you enter for the Inbox, Outbox (and optionally the Sentbox) on the **Host** > **General** panel must begin with the path that you specify in the **AS/400 Directory Path** field.

For Integrated File Systems



- In the **AS/400 Directory Path** field, enter /LexiCom (or any other appropriate IFS path).
- Select the **Integrated File System** option.
- Enter a value in the **Coded Character Set ID** field. If this field is left blank, the CCSID will be based on the default locale.

Warning: Setting a CCSID is only intended for directories where payload (e.g., inbox/ and outbox/) will be stored. **Do not set a CCSID for the /LexiCom installation directory or for any of the directories used to run the application (e.g., /LexiCom/lib; /LexiCom/hosts; /LexiCom/jre, etc.). Doing so will cause unpredictable results.**

Reading and writing into the AS/400 Native File System

Note: You should follow the instructions in this section only if you have an application or translator (such as TrustedLink) that requires you to write files into the AS/400 Native File System.

Before you can successfully read and write AS/400 native files, they must be created using the following AS/400 CL commands. In this example, we have created a LEXICOM library where the INBOUND, OUTBOUND and the optional SENTMSG files will reside:

```
CRTPF FILE(LEXICOM/INBOUND) RCDLEN(132) MAXMBRS(*NOMAX ) SIZE(*NOMAX)
```

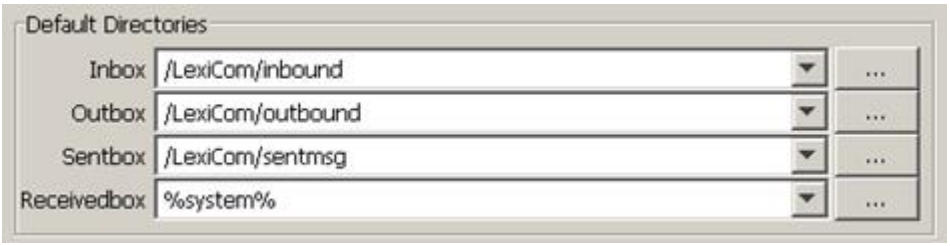
```
CRTPF FILE(LEXICOM/OUTBOUND) RCDLEN(132) MAXMBRS(*NOMAX) SIZE(*NOMAX)
```

```
CRTPF FILE(LEXICOM/SENTMSG) RCDLEN(132) MAXMBRS(*NOMAX) SIZE(*NOMAX)
```

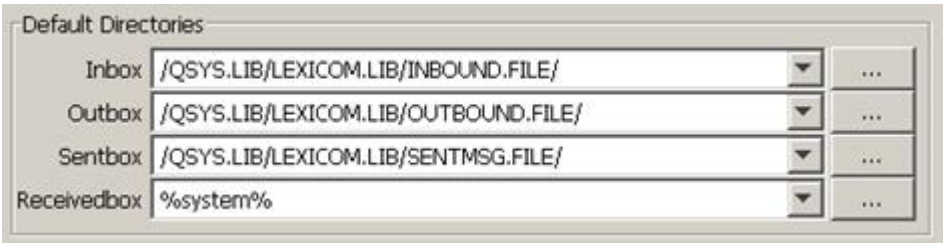
Special Note: If you are receiving fixed length documents from your trading partner and are writing to the Native File System (NFS) using the "append" option (FTP and FTP/s users only), the file you will be writing must have the same record length as the document being received and each line of the document must have the same fixed length. (The example above uses a record length of 132 characters however, in your environment this value may be different.)

The next step is to link the INBOUND and OUTBOUND (and optionally the SENTBOX) files with the "Inbox", "Outbox" and "Sentbox" in LexiCom. To do this, on the General panel at the Host level, enter the "Inbox", "Outbox" and optionally "Sentbox" entries as shown below:

For Integrated File Systems

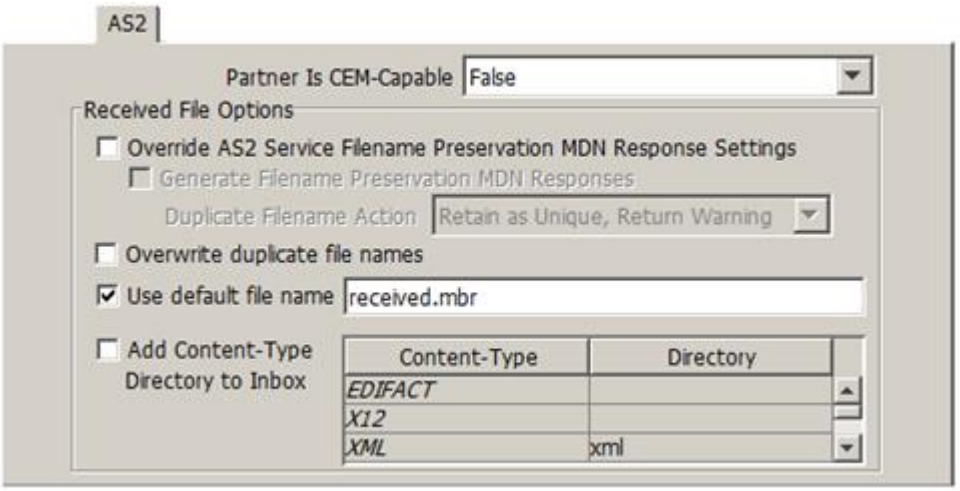


For Native File Systems



If you are using AS2 and are writing to the Native File System, in most cases you will need to define a default file name where the received entries will be stored.

An AS/400 native file must be in the form, `/QSYS.LIB/LIBRARY.LIB/OBJECT.FILE/FILE.MBR`. To accommodate this format requirement, on the **Host** > **AS2** panel, add a default file name with a `.mbr` extension, as illustrated below:

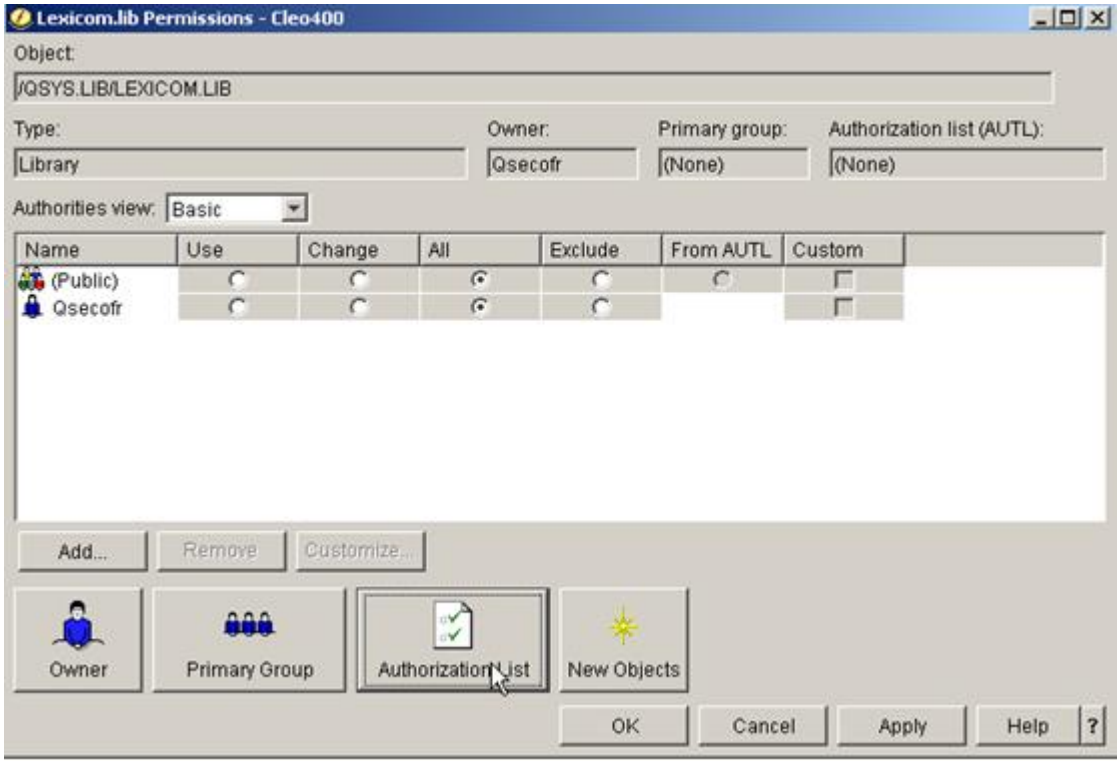


Assigning Object Authority to AS/400 Native File System Objects

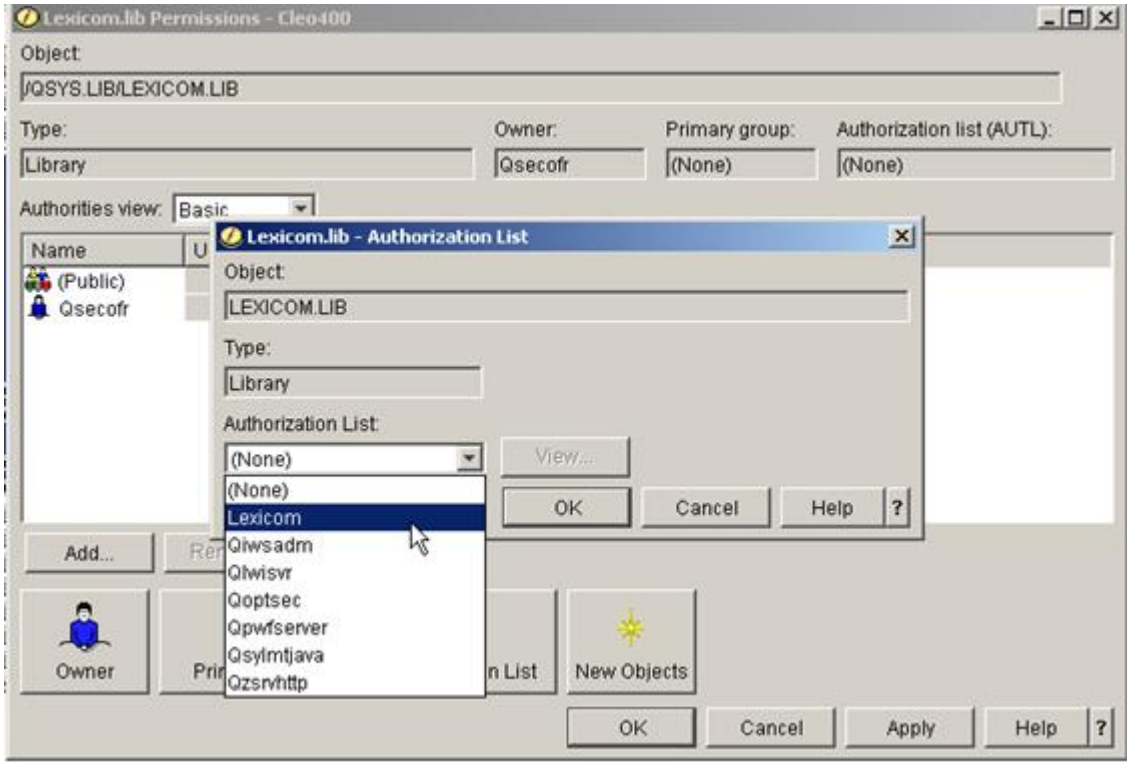
As with objects defined in the /LexiCom IFS directory that are not owned by the user who originally created them, *Authorization Lists* may be used to allow users read and write access rights to specified NFS libraries and files. If

read and/or write access is not properly assigned to users that will be reading and writing in the NFS directories, LexiCom will log errors that access to the request was denied.

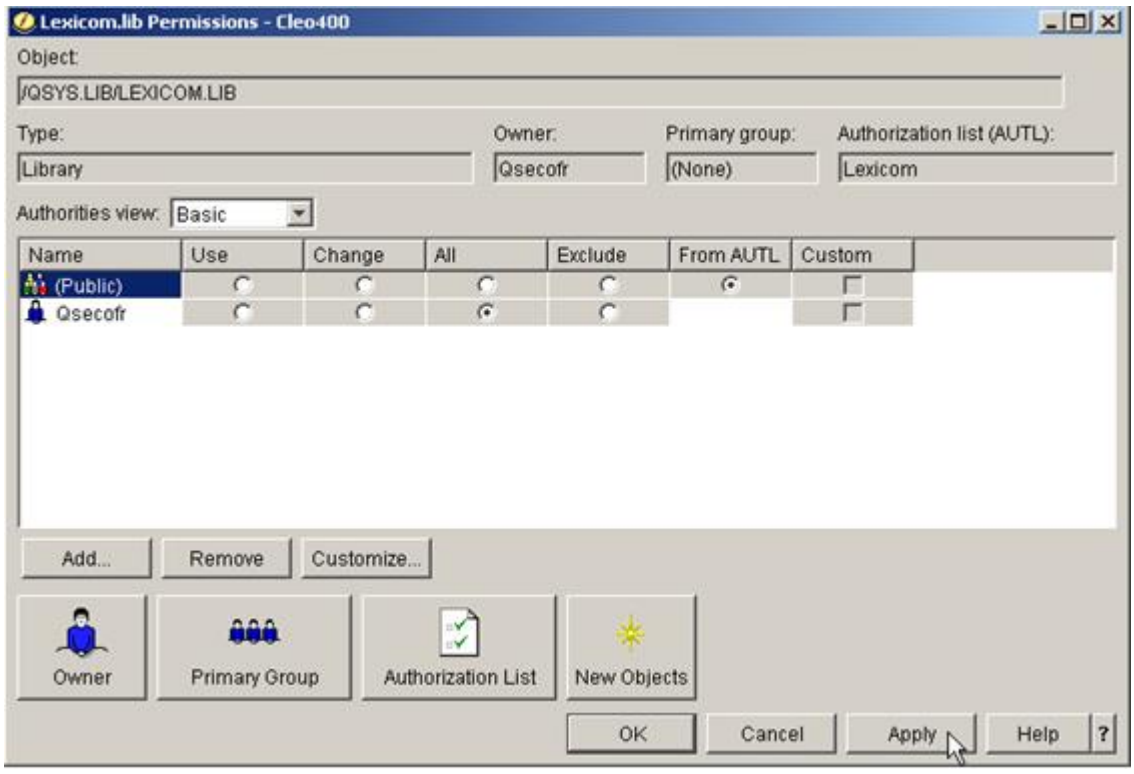
To assign permissions based on Authorization Lists, open the *File Systems* tree in System i Navigator and expand the *Integrated File System* entry. Then under the *QSYS.LIB* entry, right-click on the LEXICOM.LIB folder to choose the *Permissions* menu item and choose the **Authorization List** option:



Select the LexiCom Authorization List in the drop-down list and press “OK”:



Now, verify that the LexiCom Authorization List has been assigned to the /LexiCom Object, set the Public permissions to **From AUTL** and click **Apply**:

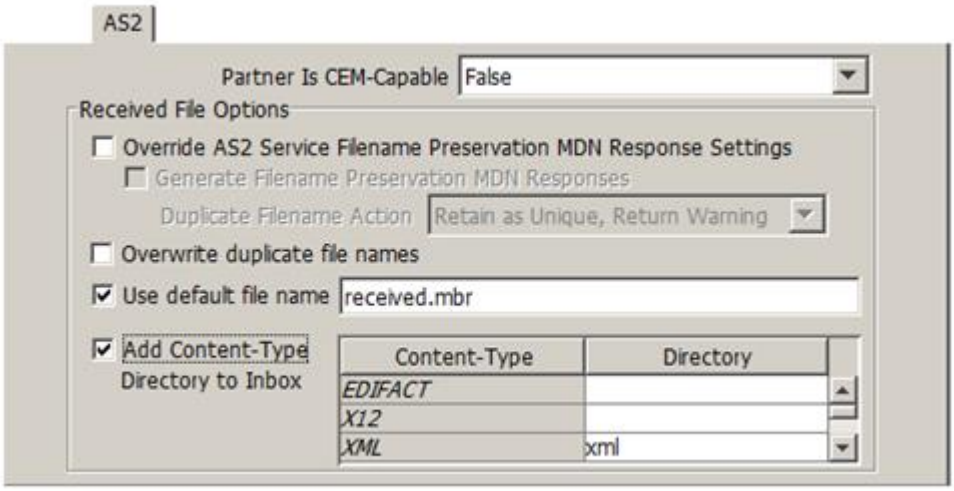


Note: The example above used the same Authorization List that was created for the /LexiCom IFS folder, but a different Authorization List may be used, if desired. Also, permissions may be applied separately to specific objects in the LEXICOM.LIB directory, e.g., INBOUND.FILE, OUTBOUND.FILE, etc.

Configuring Content-Type Inboxing for the AS/400 Native File System (AS2 only)

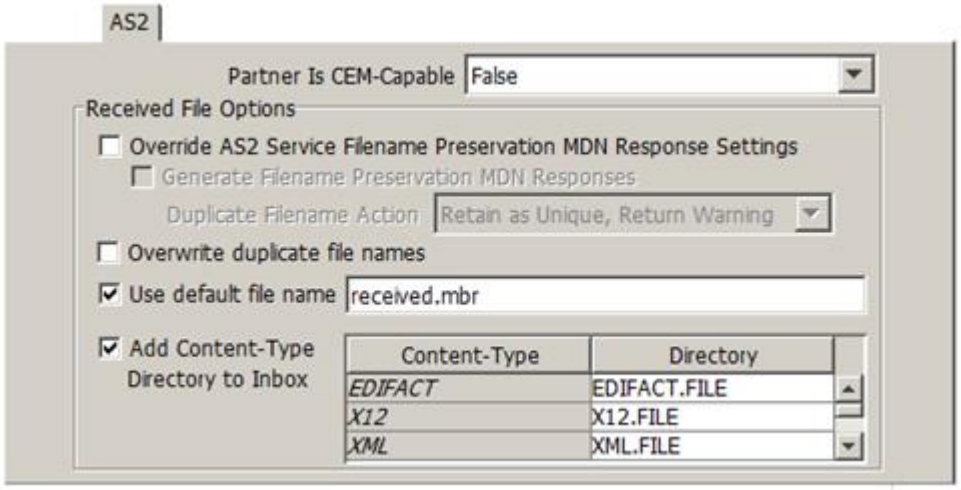
The **Add Content-Type Directory to Inbox** checkbox allows for sorting of incoming messages based on the content-type of the message to a subdirectory (under the *Inbox* specified on the General tab for the Host). You specify each of the content-types that you want directed to specified subdirectories by entering a name in the **Directory** field. Directory entries may be made for content-types of: EDIFACT, X12, XML, Binary, Plain Text, and Other (a default catch-all for messages with all other content-types you may receive.) The same subdirectory may be used for multiple content-types. You may also leave 'Directory' entries blank that will cause any received messages of that 'Content-Type' to be stored in the Inbox specified on the General tab.

Note: If you use this feature, incoming messages are placed in the specified folder based on the content type specified in the HTTP header of the message. The Cleo LexiCom application does not check the actual content of the message to determine its content type.

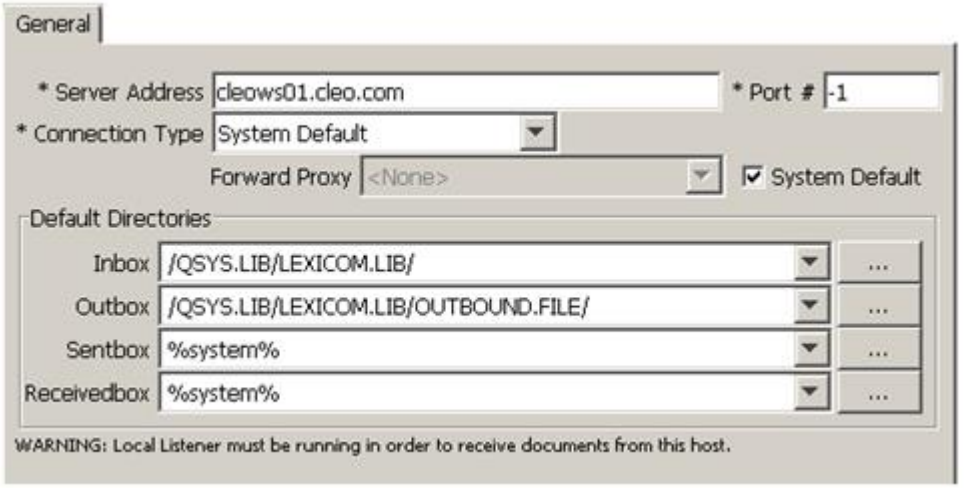


Note: If you are integrated with a translator, you should not add entries for the X12 or EDIFACT directories. These directories must remain blank for translator integration to work properly.

By default, the Content-Type directories are preconfigured for windows or IFS based folders. To use this feature on the AS/400 Native File System, you must modify all directories to be used so that the settings have the correct AS/400 syntax. That is, each directory must be specified in the form, `DIRECTORY.FILE`.



On the **General** tab, specify just the library for the `Inbox` value where the `Content-Type` files will be created. For example, `/QSYS.LIB/LEXICOM.LIB/`:



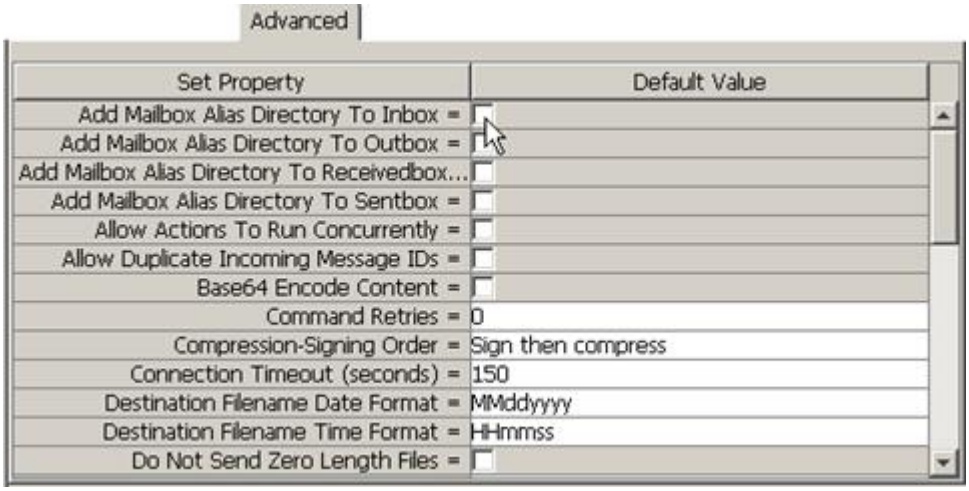
Now verify that all the "directories" that you have specified, i.e., files in the form DIRECTORY.FILE, have a matching physical file. In the example above, the files EDIFACT.FILE, X12.FILE and XML.FILE under the /QSYS.LIB/LEXICOM.LIB library are being used. If these files don't already exist, create a physical file for each of the files you have specified as follows:

```
CRTPF FILE(LEXICOM/EDIFACT) RCDLEN(132) MAXMBRS(*NOMAX) SIZE(*NOMAX)
```

```
CRTPF FILE(LEXICOM/X12) RCDLEN(132) MAXMBRS(*NOMAX) SIZE(*NOMAX)
```

```
CRTPF FILE(LEXICOM/XML) RCDLEN(132) MAXMBRS(*NOMAX) SIZE(*NOMAX)
```

As a final step, verify that the **Add Mailbox Alias Directory To Inbox** setting on the Advanced panel is not selected:



Configuring the Scheduler for the AS/400

Since the LexiCom AS/400 server does not have a UI to allow the user to manually send and receive files from trading partners, and typical AS/400 users will be integrating LexiCom with an EDI translator, the LexiCom Scheduler is a convenient way to invoke the <send> and <receive> actions that you have configured for your hosts.

See Scheduling actions - Native and Classic Web UI on page 611 for more information.

Starting and stopping on the AS/400

- To start the LexiCom server.
  a) From the AS/400 command line, type the command `STRLEXSVR` to start the LexiCom server.

     The server will take a few minutes to start.

     The server is fully started when port 1099 and the HTTP(/S) port (if using AS2) are active.

     If using only the FTP(/S) and/or HTTP(/S) protocols, the server is fully started when port 1099 is active. Additionally, the message `'LexiCom AS/400 process is now running.'` is written to the QSYSOPR log.
  b) You can easily view the existence of these ports from System i Navigator (under **Network** > **TCP/IP Configuration** > **IPv4** > **Connections**), or you can type the `WRKTCPSTS` or the `netstat` command from the AS/400 command line and then select Option 3 (Work with IPv4 connection status).
- To stop the Cleo LexiCom server.
  a) Type the command `ENDLEXSVR` from the AS/400 command line.

     You can also stop the Cleo LexiCom server from the Cleo LexiCom UI running through the IFS mapped drive. Select the **File** > **Stop AS/400** menu option.

     A dialog box appears asking you to confirm that you want to stop the LexiCom AS/400 process.

     The message, `'LexiCom AS/400 process is stopping...'` is written to the `QSYSOPR` log.
  b) Click on the "Yes" button and the LexiCom AS/400 process will be stopped and the message '**LexiCom AS/400 process has stopped.**' will be written to the QSYSOPR log.

     It may take several minutes for the server to stop, especially if the server is currently processing messages.
  c) You can verify the server has stopped by checking the port connections as described above or by checking the `QSYSOPR` log for the message '**LexiCom AS/400 process has stopped.**'.

When you want to start the Cleo LexiCom application again on the AS/400, you must run the **STRLEXSVR** command from the AS/400 command line.

Troubleshooting your AS/400 system

Following is a list of potential problems while using LexiCom on the AS/400. The list covers general problems. For technical support, please call 1-866-444-2536 or email support@cleo.com.

NOTE: Technical support is on a paid subscription basis. See Cleo Technical Support on page 11 for information.

Problem	Possible Cause(s)	Possible Solution
After installing LexiCom to the mapped drive, (e.g., "L:\"), the message "The installation of LexiCom is finished, but some warnings occurred during the install. Please see the installation log for details." When examining the LexiComInstallLog.log file, 7 Warnings are found.	All the warnings are "WARNING - String index out of range: -1" and are related to Install Uninstaller and Create LaunchAnywhere Java Executable Components.	This error occurs because LexiCom was installed to a drive letter and the Installer did not find a path. Since this is a mapped location, these are benign warnings and no further action needs to be taken.
When running AS/400 command "CALL INSTLEX" an error is returned that a jar file cannot be found	User did not install LexiCom using a network drive mapped to the AS/400 IFS directory /LexiCom	Verify that the IFS folder /LexiCom has been created and a drive has been mapped to it. Verify that LexiCom has been installed to that mapped drive and not the default directory C:\Program Files\LexiCom
Cannot access the AS/400 from System i Navigator.	User did not configure TCP/IP on the AS/400 properly. User did not define the host and domain name on the AS/400.	Verify that TCP/IP is configured properly. Use the command "GO CFGTCP". ✓ Verify that a TCP/IP host table entry has been added for your system (option 10). ✓ Verify that a host name and domain name have been configured for your system (option 12).
When sending a message to a host (specified as a host name instead of an IP address), an UnknownHostException error is returned.	User did not configure DNS on the AS/400 properly.	Configure DNS by typing the command "GO CFGTCP" (on the green screen) and choosing option 12. Enter a valid internet address in the "Domain name server" field.

Problem	Possible Cause(s)	Possible Solution
The times displayed in the LexiCom log entries are off by several hours.	User's system clock is not correctly defined for the appropriate time zone.	Using System i Navigator, go to the **Configuration and Service** > **System Values** > **Date and Time** panel. Click the **Time** tab. Click **Change Time Zone…** to reflect your current time zone.
After installing the permanent key, the AS/400 features are no longer available or the STRLEXSVR command no longer runs.	User does have not the AS/400 license specified on his permanent key.	The AS/400 option is available on the temporary key for evaluation purposes. Contact Cleo Sales for information and pricing of AS/400 features.
User cannot start LexiCom after installing the permanent key. It is returning the error: "java.io.FileNotFoundException: 'Path':\.license\.lc\.lcf (Access is denied)	The temp key was installed under a different user than the one attempting to install the permanent key.	Verify the owner of the .lcf file by viewing the "Properties" in System i Navigator. Install the permanent key using the same user as the owner of the file.
LexiCom fails to start when the STRLEXSVR command is invoked. No indication of the problem is displayed in the job log.	Various issues could cause LexiCom to fail to start.	If the failure has occurred before logging has started, the error should be recorded in the logs\exception.txt file. If there is no exception.txt file, check the LexiCom.xml file and the LexiCom.dbg file.
The error message displayed in the exception.txt file indicating that the required Java version is not installed.	User does not have Java Developer Kit (Option 17) properly installed on the AS/400.	Verify that Option 17, Feature 5117 - Java SE 8 64 bit is installed by typing the green screen command: DSPSFWRSC. If it is not there, obtain it from IBM (if you don't already have it on your installation media) and install it.
The error message "NoClassDefFoundError: com/ibm/as400/resource/ChangeableResource" is displayed when attempting to click the "New" button on the AS/400 Configuration panel.	The IBM jt400.jar file is not installed in the LexiCom home directory. The IBM jt400.jar is not in the class path.	Obtain the jt400.jar file using Cleo's software update process. Obtain a newer version of LexiCom.

Problem	Possible Cause(s)	Possible Solution
Exceptions are being logged: "Problem initializing decryption cipher. Illegal key size."	Encryption of sensitive data requires that unlimited strength jurisdiction policy files are properly installed in your JRE.	✓ Verify that you have installed LexiCom with the bundled VM. ✓ Examine the lax file and verify that the "lax.nl.current.vm" path points to the jre directory where LexiCom was installed.
When you launch the LexiCom executable, the error "Windows error 216 occurred while loading the Java VM"	This occurs when the Windows 64-bit JRE installer was used to install LexiCom on the IFS and you have mapped a drive to access it from a Windows 32-bit machine.	✓ If all users that will be launching the LexiCom executable are using Windows 32-bit machines, re-install LexiCom using the Windows 32-bit JRE installer. ✓ If there are some users that will launching the LexiCom executable from Windows 32-bit machines and others from Windows 64-bit machines, contact Cleo Support for further instructions on creating an alternate set of LexiCom executables for your Windows 32-bit machine users.
When you launch the LexiCom executable from a Windows 10 mapped drive, the LexiCom UI either never appears and/or the message "Error: Could not find or load main class com.zerog.lax.LAX " is displayed, or it takes several hours for the UI to appear and once it does, the messages in the messages panel do not display at all.	Windows 10 is incompatible with some versions of IBM i.	Use Windows 7 instead.

System

Use the **System** settings to control **Databases** and database payloads, set up **Export/Import** functions, configure **Bootstrap** options, and control and change other advanced system options. In the web UI, **System** settings can be found in the **Administration** menu. In the native UI, **System** settings can be found in **Options**. The following sections describe how to configure and set up these options.

Databases

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

In the web UI, go to **Administration** > **System** > **Databases**. In the native UI, select **Options** > **Databases**.

Use the **Databases** panel to configure one or more databases to be used either for VersaLex Transfer Logging or one of the optional Cleo VLNavigator applications. See Transfers on page 895 and Applications on page 660. When you click **New Database Connection**, the **Database Connection Configuration** dialog appears. Enter values for the following fields:

Connection Type

Choose `ODBC` for databases where ODBC (Open DataBase Connectivity) is used. Choose MySQL Connector/J if a MySQL JDBC connection is used. Otherwise, select Other.

Possible values: `ODBC`, `MySQL Connector/J`, or `Other`

Default value: `ODBC`

Connection String

JDBC connection string for accessing the database.

Examples:

```
jdbc:odbc:vltdb
```

```
jdbc:mysql://myhost:3306/vltdb
```

Driver String

This string describes the path to the Java class that will be used for accessing the database.

Examples:

```
sun.jdbc.odbc.JdbcOdbcDriver
```

```
com.mysql.jdbc.Driver
```

Username

Username for accessing the database (if required).

Password

Password for accessing the database (if required).

Single Record Timeout (seconds)

Prevents VersaLex from hanging on single-records transactional (i.e., transfer log and operator trail log) inserts and updates.

Possible values: `0-n` where `n` is a reasonable number. `0` indicates unlimited, but is not recommended as it could cause processing to hang in the event of database problems.

Default value:`150`

Test Database Connection

Attempts to create a database connection using the entered `Connection String`, `Driver String`, `Username`, and `Password` and indicates success or failure.

See Database Definitions on page 993 for information about JDBC drivers and driver/connection string values.

Database payload

See Database Definitions on page 993 for information about the database payload feature.

Database Incoming Mailboxes

For each trading partner mailbox, indicates whether VersaLex incoming payload should be inserted into the database rather than write to the file system.

Possible values: `Selected` or `Unselected`

For incoming transfers to enabled mailboxes, if the database is not currently available, the transfer from the trading partner is not accepted.

Default value: `Unselected`

Maximum supported BLOB size

The maximum BLOB size supported by the database (incoming and outgoing payload will be stored in a BLOB data type).

Possible values: Dependent on database

Default value: 65535 bytes

Polling interval for new outgoing payload

The frequency at which VersaLex will check for new outgoing payload.

Possible values: 5-60 seconds

Default value: 5 seconds

Outgoing payload attempt timeout

For abnormally terminated or unresponsive sends, the timeout at which the send will be retried by either a parallel or restarted VersaLex.

Possible values: 10-60 minutes

Default value: 30 minutes

Maximum failed outgoing payload send attempts

Dictates how many total times a transfer will be attempted before retries are halted.

Possible values: 0-n

Default value: 0 (no maximum)

Maximum number of concurrent sends

Maximum number of concurrent outgoing database payload actions that can be active at any given time. If the limit is reached and more outgoing payload is found, it is put on hold until one of the current outgoing database payload actions completes.

Possible values: 1-n

Default value: 50

Maximum number of concurrent sends per mailbox

Maximum number of concurrent outgoing database payload actions that can be active at any given time **for any given mailbox**. If the limit is reached and more outgoing payload is found for a mailbox, it is put on hold until one of the current outgoing database payload actions for that mailbox completes.

Possible values:

1-n and

<= Maximum number of concurrent sends

Default value: 5

Bundle (serialize) same mailbox sends per mailbox

At each polling interval, indicates to bundle payload for the same mailbox together up to the configured amount and send one-by-one using just one mailbox session.

Possible values: `Selected` or `Unselected`

2-n

Default value: `Unselected`

5

Database connection poolsize

If database payload is enabled, indicates the number of database connections immediately obtained and continually reused. These connections are used strictly for database payload.

Possible values: 0-n

VersaLex will still obtain connections above the poolsize specified when necessary and will continue to reuse those connections until they become idle for an extended period of time.

Default value: 20

Maximum number of database connections

If selected, specifies the absolute maximum number of allowed database connections (including poolsize) for database payload.

Possible values: `Selected` or `Unselected`

Poolsize-n

Default value: `Unselected`

0

Reserve connections for incoming

Percentage of the maximum number of database connections to reserve for incoming requests.

Possible values: 0-75 percent

Default value: 33 percent

Automatically clear outgoing payload after successfully sent

Indicates whether successfully sent payload should be automatically cleared by VersaLex.

Possible values: `Selected` or `Unselected`

Default value: `Selected`

Stream incoming payload direct into the database

Indicates whether incoming payload should be streamed directly into the database or through a temporary file. For Oracle and MySQL, this may need to be turned off depending on specific database and driver versions and configuration. This option is not available on SQL Server nor DB2, as a filesize must be known prior to initiating the stream.

Possible values: `Selected` or `Unselected`

Default value: `Selected`

Include user inbox subdirectories as incoming database payload

Indicates whether files stored by a connected HTTP, FTP, or SSH FTP client in a subdirectory of their configured inbox should be inserted into the database.

Possible values: `Selected` or `Unselected`

When this value is false, only files stored in (or renamed into) the user's inbox are inserted into the database.

Default value: `Unselected`

Include user outbox subdirectories as outgoing database payload

Indicates whether files retrieved by a connected HTTP, FTP, or SSH FTP client in a subdirectory of their configured outbox should be updated in the database.

Possible values: `Selected` or `Unselected`

When this value is false, only files retrieved from the user's outbox are updated in the database.

Default value: `Unselected`

Temporarily suspend incoming/outgoing database payload

Indicates whether the database payload feature has been temporarily put on hold by a user.

Possible values: `Selected` or `Unselected`

Default value: `Unselected`

- Unlike all other VersaLex configuration parameters, these parameters are stored in the database rather than the conf/Options.xml file.
- Retries are automatically scheduled based on **Autosend Retry Attempts** and **Autosend Restart**. See Other system options on page 729.

Exporting user files

You export user files to save configuration data you can later import into a Cleo Harmony, Cleo VLTrader, or Cleo LexiCom system.

1. In the web UI, go to **Administration** > **System** > **Export**. In the native UI, select **File** > **Export** in the menu bar.
2. Select any combination of host files, configuration files, user certificates, and CA certificate files.

   If you select a user certificate for export, you must also provide a private key password. User certificates and associated private keys are exported as `PKCS#12` files.

   You can also select any additional files, but typically you would not want to include the following:

   - Cleo Harmony, Cleo VLTrader, or Cleo LexiCom libraries (`.jar` files)
   - Java runtime environment (`jre/` files)
   - User certificate/private key store (`data/` files).

   Note: User certificates/private keys can be exported individually.

   You can export a partial host by right-clicking on a host and selecting a set of mailboxes or actions. Alternatively, you can export a partial host export by selecting **Export…** from a mailbox or action in the active host tree. The configuration, user, and trading partner certificates corresponding only to the selected hosts can also be exported by selecting the **For selected host(s) only** check box in the respective table. If you initiate export process from the active host tree, the dialog box offers the same options overall.

   Two specially named additional files, `prereadme.txt` and `postreadme.txt`, if included during **File** > **Export**, are displayed as pre-import and post-import instructions when an exported file is imported.

   Note: As an added security feature, the **Additional File(s)** section of the dialog may be removed by setting the *cleo.file.export.additional.files* system property to false in the `conf/system.properties` file or by using a `-D cleo.file.export.additional.files=false` command line parameter. This property only affects the dialog launched from the **File** > **Export** menu option and does not affect exporting additional files via the command line. See Running from the command line on page 38 for more information.
3. Select a suitable passphrase and confirm it.

This passphrase is used to encrypt secure content (for example, passwords) within the selected files. Additionally, this passphrase is used to AES encrypt the entire exported zip file. The passphrase must be a minimum of 8 characters in length. Note that the length of the password determines the strength of the AES encryption key. Refer to the following table for guidance.

Password Length	AES Key Strength
< 8	invalid -- too weak
8 <= length < 32	128-bit key (weakest)
32 <= length < 48	192-bit key
48 <= length < 64	256-bit key (strongest)

Note: The passphrase is case sensitive and that all preceding and succeeding whitespace of the passphrase is trimmed and ignored.

4. Click **Export**.
5. Select the location to save the exported zip file and click **Save**.
6. Optionally, click **Save As** to save current filter settings to an XML file. You can use this XML file later to recall these settings using **Open** or with the `Harmony`, , or `c -b` command-line option (see Running from the command line on page 38).

Importing user files

You can import data from a `.zip` file generated by the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application. You can choose a local `.zip` file or a remote file if your system is connectd to a Cleo Harmony or Cleo VLTrader trading partner and the administrator has provided a network deployment URL. Such a deployment URL points to a `.zip` file at a web location (possibly the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application).

1. To import user files from a zip file exported from the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application, select **File** > **Import** in the menu bar in the native UI to display the **Import User Files** dialog box. In the web UI, go to **Administration** > **System** > **Import** to display the **Import** page.
2. Choose a file or a deployment URL from which to import data.
   - In the native UI, in the Import User Files dialog box, select**Local File**, navigate to the local `.zip` file you want to import, and click **Open** *OR* select **Deployment URL**, specify the URL and connection type you want to use for import, and click **Download**.
   - In the web UI, click **Select file to import**, navigate to the file you want to import, and click **Open**.

   The Import User Files dialog box (native UI) or Import page (web UI) is redisplayed and populated with the contents of the `.zip` file you specified.
3. Select any combination of the available files and click **Import**. A private key password must be provided with each selected user certificate. If any of the files selected already exist, you will be prompted.

   For a partial host import where a set of mailboxes is being imported, the parent host must exist and if a mailbox being imported already exists, the user is prompted with a similar as above. Actions being imported within a partial mailboxes and partial configuration imports are handled in the same fashion.

   Note: As an added security feature, the **Additional File(s)** section of the dialog may be removed by setting the *cleo.file.import.additional.files* system property to false in the `conf/system.properties` file or by using a `-D cleo.file.import.additional.files=false` command line parameter. This property only affects the dialog launched from the **File** > **Import** menu option and does

not affect importing additional files via the command line. See Running from the command line on page 38 for more information.

4. If the host being imported is disabled in the import file, select **Enable host if disabled** to enable the host on import.
5. If the passphrase was set on export then it is required in order to decrypt and import. However, if there was no passphrase set on export then this field may be left empty.
6. Once the import is complete, the imported items (hosts, certs, etc.) are immediately available for use.

Zip files exported from the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application can also be imported using the `Harmony`, `VLTrader`, `LexiCom` commandline `-i` option.

The following example imports a file originally exported from the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application:

```
VersaLexc -i VersaLexConfig.zip -pp cleocleo -cp keypswd1 -cp keypswd2 -m
```

where:

- -i `VersaLexConfig.zip` - import the file, `VersaLexConfig.zip`.
- -pp `cleocleo` - cleocleo is the passphrase used when the data was exported.
- -cp `cleo` -cp `keypswd1` -cp `keypswd2` - certificate private key passwords that are rotated through until one matches.
- -m - shows the output of the import on the console.

See Running from the command line on page 38.

Bootstrap configuration

You can configure the settings of the Java Virtual Machine (JVM) for each instance of your Cleo product. The configured settings are used when the JVM is launched via a UI, command line or for a Windows service (Windows only).

Note: You can disable this option by setting *cleo.configure.launcher* property to `false` in the `conf/system.properties` file or by using a `-D cleo.configure.launcher=false` command line parameter.

To configure the launcher for an instance of your Cleo product, do the following:

1. In the web UI, go to **Administration** > **System** > **Bootstrap**. In the native UI, select **Configure** > **Launcher** from the menu bar.
2. You can configure a launcher for the **UI**, **Command Line** or **Windows Service**. For the launcher you want to configure, specify values for the following parameters:

   Maximum Memory

   Sets the maximum heap size the application will use. The example below configures the maximum heap size for 700M (700 megabytes). To set the maximum heap size to 2 gigabytes, enter 2048M or 2G. If this field is blank the default maximum heap size will be used. The default maximum heap size can be determined from the table below for most platforms.

Oracle (Sun)JVMs

Client JVMs	The default maximum heap size is half of the physical memory up to a physical memory size of 192 megabytes and otherwise one fourth of the physical memory up to a physical memory size of 1 gigabyte. For example, if your machine has 128 megabytes of physical memory, then the maximum heap size is 64 megabytes, and greater than or equal to 1 gigabyte of physical memory results in a maximum heap size of 256 megabytes.
Server JVMs	Server JVM heap configuration is the same as the Client, except the default maximum heap size for 32-bit JVMs is 1 gigabyte, corresponding to a physical memory size of 4 gigabytes, and for 64-bit JVMs is 32 gigabytes, corresponding to a physical memory size of 128 gigabytes.
IBM JVMs	
Windows FIPS	Half the available memory with a minimum of 16 MB and a maximum of 512 MB

Override Default Time Zone

Allows you to override the operating system time zone. Select the appropriate time zone from the list of time zone settings available to the JVM. If this field is blank, the default operating system time zone will be used.

Other Settings

Allows you to specify other parameters to the JVM. For example, to specify the initial Java heap size to 70M (70 megabytes), enter `-Xms70M` in the **Other Settings** field.

LexiCom AS/400 Install Share Directory

Allows you to install Cleo LexiCom locally in addition to on an AS/400 share for better UI performance. Once you point the local LexiCom install at the AS/400 share and restart the local install, the local install is pointed at the AS/400 `config/logs/...`. When you perform a software update, the update is applied to both locations whether it's a release or a patch, helping to ensure versions are kept in sync across locations.

3. Click **Test** to test the configured settings by launching a JVM.

   If the JVM is launched successfully with the configured parameters, the system displays a success confirmation dialog box. Click **OK** to dismiss the dialog box.

   If the test is not successful, the system displays a dialog box indicating the test was not successful. Click **OK** to dismiss the dialog box.
4. Click **Apply**. The application must be restarted for any changes to take effect.

Other system options

The **Other** tab allows you to set some options that apply to various sections of the product.

In the web UI, go to **Administration** > **System** > **Other**. In the native UI, go to **Options** > **Other**.

To filter the display, enter a case-insensitive string in the **Filter String** field. Note that for the web UI you must press **Enter** after typing **Filter String** text.

Allow Scheduled Actions to Run Concurrently

Normally, actions and hostactions scheduled to run concurrently will in fact run concurrently. If this option is disabled, the scheduler will wait for the currently scheduled action to stop before starting another scheduled action.

If two actions within the **same** host are scheduled to run concurrently and this option is enabled, the host's Advanced property setting for **Allow Actions to Run Concurrently** dictates whether the actions are run sequentially or concurrently.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values: `On` or `Off`

Default value: `On`

Always Show The Logged Message Date

Indicates to display both the message date and time when scrolling messages. By default only the logged message time is shown when scrolling messages in the messages pane or with the command-line -m option.

Possible values: `On` or `Off`

Default value: `Off`

Autorun Directory

Directory in which command files are to be automatically processed.

Possible values: Any local or shared directory

Default value: `autorun\`

Autosend Check Every (seconds)

Number of seconds scheduler should wait before checking again if there are files to send. Note that this property is only used with continuous autosend.

For the Cleo VLTrader and Cleo Harmony applications, this value is also used to control the frequency of checking for autoroute files, as well as determine the frequency autochecking commands that are simply checking for the existence of a file or directory existence (that is, the `Age` parameter has a value of `>0D`).

Possible values: 5-60

Default value: 5

Autosend Restart

Used to determine the period before restarting certain operations. These operations include, but are not limited to, certain failed scheduled actions (both autosend and periodic), router restart, database payload restart, and trigger processing restart.

Possible values: 1-60

Default value: 30

Autosend Retry Attempts

Number of contiguous retries of failed scheduler autosend of a file, after which the action is skipped until the number of minutes specified for **Autosend Restart** have passed.

Possible values: -1-n

`-1` indicates to never stop retrying

Default value: `2`

Autosend Round Robin

If on, indicates to check only the **next** autosend action at each **Autosend Check Every** interval. If off, indicates to check **all** autosend actions at each interval.

Possible values: `On` or `Off`

Default value: `Off`

Client SSH FTP Cipher Pattern

Regular expression (enclosed in brackets) that limits the set of cipher algorithms available for all SSH FTP client connections. The [List] button shows the resulting set of cipher algorithms for this property setting.

Example values include:

- `[.*]` - All supported cipher algorithms
- `[.*cbc.*]` - Only supported cipher algorithms containing 'cbc' in the name.
- `[((?!cbc).)*]` - All supported cipher algorithms except those containing 'cbc' in the name.

Protocols supported: SSH FTP

Client SSH FTP Key Exchange Pattern

Regular expression (enclosed in brackets) that limits the key exchange algorithms available for all SSH FTP client connections. The **List** button shows the resulting set of key exchange algorithms for this property setting.

Example values include:

`[.*]` - All supported key exchange algorithms

`[.*group14.*]` - Only supported key exchange algorithms containing `group14` in the name, for example, `diffie-hellman-group14-sha1`.

`[((?!group14).)*]` - All supported key exchange algorithms *except* those containing `group14` in the name

`[.*curve.*]` - Only support `curve25519-sha256@libssh.org` key exchange algorithm

`[((?!sha1).)*]` - Do not support algorithms containing `sha1` in the name, that is, `diffie-hellman-group1-sha1` and `diffie-hellman-group14-sha1`

Protocols supported: SSH FTP

Client SSH FTP MAC Pattern

Regular expression (enclosed in brackets) that limits the set of MAC algorithms available for all SSH FTP client connections. The [List] button shows the resulting set of MAC algorithms for this property setting.

Example values include:

`[.*]` - All supported MAC algorithms

`[.*sha1.*]` - Only supported MAC algorithms containing `sha1` in the name.

`[((?!sha1).)*]` - All supported MAC algorithms except those containing `sha1` in the name.

Protocols supported: SSH FTP

Client SSH FTP Public Key Pattern

Regular expression (enclosed in brackets) that limits the set of public keys available for all SSH FTP client connections. The [List] button shows the resulting set of public keys for this property setting.

Example values include:

- `[.*]` - All supported public keys
- `[.*cbc.*]` - Only supported public keys containing 'cbc' in the name.
- `[((?!cbc).)*]` - All supported cipher algorithms except those containing 'cbc' in the name.

Protocols supported: SSH FTP

Cluster Network Not Fully Reachable

When selected, this property prevents the document database from attempting to replicate itself. It is useful in cases where synced servers are not fully able to connect with each other over the required doucment database

ports. This property prevents the document DB from restarting repeatedly, but also causes the failover server to exclude events and transfers for the primary server should it become active.

Possible values: `On` or `Off`

Default value: `Off`

Custom ILexiComIncoming Class

Custom LexiComLogListener Class

Custom LexiComOutgoingThread Class

Refer to the API javadocs for a description of the interfaces:

- `ILexiComIncoming` can be used to filter incoming payload streams to an independent repository (database, message queue, different directory/filename, etc.) based on the originating trading partner or payload content or protocol headers/parameters.
- `LexiComLogListener` can be used to watch XML log events and react to successful/ unsuccessful sends/ receives.
- `LexiComOutgoingThread` can be used to wait/watch for new outgoing payload in an independent repository (database, message queue, directory/filename, and so on) and then stream to the appropriate trading partner using a VersaLex IMailboxController.

Note: For instance, the sample API class `PartnerComm` in the examples package would be specified as `examples.PartnerComm`

Note: For Cleo LexiCom, API option must be specifically licensed.

Possible values: Fully-qualified name of class implementing interface.

Archive containing the implementation(s) must be copied to the `lib/api/` folder.

Disable Date/Time Portion of Filenames In Sent/Received Box

When selected, filenames written to the sent and received box will not include a date/time stamp or the product serial number (if synced).

Possible values: `On` or `Off`

Default value: `Off`

Document DB Health Check Retry Attempts

The number of repetitive exceptions that must be thrown in document DB maintenance operations (for example, health checks) before the document DB cluster is restarted.

Default value: `3`

Document DB Maximum Result Window

The maximum number of returned events for document DB searches per daily index. Increases in this limit will impact the VersaLex OSGi process memory usage if large queries are frequent. A change to this limit may take a minute to take effect.

Minimum value: `2000`

Default value: `100000`

Document DB Query Maximum Total Hits

The maximum total number of returned events for document DB searches. Increases in this limit will impact VersaLex main process memory usage if large queries are frequent.

Minimum value: `10000`

Default value: `500000`

Document DB Query Page Size

The number of events returned with each document DB query page as a document search result is built. Specifying larger values results in fewer round trips with the OSGi process to build the result. Increases in this limit will impact the VersaLex OSGi process memory usage if large queries are frequent.

Minimum value: `100`

Default value: `5000`

Document DB Scroll Size

The maximum number of results returned with each document DB scroll request.

Minimum value: 10000

Default value: 100000

Email And Execute On Resolution

If this option is set to true and "Email/Execute on Repetitive Failures" is turned off, when the failure is resolved, an email is sent and/or "execute on" is performed. This option applies to all three levels of "Email/Execute On Repetitive Failures".

Default value: `True`

Email Local And Partner Activation Notifications

When this option is set to true and a scheduled certificate is activated, an email is sent to the system administrator.

Default value: `True`

Enable GUI as Cleo Harmony Service/Daemon

Enabling the GUI as a service/daemon allows the normally GUI-only process to run as a (semi-limited) independent service/daemon. It is only possible for the GUI to operate in this capacity when there is not already a Cleo Harmony service/daemon running.

Note: Leaving this option *off* ensures that the service/daemon is capable of starting up.

Possible values: `On` or `Off`

Default value: `On`

Enable Cleo Harmony Service/Daemon as GUI

Normally if the product is running as a service/daemon, when the product GUI is displayed, it remains a second process and communicates with the service/daemon over the RMI port.

Enabling the service as a GUI will force the service/daemon to display the GUI itself and eliminate the second GUI-only process.

Possible values: `On` or `Off`

Default value: `Off`

Except on Windows 98, where defaults to `On`

Enforce Password Policy

When selected, the configured password policy is enforced for all local user mailboxes that have not overridden this password policy.

Click **Configure** to customize the Password Policy. See Configuring password policies on page 55 for further information.

Possible values: `On` or `Off`

Default value: `Off`

Note: This is a Cleo VLTrader and Cleo Harmony option.

FIPS Mode

If licensed, this FIPS Edition option may be used to enable use of only the FIPS 140-3 approved cryptographic operations.

Note: When enabled, this mode is not compatible with certain versions of the Microsoft SQL JDBC data base driver. OpenPGP operations are not supported when FIPS Mode is enabled.

Note: This is a Cleo VLTrader and Cleo Harmony FIPS Edition Only option, which has additional license restrictions.

Possible values: `On` or `Off`

Default value: `Off`

Force Apply/Reset When Changing Content Panes

When selected, the product displays a dialog box that prompts you to either apply or reset any pending changes before you can move to another content pane.

Note: This option applies only to the native UI. In the web UI, whether this option is selected or not, the product does not prompt you to save any pending changes and does not save any pending changes if you do not explicitly click **Apply** before you transition to another content pane.

Possible values: `On` or `Off`

Default value: `On`

Heap Dump on Memory Errors

When selected, a heap dump is performed for the first occurrence of an out of memory error for the current process. The heap dump will be created only when detected by the internal Cleo Harmony memory monitor.

Possible values: `On` or `Off`

Default value: `Off`

High Priority Transfers Percentage Available Bandwidth

The percentage of the detected available bandwidth that is allotted to high priority transfers. The bandwidth available to the Cleo Harmony application is continuously calculated based upon the total transfer rate within the last minute of the currently active transfers.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values: 60-100

Default value: 75

Include Millisecond In System Log File

Indicates to add a millisecond (ms=) attribute to each `<Mark>` element in the system xml log file, which allows for finer granularity on event time stamps. This option will also cause a .millisecond value to be appended to each event's time in the listener's and actions' logged messages.

Possible values: `On` or `Off`

Default value: `Off`

LDAP SSL Maximum Protocol Version

Specifies the maximum protocol version allowed for all LDAP connections that use SSL security.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values:

- SSL 3.0 - refer to RFC6101
- TLS 1.0 (SSL 3.1) - refer to RFC2246

- TLS 1.1 (SSL 3.2) - refer to RFC4346
- TLS 1.2 (SSL 3.3) - refer to RFC5246
- TLS 1.3 - refer to RFC8446

Default value: TLS 1.3

LDAP SSL Minimum Protocol Version

Specifies the minimum protocol version allowed for all LDAP connections that use SSL security.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values:

- SSL 3.0 - refer to RFC6101
- TLS 1.0 (SSL 3.1) - refer to RFC2246
- TLS 1.1 (SSL 3.2) - refer to RFC4346
- TLS 1.2 (SSL 3.3) - refer to RFC5246
- TLS 1.3 - refer to RFC8446

Default value: SSL 3.0

Macro Multiple Value Separator

When passing a macro value as a parameter to a batch job (for example, when using an **Execute On** property) where multiple values are being collected (for example, in a `PUT -MUL` command), this property can be used to replace the default `\n` separator character which is interpreted by the batch job as a terminator causing only the first value to be passed as the parameter.

This applies these macro values:

- `%file%`
- `%sourcefile%`
- `%srcfile%`
- `%sourcefilebase%`
- `%srcfilebase%`
- `%sourcefileext%`
- `%srcfileext%`
- `%destfile%`
- `%destfilebase%`
- `%destfileext%`
- `%transferid%`

Possible values:Any desired character(s) that can be used to separate multiple values (for example, a semi-colon or comma). Additionally, the following escaped characters are also valid:

- `\n` (carriage return), `\t` (tab) or `\s` (space)

Default value: `\n`

Maximum Allowed Synchronization Queue Size

If the synced Cleo Harmony instance is offline and the maximum queue size is reached, synchronization is disabled and will require re-initialization once the instance is again online.

Possible values: 0-n

Default value: 10000

Maximum Number of Concurrent Routes

Maximum number of concurrent router actions that can be active at any given time. If the limit is reached and a new route is needed, it is put on hold until one of the current route actions completes.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values: 1-n

Default value: 10

Maximum Number of Concurrent Scheduled Actions

Maximum number of concurrently scheduled actions that can be active at any given time (per instance of the Cleo Harmony application). If the limit is reached and a new action is scheduled to run presently, it is put on hold until one of the currently running scheduled actions completes.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values: 0-n, where 0 indicates no maximum limit.

Default value: 0

Maximum Number Of Concurrent Transfer Checks

Maximum number of concurrent transfer checks (`CHECK -TRA`) that can be active at any given time. If the limit is reached when a `CHECK -TRA` action is invoked, the action is suspended until one of the current transfer checks completes. All pending requests are processed in the order in which they are issued.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values: -1-n

-1 indicates no maximum limit.

0 indicates only one check can run at any given time.

Default value: 0

Maximum Number Of Concurrent Users

Maximum number of concurrent GUI users allowed at any given time.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values: 1-n

Default value: 5

Maximum Number Of Trigger Event Threads

Controls the number of execution threads created for running the actions configured for trigger events.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values: 1-n

Default value: 15

Maximum Saved Database Transfer Log Entries

If database transfer logging is enabled but the database is unavailable, transfer log entries are saved to disk and the database is brought up-to-date when it is again available. This applies to the basic send/receive transfer log and EDI option, but does not apply to the database payload option. If the maximum saved entries is reached while the database is down, the oldest saved entries are deleted when new entries are added.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values: -1-n

-1 indicates no maximum limit.

Default value: 10000

Maximum Trigger Persistor File Size (mbytes)

Controls the rollover of the trigger file once the specified size is reached.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values: 1-n

Default value: 5

Minimum Memory Free Percentage

Minimum percentage of maximum available memory allowed before low memory warnings may be logged. If zero, the internal memory monitor will be disabled.

Note: This option is only available when the optional Cleo System Monitor module has not been licensed.

Possible values: 0-100

Default value: 20

Minimum Number Of Macro Index Digits

When the `%index%` macro is used, this property determines the minimum number of digits for the index string. The index string is padded with zeros to fill the minimum digit requirement.

Possible values: 1-n, where n is a reasonable number for the application.

Default value: 1

MSMQ Administrative Queue Suffix

The suffix used for the inbound administrative queue. This is the queue used to monitor MSMQ send acknowledgments. See MLLP Configuration on page 367 for more information about the **Mailbox Queuing** tab.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values: Any reasonable expression.

Default value: '_r_admin'

MSMQ Write Timeout (seconds)

When writing to an inbound queue, this is the maximum time it should take to receive an acknowledgment on the administrative queue.

Possible values: 1-n, where n is a reasonable number for the application.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Default value: 30

No Reply Sender Display Name

When an email is sent from Cleo Portal to a user (for example, forgot password reset email), this value is the display name of the (automated) sender.

Default value: Empty (no display name)

No Reply Sender Email Address

When an email is sent from Cleo Portal to a user (for example, forgot password reset email), this value is the email address of the (automated) sender.

Default value: Empty (will use user's own email)

Number Of Scheduler Threads

If the scheduler has a large number of autosend tasks to be performed on a very frequent basis, the number of scheduler threads can be increased to help imrprove scheduler performance. Normally, this value should be set to '1' and only increased if performance is seen to be a problem. Use caution when tuning this variable, as too many threads could create downstream bottlenecks.

Note: By default, periodic (non-autosend) actions run independently from autosend actions. Therefore, the total number of scheduler threads will actually be set to this value **plus one**. The only exception to this is if host-level or system-level action concurrency is disabled.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values: 1-10

Default value: 1

Only Cleo Harmony Service/Daemon Auto-Starts Tasks

Normally if Cleo Harmony is NOT running as a service/daemon and if the Cleo Harmony GUI is displayed, it will start up the schedule and local hosts if they have been marked for automatic startup.

Possible values: `On` or `Off`

Default value: `Off`

Portal Application Name

The name to be used in emails sent from Cleo Portal, displayed in the browser, and so on, to identify Cleo Portal.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Default value: Cleo Portal

Portal Auth Token Expiration (seconds)

Controls how long a user session in Cleo Portal will last before timeout/expiration.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Default value: 3600 seconds (1 hour)

Portal Custom Forgot Password URL

Indicates an URL to send Cleo Portal users to when they click **Forgot your password?** link instead of displaying the default dialog.

If you specify a value for the Portal Custom Forgot Password URL property, when the user clicks the Forgot Password link on the Portal login page, it opens the URL specified in the property and your URL handles the forgotten password processing.

If you do not specify a value, when the user clicks the Forgot Password link on the Portal login page, it opens the built-in modal dialog box and Cleo VLTrader or Cleo Harmony handles the forgotten password processing.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Default value: Empty (just display default dialog)

Portal Forgot Password Link Expiration (seconds)

Controls how long an emailed Cleo Portal password reset link lasts before becoming expired.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Default value: 3600 seconds (1 hour)

Portal Idle Timeout (minutes)

Controls how long Cleo Portal can be idle before it times out.

Possible values: -1 or a positive integer. Specify -1 for no time out.

Default value: -1

Portal Maximum Outlook Attachment Size (bytes)

Controls the threshold for uploading files from Outlook. Files smaller than this value are attached to Outlook. Files equal to or larger than this value are uploaded to Cleo Portal.

Note: Do not set this value higher than the mail server's attachment size limit.

Note: This is a Cleo Harmony option.

Default value: 10 MB

Portal Self Registration Link Expiration (hours)

Controls how long an emailed Cleo Portal invitation link lasts before before becoming expired (after which the invited user will need to request a reinvitation).

Note: This is a Cleo VLTrader and Cleo Harmony option.

Default value: 168 hours (7 days)

VersaLex Service/Daemon RMI Port

When Cleo Harmony software is installed and/or running as a Windows service or Unix daemon, it listens on this TCP/IP port to accept VersaLex client commands.

Possible values: 1024-49151, comma or dash separated (ex. 1100-1105,2100-2105)

Default value: 1099-1109

VersaLex Service/Daemon RMI Secondary Ports

In addition to the main RMI port above, one additional RMI port is used by the service/daemon and each Cleo Harmony client (GUI or commandline). By default, these secondary ports are dynamically allocated, which is potentially a problem for installations accessed over a WAN and/or through a firewall. At least two secondary ports should be specified (these ports need to be open both inbound and outbound through the firewall).

Possible values: 1024-49151, comma or dash separated (ex. 1100-1105,2100-2105)

VersaLex Service RMI Bind Address

The RMI server bind address. Only change the default setting if Cleo Harmony UI or API client access is needed across nodes. If this is the case, remember to block the RMI ports except between the nodes involved.

Possible values:

- IPv4 address or IPv6 address or `hostname` or `*`
- A blank value (default) indicates to bind to the loopback address (127.0.0.1), except for LexiCom running on an AS400 where a blank value indicates to bind to any/all local addresses to allow the Windows UI to be accessed
- A value of 'localhost' also means 127.0.0.1
- A value of '*' indicates to bind to any/all local addresses

Replicate Event Log Queue Size

The maximum in-memory replicate event log queue size. A larger queue size might be necessary for high-throughput spikes to buffer against adversely affecting active and new transfers.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Possible values: `1000 - n`

Default value: `1000`

Retry All Failed Scheduled Actions

Select this option to automatically retry scheduled actions that fail. For autosend actions, retries occur after the `Autosend Restart` time (in minutes) has elapsed. For periodic actions, retries occur at the next scheduled time that falls after the `Autosend Restart` time.

By default, when some actions fail (both autosend and periodic), the user is instructed to correct the action and either run it interactively or restart the schedule. Select this option to avoid this manual intervention.

Possible values: `On` or `Off`

Default value: `Off`

Run Scheduler Automatically At Startup

Select this option to run scheduled actions at start up. For synchronized systems, also called a *cluster*, selecting this option ensures that schedulers are synchronized across the cluster.

Possible values: `On` or `Off`

Default value: `On`

Save Messages in Host Files

In addition to the Cleo Harmony log file, messages generated by a specific action are saved in its host file for later recall.

When disabled, the Cleo Harmony application will no longer update host files when an action stops. This may help eliminate periodic host file corruption.

Possible values: `On` or `Off`

Default value: `Off`

Sent/Received Box Archive

Enables automatic archiving of configured host sentbox and receivedbox folders. The Cleo Harmony application checks each enabled host every 15 minutes. As files are archived, a timestamp indicating when the file was originally created is appended to the file name to ensure the archive contains unique files.

When this feature is enabled, files in the sentbox and receivedbox are not set to read-only and conversely when this feature is not enabled, the files in the sentbox and receivedbox are set to read-only.

Possible values: `On` or `Off`

Default value: `Off`

Sent/Received Box Archive After Files

The maximum number of files allowed in the sentbox and receivedbox directory. The Cleo Harmony application will automatically archive the oldest files into the archive subdirectory until n / 2 files remain in the directory.

Setting this value to -1 when the Sent/Received Box Archive option is selected will keep the files copied to the sentbox and receivedbox directories from being set to read-only but archiving of those files will not be done. Please note that an alternative process for archiving these files to manage disk space should be considered.

Possible values: 1-n or -1

Default value: 100

Sent/Received Box Archive Size (mbytes)

The maximum size in megabytes of the files allowed in the sentbox and receivedbox directory. The Cleo Harmony application will automatically archive the oldest files into the archive subdirectory until the size of the files to retain in the directory is less than `n/2` files. This parameter also controls the maximum size of the archive file stored in the archive subdirectory. When this file size is exceeded a new archive file is created.

Possible values: 0.1-n

Default value: 50.0

Sent/Received Box Archive Append To Zip

Determines whether when archiving, compressed file entries will continue to be appended to existing zip files until the maximum archive size is reached; or whether new zip files should be created during each archive cycle. On very busy systems where the number of files to be archived is large, disabling this setting may allow archiving to complete faster, however the resulting zip files may be significantly smaller.

Possible values: `On` or `Off`

Default value: `On`

Show Hidden Panels

Some hosts have configuration panels that are by default hidden from view.

Possible values: `On` or `Off`

Default value: `Off`

Starting Unique File Affix

Text appended to an incoming filename that is repeatedly incremented by 1 until a unique name is found.

This option is not applicable if you choose **Random** for **Unique File Algorithm**.

Possible values: Any numeric text

Synchronized Backup Failover (minutes)

If a production system should go offline, number of minutes that a synchronized backup waits before it switches into a "production" mode.

Possible values: 1-n

Default value: 5

System Administrator Email Address

The value to use as the System Administrator email address. You can specify a comma-, semicolon-, or colon-delimited list of email addresses. If you specify a list, the first address in the list is considered both the FROM and the TO. Subsequent e-mail addresses will only be considered TO. The first e-mail address should be an address internal to the company.

Note: The System Administrator Email Address can be used anywhere where an email address is configured for an email notification by specifying the `%admin%` macro.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons(:). The first address should be an internal email address.

Default value: The email address that may have previously been set in the on the **AS2 Service: AS2** tab. Otherwise it is left empty. See Configuring AS2 Service on page 767.

System From Email Address

The value to use as the FROM address in email sent from the system. If you specify a value, it supersedes the value specified for the **System Administrator Email Address** property. If no value is specified, the system uses the value specified for the **System Administrator Email Address** property.

Possible values: A valid email address.

Default value: None

Timeout For Directory Operations (seconds)

Length of time the scheduler will wait for directory operations (for example, file listing) when pre-checking actions for runnability. If a runnability check exceeds this time due to a nonresponsive file system, the root of the associated directory path is added to a wait list. Once a root (for example, `D:` or `\\filsvr01\folder`) is on a wait list, all subsequent attempts by the scheduler to access any descendent of this path will be bypassed immediately, thereby avoiding large delays due to a nonresponsive file system. The root path will only remain on the wait list for a given period, as specified through the property, **Wait Time For Nonresponsive File Systems (minutes)**.

To disable monitoring of directory operations, set this value to zero (0).

See also Timeout For File Operations (seconds) on page and Wait Time For Nonresponsive File Systems (minutes).

Possible Values: `0 - n`

Default Value: `0`

Timeout For File Operations (seconds)

Length of time the scheduler will wait for file operations (for example, file existence) when pre-checking actions for runnability. If a runnability check exceeds this time due to a nonresponsive file system, the root of the associated directory path is added to a wait list. Once a root (for example, `D:` or `\\filsvr01\folder`) is on a wait list, all subsequent attempts by the scheduler attempts to access any descendent of this path will be immediately bypassed, thereby avoiding large delays due to a nonresponsive file system. The root path will only remain on the wait list for a given period, as specified through the property, **Wait Time For Nonresponsive File Systems (minutes)**.

To disable monitoring of file operations, set this value to zero (0).

See also Timeout For Directory Operations (seconds) on page and Wait Time For Nonresponsive File Systems (minutes).

Possible Values: `0 - n`

Default Value: `0`

Transfer Log Queue Size

The maximum in-memory transfer log queue size. A larger queue allows more time before a database outage adversely affects active and new transfers.

Possible values: 250-n

Default value: 250

Transfer Query Size

The maximum number of results to be returned and displayed when you query transfers. If the number of results returned exceeds this value, the product displays a message to that effect and that you should refine the query to return fewer results.

Minimum value: `10`

Maximum value: no maximum

Default value: `5000`

Unique File Algorithm

Algorithm that determines how incoming files are uniquely named.

- **Increment** - Name files incrementally based on files already in the destination directory.
- **Random** - Names file randomly. If you choose **Random**, **Starting Unique File Affix** is not applicable.

Possible values: Increment

Wait for Dial-up Disconnect Before Exiting

Normally Cleo Harmony will exit without waiting for the Cleo LexiCom dialer to disconnect.

Possible values: `On` or `Off`

Default value: `Off`

Wait Time For Nonresponsive File Systems (minutes)

The length of time a root path will remain on the wait list after a failed attempt (timeout) to access it during scheduler runnability pre-checks. While a root path is on the wait list, any attempt to access it during scheduler pre-checks will fail immediately, thereby avoiding large delays in the scheduler. Once the wait time has expired, assuming the file system problem has been resolved, all future access is restored.

See also Timeout For Directory Operations (seconds) on page and Timeout For File Operations (seconds) on page .

Possible Values: `0 - n`

Default Value: `5`

Zero Byte File Threshold (bytes)

When the **Delete Zero-Length Files** option is enabled, the **Zero Byte File Threshold** determines the minimum file size required for retention. Files smaller than this threshold are considered zero-length and are automatically deleted.

Advanced system options

The **Advanced** tab enables you to set default values for many host-level advanced properties at the system level. Note that if a property is set within this tab, it is only used if the associated host-level setting has **not** been set.

In the web UI, go to **Administration** > **System** > **Advanced**. In the native UI, go to **Options** > **Advanced**.

The **Filter Group** drop-down list allows you to condense the display of properties by selecting a category on which to filter. To further filter the display, enter a case-insensitive string in the **Filter String** field. Note that for the web UI you must press **Enter** after typing a value in the **Filter String** field.

Advanced properties reference

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Repetitive Listener Failures

When "Email On Fail" is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, an email alert will be sent when the failure is resolved. Failure resolution email alerts will not be sent for general Listener failures since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Repetitive System Failures

When “Email On Fail” is enabled and the same system failure occurs (unrelated to an action or inbound Listener message for a specific host), leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. Since it is not possible to determine that a system failure has been resolved, failure resolution email alerts will not be sent.

Note: This feature only suppresses multiple emails if the *same* failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts, nor is supported for host-based actions.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the

failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Repetitive Listener Failures

When `Execute On Fail` is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, the `Execute On Fail` command will be executed again when the failure is resolved. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure. Executions of the "Execute On Fail" command for resolution of general Listener failures will not be done since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Repetitive System Failures

When `Execute On Fail` is enabled and the same system failure occurs (unrelated to an action or inbound Listener message for a specific host), leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed if the failure occurs again. Since it is not possible to determine that a system failure has been resolved, the `Execute On Fail` command will not be executed on resolution of the failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the *same* failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers,

the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512

Default value: System Default

Unzip Use Path

Indicates whether or not zip entry paths should be used for LCOPY -UNZIP operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: On or Off

Default value: On

Wait For Execute On

Indicates whether execution should wait for processing to complete within an Execute On Fail, Execute On Successful Copy, Execute On Successful Receive, or Execute On Successful Send command. Note that this option does not apply to native AS400 execution.

Possible values: On or Off

Default value: On

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If System Default is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

System Default
TripleDES
AES-128
AES-192
AES-256

Default value: System Default

Zip Comment

Specifies the comment to be added to the zip archive file in LCOPY -ZIP operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for LCOPY -ZIP operations. If System Default is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

System Default
9 - (Best Compression)
8
7

6
5
4
3
2
1
0 - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

Network

Network allows you to configure network settings for your Cleo Harmony, Cleo VLTrader, and Cleo LexiCom software. You can configure **Local Listener**, **Clustering**, **Proxies**, **IP Filters**, **Ports**, and **Synchronization** settings in the **Network** menu. The following sections explain these settings and configurations in detail.

Local Listener

The Local Listener receives and handles all inbound requests to Cleo Harmony, Cleo VLTrader, and Cleo LexiCom systems, where the partner or backend system initiates the request.

Once the connection is established, data can flow inbound or outbound.

Inbound requests include unsolicited and asynchronous AS2/HTTP trading partner messages and Cleo Harmony, Cleo VLTrader, and Cleo LexiCom web browser user requests. Inbound requests can also include FTP messages and web service requests.

Configuring the Local Listener

The Local Listener is automatically activated (on HTTP port 5080) the first time the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application is launched. This makes web browser service **(supported only on Unix and Windows platforms)** available out-of-the-box for systems lacking a graphics console. All other services require further user configuration before they are ready and available.

The Local Listener runs with the default, minimal configuration. You can change and save configuration as needed for the AS2 service or other services while the Local Listener is still running and it will remain running as long as it is listening on at least one port. **If you save invalid or incomplete configuration changes, the Local Listener will fail to run the next time it is restarted.**

Configuring a Local Listener for HTTP

The Cleo Harmony application contains an embedded web server for receiving HTTP requests and directing them to the appropriate Cleo Harmony service, based on the requested resource path.

1. Click the **Local Listener** in the tree pane, and then click the **HTTP** tab.
2. Specify parameter values as appropriate.

See HTTP Local Listener reference on page 751 for information about the parameters available.

3. Click **Apply**.

   The values you specified are saved.

HTTP Local Listener reference

Automatically run at startup

Select this check box to have the receiver automatically start each time the Cleo Harmony application is launched.

HTTP

Select the check box to allow remote host or user to send requests over clear-text HTTP.

Port #

Specify a Port number. `5080` is the default for HTTP. Port number `80` is standard for clear-text HTTP. You can also use any other unused port value in the range of `1024 - 65535`. Using non-standard HTTP ports in the range of `1 - 1023` might interfere with port numbers reserved by TCP/IP for other purposes.

You can configure HTTP to listen on multiple ports by separating the field values with commas. For example, suppose you specified port 5080, but you have some trading partners who have outbound firewall restrictions and can only send to port 80. Specifying `5080,80` in the **Port** field allows the firewall-restricted trading partners to be able to send to your server while allowing you to continue to accept inbound messages from your other trading partners on port 5080.

HTTP/s

Select the check box to allow remote host or user to send requests over both clear-text, non-secure HTTP and encrypted HTTP.

Port #

Specify a port number. There is no default for HTTP/s. Port number `443` is standard for HTTP/s and `5443` is suggested. You can also use any other unused port value in the range of`1024 - 65535`. Using non-standard HTTP ports in the range of `1 - 1023` might interfere with port numbers reserved by TCP/IP for other purposes.

You can configure HTTP/s to listen on multiple ports by separating the field values with commas. For example, suppose you specified port 5443, but you have some trading partners who have outbound firewall restrictions and can only send to port 443. Specifying `5443,443` in the Port field allows the firewall-restricted trading partners to be able to send to your server while allowing you to continue to accept inbound messages from your other trading partners on port 5080.

Note: If you enable HTTPs, you must apply an SSL server certificate. If that certificate contains the `keyEncipherment` attribute, the `digitalSignature` attribute must also be used. Otherwise, the Local Listener will not start.

Synchronization Port #

Optional. Specify a TCP/IP port not accessible from outside the customer environment to be used only for synchronizing multiple instances of Cleo Harmony and/or Cleo VLTrader. You can use any port number not already in use, but you can specify only one port.

Note: You are responsible for configuring your firewall so that this port is only accessible from other instances of Cleo Harmony and/or Cleo VLTrader and not from outside your environment.

SSL Server Certificate

If you select **HTTP/s**, select a valid **SSL Server Certificate**. Click **Browse...** to navigate to and select a certificate. Then, enter the **Password** for the SSL Server Certificate's private key.

Authenticate Client

If you select **HTTP/s**, select **Authenticate Client** to require the SSL client to provide a valid certificate during SSL negotiation.

Authentication Certificates

By default, all of the Certificate Manager Trusted CA and user certificates are accepted for client authentication. To change this, use the **Authentication Certificates** button to establish the list of accepted FTP client authentication certificates, which can be:

- all of the local HTTP user certificates and/or
- all or a subset of the trusted CA certificates and/or
- all or a subset of the user certificates.

This option must be decided and agreed upon between trading partners before sending messages via SSL. After changing this setting, stop and restart the VersaLex service or daemon to clear cached SSL sessions.

Optional

If you select **HTTP/s**, select the **Optional** check box to request (but not require) the SSL client to provide a certificate.

Requesting but not requiring client authentication only makes sense if clients can also authenticate by other means (for example, WWW-authentication or signing certificate).

Note: Non-optional client authentication is not compatible with HTTP Portal Applets. The applet will not be able to initialize in the browser without a client certificate. See Configuring access for HTTP host users on page 835.

These settings must be decided and agreed upon between trading partners before sending messages via SSL. After changing this setting, stop and restart the VersaLex service or daemon to clear cached SSL sessions.

Note: If you configure an HSP host, you must either select both the **Authenticate Client** check box and the **Optional** check box or neither. HSP will fail if you select the **Authenticate Client** check box and not the the **Optional** check box.

Exchange Certificates

Click **Exchange Certificates** to send the SSL Server Certificate to your trading partner(s). See Exchanging certificates with your trading partner on page 672 for further information.

Configuring a Local Listener for FTP

The Cleo Harmony and Cleo VLTrader applications contain a full-featured, embedded FTP server for receiving FTP requests.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

FTP clients must present a valid username and password; anonymous logins are not supported. See Configuring local FTP users on page 809 for information about how to configure FTP usernames, passwords, and home directories.

1. Click the **Local Listener** in the tree pane, and then click the **FTP** tab.
2. Specify parameter values as appropriate.

   See FTP Local Listener reference on page 753 for information about the parameters available.
3. Click **Apply**.

   The values you specified are saved.

FTP Local Listener reference

FTP

Select **FTP** to allow FTP clients to send requests over clear-text FTP.

Specify a **Port** number. A value of `21` is the default for FTP. You can also use any other unused port value in the range of `1024 - 65535`. Using non-standard ports in the range of `1 - 1023` might interfere with port numbers reserved by TCP/IP for other purposes.

You can configure FTP to listen on multiple ports by separating the field values with commas. For example, suppose you specified port 5021, but you have some trading partners who have outbound firewall restrictions and can only send to port 21. Specifying `5021,21` in the **Port** field allows the firewall-restricted trading partners to be able to send to your server while allowing you to continue to accept inbound messages from your other trading partners on port 5021.

FTP/s Explicit (AUTH TLS)

Select **FTP/s Explicit (AUTH TLS)** to allow FTP clients to send requests over both clear-text, non-secure FTP and encrypted, secure FTP/s.

Specify a **Port** number. Port number `989` is standard for implicit FTP/s. You can also use any other unused port value in the range of `1024 - 65535`. Using non-standard HTTP ports in the range of `1 - 1023` might interfere with port numbers reserved by TCP/IP for other purposes.

Select **AUTH Required** to allow only encrypted communication on the FTP/s explicit port. This means a client must issue an `AUTH` command to explicitly request security upon connecting or the server will refuse the connection. However, you can configure FTP/s explicit to allow unencrypted communication as well by clearing the **AUTH Required** check box. In this configuration, both clear-text, non-secure FTP and encrypted, secure FTP/s are supported on the same port. Note that this setting has no effect on the plain FTP port or the FTP/s implicit port.

FTP/s Implicit

Select **FTP/s Implicit** to allow FTP clients to send requests over both clear-text, non-secure FTP and encrypted, secure FTP/s.

Specify a **Port** number. Port number `989` is standard for implicit FTP/s. You can also use any other unused port value in the range of `1024 - 65535`. Using non-standard HTTP ports in the range of `1 - 1023` might interfere with port numbers reserved by TCP/IP for other purposes.

SSL Server Certificate

If you select **FTP/s Explicit (AUTH TLS)** or **FTP/s Implicit**, select a valid **SSL Server Certificate**. Click **Browse...** to navigate to and select a certificate. Then, enter the **Password** for the SSL Server Certificate's private key.

Enable Passive Mode

Select **Enable Passive Mode** to configure the FTP server to support both active mode (unlike the command port, the client serves data ports) and passive (or port) mode (like the command port, the server serves data ports).

If you enable passive mode, specify a passive port range using the **Low Port** and **High Port** fields. The FTP server will sequentially cycle through the passive port range while serving data ports during the course of client connections.

Authenticate Client

If you select **HTTP/s**, select **Authenticate Client** to require the SSL client to provide a valid certificate during SSL negotiation.

Authentication Certificates

By default, all of the Certificate Manager Trusted CA and user certificates are accepted for client authentication. To change this, use the **Authentication Certificates** button to establish the list of accepted FTP client authentication certificates, which can be:

- all or a subset of the trusted CA certificates and/or
- all or a subset of the user certificates.

This option must be decided and agreed upon between trading partners before sending messages via SSL. After changing this setting, stop and restart the VersaLex service or daemon to clear cached SSL sessions.

Exchange Certificates

Click **Exchange Certificates** to send the SSL Server Certificate to your trading partner(s). See Exchanging certificates with your trading partner on page 672 for further information.

Configuring a Local Listener for SMTP

The Cleo Harmony and Cleo VLTrader applications contain an embedded SMTP server for receiving email payload.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

1. Click the **Local Listener** in the tree pane, and then click the **SMTP** tab.
2. Specify parameter values as appropriate.

   See SMTP Local Listener reference on page 754 for information about the parameters available.
3. Click **Apply**.

SMTP Local Listener reference

SMTP

Select **SMTP** to allow SMTP clients to send requests over clear-text SMTP.

Specify a **Port** number. Port `25` is standard. You can also use any other unused port value in the range of `1024` - `65535`. Using non-standard ports in the range of `1` - `1023` might interfere with port numbers reserved by TCP/IP for other purposes.

You can configure SMTP to listen on multiple ports by separating the field values with commas. For example, suppose you specified port 5025, but you have some trading partners who have outbound firewall restrictions and can only send to port 25. Specifying `5025,25` in the **Port** field allows the firewall-restricted trading partners to be able to send to your server while allowing you to continue to accept inbound messages from your other trading partners on port 5025.

SMTP/s Explicit (STARTTLS)

STARTTLS Optional

STARTTLS Requied

Select **SMTP/s Explicit (STARTTLS)** and **STARTTLS Optional** to allow clear-text SMTP trades or SSL trades.

Select **SMTP/s Explicit (STARTTLS)** and **STARTTLS Required** to allow only SSL trades.

Specify a **Port** number. Port `25` is standard. You can also use any other unused port value in the range of `1024` - `65535`. Using non-standard ports in the range of `1` - `1023` might interfere with port numbers reserved by TCP/IP for other purposes.

You can configure SMTP to listen on multiple ports by separating the field values with commas. For example, suppose you specified port 5025, but you have some trading partners who have outbound firewall restrictions and can only send to port 25. Specifying `5025,25` in the **Port** field allows the firewall-restricted trading partners to

be able to send to your server while allowing you to continue to accept inbound messages from your other trading partners on port 5025.

SMTP/s Implicit

Select this option to require SMTP/s for all trades.

Specify a **Port** number. Port `25` is standard. You can also use any other unused port value in the range of `1024 - 65535`. Using non-standard ports in the range of `1 - 1023` might interfere with port numbers reserved by TCP/IP for other purposes.

You can configure SMTP to listen on multiple ports by separating the field values with commas. For example, suppose you specified port 5025, but you have some trading partners who have outbound firewall restrictions and can only send to port 25. Specifying `5025,25` in the **Port** field allows the firewall-restricted trading partners to be able to send to your server while allowing you to continue to accept inbound messages from your other trading partners on port 5025.

SSL Server Certificate

If you select **SMTP/s Explicit (STARTTLS)** or **SMTP/s Implicit**, select a valid **SSL Server Certificate**. Click **Browse...** to navigate to and select a certificate. Then, enter the **Password** for the SSL Server Certificate's private key.

Authenticate Client

Select **Authenticate Client** to require the SSL client to provide a valid certificate during SSL negotiation.

Authentication Certificates

By default, all of the Certificate Manager Trusted CA and user certificates are accepted for client authentication. To change this, use the **Authentication Certificates** button to establish the list of accepted FTP client authentication certificates, which can be:

- all or a subset of the trusted CA certificates and/or
- all or a subset of the user certificates.

This option must be decided and agreed upon between trading partners before sending messages via SSL. After changing this setting, stop and restart the VersaLex service or daemon to clear cached SSL sessions.

Exchange Certificates

Click **Exchange Certificates** to send the SSL Server Certificate to your trading partner(s). See Exchanging certificates with your trading partner on page 672 for further information.

Configuring a Local Listener for OFTP

The Cleo Harmony application contains an Odette FTP (OFTP) server which can host either ISDN (Windows users only) or TCP/IP OFTP sessions.

1. Click the **Local Listener** in the tree pane, and then click the **OFTP** tab.
2. Specify parameter values as appropriate.

   See OFTP Local Listener reference on page 755 for information about the parameters available.
3. Click **Apply**.

OFTP Local Listener reference

ISDN

Listen for incoming ISDN connections. ISDN equipment must already be installed and must support the Common ISDN API (CAPI) interface, version 2.0.

My OFTP ISDN Address(es)

If you select ISDN, specify which of your **ISDN Address(es)** you want to use for OFTP. When filling in your ISDN OFTP phone number(s), only specify the local number. Do not include your area code, country code, or

any other prefixes. The phone numbers configured are only used for screening incoming calls. Outgoing calls are automatically referenced by the ISDN layer to your calling number.

Log ignored incoming ISDN calls

Toggles making entries in the system log whenever an incoming ISDN call is ignored.

TCP/IP

Listen for incoming TCP/IP connections.

Specify a **Port** number. By default, the Cleo Harmony application will listen on standard OFTP port 3305, but any port number can be specified.

You can configure **TCP/IP** to listen on multiple ports by separating the field values with commas. For example, suppose you specified port 3305, but you have some trading partners who have outbound firewall restrictions and can only send to port 21. Specifying `3305,21` in the **Port** field allows the firewall-restricted trading partners to be able to send to your server while allowing you to continue to accept inbound messages from your other trading partners on port 3305.

Secure TCP/IP

Listen for incoming secure TCP/IP connections. This is for OFTP2 connections connection using Transport Layer Security (TLS).

Specify a **Port** number. By default, the Cleo Harmony application will listen on standard OFTP port `6619`, but you can specify any other unused port value in the range of `1024 - 65535`. Using non-standard ports in the range of `1 - 1023` might interfere with port numbers reserved by TCP/IP for other purposes.

You can configure multiple ports by separating the field values with commas. For example, suppose you specified port 6619, but you have some trading partners who have outbound firewall restrictions and can only send to port 25. Specifying `6619,25` in the **Port** field allows the firewall-restricted trading partners to be able to send to your server while allowing you to continue to accept inbound messages from your other trading partners on port 6619.

SSL Server Certificate

If you select **TCP/IP** or **Secure TCP/IP**, select a valid **SSL Server Certificate**. Click **Browse...** to navigate to and select a certificate. Then, enter the **Password** for the SSL Server Certificate's private key.

Authenticate Client

Select **Authenticate Client** to require the SSL client to provide a valid certificate during SSL negotiation.

Optional

Select **Optional** to request (but not require) the SSL client to provide a valid certificate during SSL negotiation.

Verify Key Usage

Select **Verify Key Usage** to validate that the SSL client certificate contains the "clientAuth" extended key usage setting.

Authentication Certificates

By default, all of the Certificate Manager Trusted CA and user certificates are accepted for client authentication. To change this, use the **Authentication Certificates** button to establish the list of accepted OFTP client authentication certificates, which can be:

- all or a subset of the trusted CA certificates and/or
- all or a subset of the user certificates.

This option must be decided and agreed upon between trading partners before sending messages via SSL. After changing this setting, stop and restart the VersaLex service or daemon to clear cached SSL sessions.

Exchange Certificates

Click **Exchange Certificates** to send the SSL Server Certificate to your trading partner(s). See Exchanging certificates with your trading partner on page 672 for further information.

Configuring a Local Listener for SSH FTP

The Cleo Harmony and Cleo VLTrader applications contain a full-featured, embedded SSH FTP server for receiving SSH FTP requests. The server supports version 3 of the SSH FTP (SFTP) protocol. The server does not support other SSH requests for shells, port forwarding, etc.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

See Local SSH FTP Users configuration on page 851

1. Click the **Local Listener** in the tree pane, and then click the **SSH FTP** tab.
2. Specify parameter values as appropriate.

   See SSH FTP Local Listener reference on page 757 for information about the parameters available.
3. Click **Apply**.

SSH FTP Local Listener reference

SSH FTP

Allow a client to send SSH FTP requests.

Specify a **Port** number. Port `22` is the standard TCP/IP port for SSH FTP. You can also use any other unused port value in the range of `1024 - 65535`. Using non-standard ports in the range of `1 - 1023` might interfere with port numbers reserved by TCP/IP for other purposes.

SSH FTP Server Private Key(s)

Select one or more valid **SSH FTP Server Private Keys**. Use the table right-click menus and buttons to insert, move, and remove keys in the list. A valid **Password** is required for each Private Key specified. A key for each supported key algorithm is allowed, which includes `rsa-sha2-512`, `rsa-sha2-256`, `ssh-rsa`, `ssh-dss`, `ecdsa-sha2-nistp256`, `ecdsa-sha2-nistp384`, `ecdsa-sha2-nistp521`, and `ssh-ed25519`.

Note that if an RSA server key is configured, the `ssh-rsa`, `rsa-sha2-256`, `rsa-sha2-512` algorithms are also enabled using that same key. The Local Listener Advanced property, SSH FTP Public Key Pattern, can be used to limit which public key algorithms are offered. For example, setting the property to `[^(?!ssh-rsa $).*]` will result in only the `rsa-sha2-256` and `rsa-sha2-512` algorithms being offered by the server for a configured RSA server key. The order of the keys configured dictates the order of the algorithms presented to clients. Also note that the `ssh-rsa` and `ssh-dss` algorithms are eliminated at runtime in FIPS mode as they are not allowed by FIPS 140-3.

Exchange Certificates

Send the SSL Server Certificate to your trading partner(s). See Exchanging certificates with your trading partner on page 672 for further information.

Configuring Local Listener Responses

You can configure welcome and banner messages to send as part of the response when a client connects to the corresponding server. For FTP, `SYST` command responses can also be customized.

The welcome message is typically used to identify the server software version and for FTP, you can also optionally use it for the `SYST` response. You can use a banner message to send a warning or other information to the client as each connection is established.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

You can use `%date%` and `%time%` macros in both the welcome and banner messages, and the `SYST` responses. Use the `%date[+/-#y][+/-#m][+/-#d][,MacroDateFormat=...]%` and `%time[+/-#h][+/-#m][+/-#s][,MacroTimeFormat=...]%` variants of the macros. Otherwise, the default formats of `yyyyMMdd` (date) and `HHmmssSSS` (time) will be used. See Using macro variables on page 59.

1. Click the **Local Listener** in the tree pane, and then click the **Responses** tab.

2. Click the tab for the protocol you want to configure a response for. Choose from **HTTP**, **FTP**, **SMTP**, and **SSH FTP**.
3. Enter your custom **Welcome Message**.

   If this field is not configured, the Cleo Harmony application will respond with its software version. For SSH FTP, this field must be less than 128 characters.
4. Enter a custom **Banner Message**.

   For FTP and SMTP, the banner message you configure precedes the welcome message in a multiline response. For SSH FTP, a configured banner message is sent to the client during authentication. If this field is not configured, no banner message is sent.

   Note: Banner messages are not supported for HTTP.
5. Enter a custom **SYST Response (FTP Only)**.

   Select the **Use Welcome Message for SYST Response** option to use the welcome message for the `SYST` response. Otherwise, enter a custom `SYST` response.

   If this field is not configured, the VersaLex application will respond with the server's operating system and FTP server version.
6. Click **Apply**.

Configuring certificates for Local Listener

Define Local Listener default signing and encryption certificates for applicable services, for example, AS2 or ebXML.

1. Click the **Local Listener** in the tree pane, and then click the **Certificates** tab.
2. Specify parameter values as appropriate.

   See Local Listener Certificates reference on page 758 for information about the parameters available.
3. Click **Apply**.

   The values you specified are saved.

Local Listener Certificates reference

Signing Certificate Alias

The name of the signing certificate registered with the Cleo Harmony application through the Certificate Manager. The certificate must be the same as the one exchanged with your remote trading partners, unless you want to override it at the Mailbox level. See Configuring local FTP users on page 809.

Click **Browse** to view and select a certificate. Enter the **Password** for your signing certificate's private key.

Encryption Certificate Alias

The certificate for decrypting your trading partner's messages, if you have created or obtained a separate certificate.

Click **Browse** to view and select a certificate. Enter the **Password** for your encryption certificate.

Use signing certificate

Select this check box to use the same certificate for signing and decrypting your trading partner's messages. The **Encryption Certificate Alias** and **Password** are populated to match the **Signing Certificate Alias** and disabled.

Exchange Certificates

Click **Exchange Certificates** to send the SSL Server Certificate to your trading partner(s). See Exchanging certificates with your trading partner on page 672 for further information.

Specifying Local Listener advanced properties

Use the **Advanced** tab to specify advanced properties for your listener. Not all properties apply to all protocols. By default, all advanced properties are displayed regardless of the protocols to which they apply. Use the **Filter** drop-drown menu to select a single protocol for which to display advanced properties. In addition, you can specify a string on which to filter the list of properties.

Allow AS2 Identifiers in Actions

When this property is not set, AS2 identifiers are not resolved by checking the commands in the actions. Consequently, AS2 Identifiers that are set in the actions will result in a run-time exception when sending and might result in an unknown trading partner relationship exception when receiving. **Although this value is set to `true` by default, setting this property to `false` might help performance in environments with a large number of hosts and mailboxes.**

Protocols supported: AS2

Archive Automatically After Maximum Receipts

When the number of MDNs in the MDN directory (for example, `as2\mdn` or `as3\mdn`), the number of ACKs in the ACK directory (for example, `ebXML\ack`, `RNIF\ack`, `AS4\receipt`, or `EBICS\ack`), the number of EERPs in the EERP directory (for example, `OFTP\eerp`), or the number of DSNs in the DSN directory (for example, `SMTP\dsn`) exceeds this value (`n`), the Cleo Harmony application automatically archives the oldest receipts into the archive subdirectory until `n/2` receipts remain in the directory. **By default, this value is set to 500.**

Protocols supported: AS2, AS3, AS4, OFTP, RNIF, SMTP, RNIF

Archive File Maximum Size (mbytes)

The maximum size of the receipt archive file stored in the archive subdirectory. When this file size is exceeded, a new, unique archive file is created.

Protocols supported: AS2, AS3, AS4, OFTP, RNIF, SMTP, RNIF

Async Resends

Specifies the number of attempts that will be made to resend an asynchronous transaction that was not completed (that is, an AS2 MDN, ebXML ACK, or OFTP EERP/NERP response has not been received asynchronously) within the specified timeout period.

Protocols supported: AS2, ebXML, OFTP

Async Timeout

The maximum time (in minutes) that the Local Listener will wait for an asynchronous response before either resending the transaction (if AsyncResends > 0) or logging an error.

Protocols supported: AS2, ebXML, OFTP

Auto Accept Received Certificate (CEM)

When selected, automatically accepts all partner certificates sent as part of an inbound Certificate Exchange Message (CEM) request. This setting can be overridden by selecting the **Override Listener CEM Auto Accept Setting** in the desired AS2 host(s). See Auto-accepting inbound EDIINT CEM requests on page 675 for further information. **By default, this property is not selected.**

Protocols supported: AS2

Connection Timeout

The amount of time (in seconds) allowed for each read operation on a connected port. In the Cleo VLTrader and Cleo Harmony applications, this also includes the amount of time allowed for data socket connections.

Protocols supported: All

Do Not Create Inbox Subdirectories For Multipart Payload Files

Indicates, when a multipart payload message is received, whether the payload files should be placed in a date/time stamped subdirectory under the inbox. If a receivedbox is being used, this property also governs the policy for multipart receivedbox payloads.

Protocols supported: AS2, AS4, RNIF, SMTP.

Email And Execute On Unknown Trading Partner Failures

Works in conjunction with the existing `Email On Fail` and `Execute On Fail` properties. When this property is set to `false`, only inbound transfer failures associated with a known mailbox result in email on fail and/or execute on fail being invoked. This eliminates unnecessary emails and executed commands related to cyberattacks, and applies to all local listener protocols and services.

Possible values: `true` or `false`

Default values: `true`

Protocols supported: All

Email Local And Partner Certificate Expiration Notices

When this field is populated, an email notification is sent to all recipients specified in this field when any local user or partner/CA certificates, that is, signing, encryption or packaging certificates (defined at the local listener level and/or those defined at the mailbox level) have expired or will expire within the number of days configured in the **Email Local And Partner Certificate Expiration Warning Days** property.

By default, this value is set to `%admin%`, which points to the System Administrator Email Address defined in the **Other** tab in Configure System Options. See Other system options on page 729 for more information.

When this property is not set, certificate expiration notifications are logged to the System Event log/file instead if errors and warnings are enabled in the **Messages** tab in the native UI and the **Logs** panel in the web UI. See Logs on page 892 for more information.

The frequency of this notification is controlled by the property, **Email Local And Partner Certificate Expiration Notification Frequency Days**.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: All

Email Local And Partner Certificate Expiration Notification Frequency Days

When the **Email Local And Partner Certificate Expiration Notices** property is configured with at least one email address, this property is used to define how often certificate expiration notifications should be sent. The value you specify represents the interval (in days) between notifications. For example, if you specify `4`, notifications are sent every fourth day.

By default, this value is set to `1` so that an email is sent every day. Setting this value to `0` disables notifications, even if the **Email Local And Partner Certificate Expiration Notices** property is configured.

Protocols supported: All

Email Local And Partner Certificate Expiration Warning Days

When the **Email Local And Partner Certificate Expiration Notices** property is configured with at least one email address, this property is used to define the number of days before a certificate is about to expire to trigger sending email warning notifications. **By default, this value is set to 30.**

Protocols supported: All

Email Recipient When Unable To Send Async AS2 MDN

When this property is selected, the Local Listener will attempt to notify the intended recipient of an asynchronous MDN when it is unable to send it via HTTP or HTTP/s.

Email messages may only be returned if the trading partner's raw incoming message contains an HTTP "From:" header and that header contains a valid email address. (The HTTP "From:" header is optional for AS2 and may not always be used or populated with a valid email address.)

Protocols supported: AS2

Email Server Certificate Expiration Notices

When this field is populated, an email notification is sent to all recipients specified in this field when any SSL certificates for HTTPs, FTPs, OFTPs, SMTPs and/or SSH FTP (defined at the local listener level) have expired or will expire within the number of days configured in the **Email Server Certificate Expiration Warning Days** property. By default, this value is set to `%admin%`, which points to the System Administrator Email Address defined in the Other tab in Configure System Options. See Other system options on page 729 for more information.

The frequency of this notification is controlled by the property, **Email Server Certificate Expiration Notification Frequency Days**.

When this property is not set, certificate expiration notifications are logged to the System Event log/file instead if errors and warnings are enabled in the **Messages** tab in the native UI and the Logs panel in the web UI. See Logs on page 892 for more information.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: All

Email Server Certificate Expiration Notification Frequency Days

When the **Email Server Certificate Expiration Notices** property is configured with at least one email address, this property is used to define how often certificate expiration notifications should be sent. The value you specify represents the interval (in days) between notifications. For example, if you specify `4`, notifications are sent every fourth day.

By default, this value is set to `1` so that an email is sent every day. Setting this value to `0` disables notifications, even if the **Email Server Certificate Expiration Notices** property is configured.

Protocols supported: All

Email Server Certificate Expiration Warning Days

When the **Email Server Certificate Expiration Notices** property is configured with at least one email address, this property is used to define the number of days before a certificate expires to send email warning notifications. By default, this value is set to `30`.

Protocols supported: All

FTP Idle Timeout

The amount of time (in seconds) allowed between each FTP command.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: FTP, SSH FTP

FTP UTF8 Pathnames

Indicates to support UTF8 pathnames. When enabled, UTF8 included in response to FEAT command.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: FTP

Ignore RNIF Attachments

Indicates whether attachments to received RNIF messages should be ignored. If selected, only the payload is extracted into the inbox and attachments are ignored.

Protocols supported: RNIF

Incoming Connection Backlog Size

This is the network socket backlog size per listening port. There is a handshake that the client and server go through to set up a connection, which allows the server to then accept the connection, and this backlog setting is the queue size for incoming connections that are in the process of being accepted. The larger the backlog size, the larger number of connections that can be in the process of being accepted at the same time. Connections that are not accepted result in a connection refused on the client side.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: AS2, AS3, AS4, ebXML, FTP, HSP, HTTP, RNIF, SMTP, SSH FTP

ISDN Controllers

For those cases where is it is not possible through CAPI to ascertain the number of available controllers or the available controller number list is not sequential starting at 1. When necessary, property accepts comma-separated values, as well as dash-separated ranges.

Protocols supported: OFTP

Local Bind Address

When specified, all listening server ports for HTTP, FTP (Cleo VLTrader and Cleo Harmony applications only), OFTP, SMTP (Cleo VLTrader and Cleo Harmony applications only) and SSH FTP (Cleo VLTrader and Cleo Harmony applications only) will bind only to this address. By default, this field is blank designating that the Cleo Harmony application will bind its listening ports to all addresses available to the server.

Protocols supported: All

Log Received Message Details

When this property is selected, additional information about the incoming message, i.e., whether it is signed, encrypted and compressed is logged.

Protocols supported: AS2, AS3, AS4, ebXML

Maximum Allowed CEM Response Days

The maximum number of days allowed for receiving a partner response when sending a set of certificates via Certificate Exchange Messaging (CEM) before the request is expired. By default, this value is set to 7 days.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: AS2

Maximum Concurrent FTP Logins Per User

The total number of logins allowed at any one time for any user. With the default value of 0, the number of concurrent connections per user will be limited to the **Maximum Concurrent FTP Users** mailbox setting.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: FTP, SSH FTP

Maximum Concurrent FTP Users

The total number of active FTP users allowed at any one time.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: FTP, SSH FTP

Number Days Before Auto Delete Files In Local User Sent/Receivedbox

If a sentbox and/or receivedbox is configured for local FTP, HTTP, or SSH FTP users, files not already deleted by the client will be automatically deleted after this many days. **By default, this value is set to 7 days.** A value of 0 turns off automatic deletion.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: FTP, HTTP, SSH FTP

Number Of Passwords Before Repeats Allowed

Specifies the number of previous passwords that cannot be used when changing the password for a local user.

Omit Domain Names From Message IDs

By default, message IDs for outbound messages are constructed to include the full domain name from which it is being sent. Select this option if you do not want to include the name of your full domain as part of the message.

Note: This property may have slightly different implementations for each protocol.

Protocols supported: AS2, AS3, AS4, ebXML, RNIF, SMTP

Proxy Protocol: Regex To Match Load Balancer

Specify a regex value for this property to cause the application to look for the Proxy Protocol header on all TCP traffic from IPs that match the specified value.

For example, if you set the value to `172.163.23.225`, the application will expect the proxy protocol header on all TCP traffic from that IP.

To match all IPs in the CIDR blocks, `172.31.48.0/24`, `172.31.49.0/24`, and `172.31.50.0/24` you could specify the following:

```
172\.31\.(48|49|50)\.([0-9]|[1-9][0-9]|1([0-9][0-9])|2([0-4][0-9]|5[0-5]))
```

Save Sent Receipt

Specifies that a copy of all receipts sent to your trading partners will be saved in the sent folder (that is, `AS2\mdn\sent`, `AS3\mdn\sent`, `AS4\receipt\sent`,`ebXML\ack\sent`, `OFTP\eerp\sent`, `RNIF\ack\sent`, `SMTP\dsn\sent`, `EBICS\ack`).

Note: This is a Cleo LexiCom-only option. For Cleo VLTrader and Cleo Harmony, sent receipts are always saved.

Note: For AS2, within Cleo LexiCom, receipts are always retained in the `AS2\mdn\sent` folder for 24 hours to allow for possible retransmission of a previously sent MDN when a duplicate message is received.

Send '200 OK' For Empty AS2 Responses

By default, when either no MDN is specified or an asynchronous MDN is requested and there is no content to return, a `204 No Content` is returned by the Local Listener. Selecting this option returns a `200 OK` response and `200 OK` in the content of the response instead.

Protocols supported: AS2

SMTP Payload Resend Delay

The time (in minutes) that the Local Listener will wait before either trying to resend an SMTP message to one or more multiple recipients that had previously failed to be sent (if SMTP Payload Resend Duration has not expired) or logging an error.

Protocols supported: SMTP

SMTP Payload Resend Duration

The maximum time (in minutes) that the Local Listener will continue to attempt to resend the original SMTP message when it had previously failed to be sent to one or more multiple recipients.

Protocols supported: SMTP

SMTP Receive DSN Timeout

The time (in minutes) that the Local Listener will wait for a delivery status notification before either resending the original message (if SMTP Payload Resend Duration has not expired) or logging an error.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: SMTP

SMTP Send DSN Retry Delay

The time (in minutes) that the Local Listener will wait before either trying again to send a DSN that previously failed to be sent (if SMTP Send DSN Retry Duration has not expired) or logging an error.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: SMTP

SMTP Send DSN Retry Duration

The maximum time (in minutes) that the Local Listener will retry sending a DSN.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: SMTP

SSH FTP Ciper Pattern

Regular expression (enclosed in brackets) that limits the set of cipher algorithms available for all listening SSH FTP server ports. The [List] button shows the resulting set of cipher algorithms for this property setting.

Example values include:

- `[.*]` - All supported cipher algorithms
- `[.*cbc.*]` - Only supported cipher algorithms containing ‘cbc’ in the name.
- `[((?!cbc).)*]` - All supported cipher algorithms except those containing ‘cbc’ in the name.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: SSH FTP

SSH FTP Compression

When this property is selected the SSH FTP server will enable supported compression algorithms. The default setting disables compression algorithms.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: SSH FTP

SSH FTP Key Exchange Pattern

Regular expression (enclosed in brackets) that limits the key exchange algorithms available for all listening SSH FTP server ports. The **List** button shows the resulting set of key exchange algorithms for this property setting.

Example values include:

`[.*]` - All supported key exchange algorithms

`[.*group14.*]` - Only supported key exchange algorithms containing `group14` in the name, for example, `diffie-hellman-group14-sha1`.

`[((?!group14).)*]` - All supported key exchange algorithms *except* those containing `group14` in the name

`[.*curve.*]` - Only support `curve25519-sha256@libssh.org` key exchange algorithm

`[((?!sha1).)*]` - Do not support algorithms containing `sha1` in the name, that is, `diffie-hellman-group1-sha1` and `diffie-hellman-group14-sha1`

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: SSH FTP

SSH FTP MAC Pattern

Regular expression (enclosed in brackets) that limits the set of MAC algorithms available for all listening SSH FTP server ports. The [List] button shows the resulting set of MAC algorithms for this property setting.

Example values include:

`[.*]` - All supported MAC algorithms

`[.*sha1.*]` - Only supported MAC algorithms containing `sha1` in the name.

`[((?!sha1).)*]` - All supported MAC algorithms except those containing `sha1` in the name.

Protocols supported: SSH FTP

SSH FTP Public Key Pattern

Regular expression (enclosed in brackets) that limits the public key algorithms available offered by the server for configured server keys. The [List] button shows the resulting set of public key algorithms for this property setting.

Examples:

- `[.*]` - All supported algorithms
- `[^(?!ssh-rsa$).*]` - The `ssh-rsa` algorithm is not included.

Protocols supported: SSH FTP

SSH FTP Window Size

Specifies the maximum number of received bytes allowed before a window adjustment is required. A large window size may significantly increase memory requirements if there are numerous large file transfers occurring concurrently. If VLProxy is used as a SSH FTP reverse proxy, this parameter will also affect VLProxy memory requirements. When receiving (client uses a PUT command), a typical SSHFTP Window Size setting would be equal to the largest expected file size or the default setting, whichever is greater. This setting will not normally affect sends since the receiver (the client) requires the majority of adjustments.

Note: This is a Cleo VLTrader and Cleo Harmony option.

Protocols supported: SSH FTP

SSL Allow Legacy Renegotiation

When this property is selected (default value), legacy renegotiation will be allowed. If this property is not selected, the extension described in RFC5746 will be used for renegotiation and any SSL clients must also support this extension. See RFC5746 for a description of the extension and the vulnerability it addresses.

Protocols supported: AS2, AS3, AS4, ebXML, FTP, HSP, HTTP, OFTP, RNIF, SMTP

SSL Cipher Pattern

Regular expression (enclosed in brackets) or wildcard expression that limits the set of SSL ciphers available for all listening secure server ports. SSL Cipher Pattern works in conjunction with certificates for all the applicable SSL servers, the SSL Ciphers setting, and the SSL Minimum Encryption Key Size setting. The **List** button shows the resulting set of ciphers for the applicable SSL server certificates and these three property settings.

Protocols supported: AS2, AS3, AS4, ebXML, FTP, HSP, HTTP, OFTP, RNIF, SMTP

SSL Ciphers

Specifies the list of ciphers available for all listening secure server ports (HTTP, OFTP, and, for Cleo VLTrader and Cleo Harmony applications, FTP and SMTP).

- Default Set (default value) – All standard ciphers excluding anonymous (DH_anon) and non-encrypting (NULL) ciphers.
- All Implemented – All standard ciphers including anonymous (DH_anon) and non-encrypting (NULL) ciphers.

Protocols supported: AS2, AS3, AS4, ebXML, FTP, HSP, HTTP, OFTP, RNIF, SMTP

SSL Ignore Client Cipher Preference Order

Protocols supported: AS2, AS3, AS4, ebXML, FTP, HSP, HTTP, OFTP, RNIF, SMTP

SSL Maximum Protocol Version

Specifies the maximum protocol version allowed for all listening secure server ports (HTTP, OFTP, and, for Cleo VLTrader and Cleo Harmony applications, FTP and SMTP). By default, this field is blank designating that the Cleo Harmony application will select the most recent version (currently TLS 1.3).

SSL 3.0 - refer to RFC6101

TLS 1.0 (SSL 3.1) - refer to RFC2246

TLS 1.1 (SSL 3.2) - refer to RFC4346

TLS 1.2 (SSL 3.3) - refer to RFC5246

TLS 1.3 - refer to RFC8446

Protocols supported: AS2, AS3, AS4, ebXML, FTP, HSP, HTTP, OFTP, RNIF, SMTP

SSL Minimum Encryption Key Size

Specifies the minimum encryption key size allowed for all listening secure server ports (HTTP, OFTP, and, for Cleo VLTrader and Cleo Harmony application, FTP and SMTP). To prevent use of low- or medium-strength ciphers, change from the default value of `0` to `112`, `128` or `256` (depending on the requirement). Note that if this value is set too high, all ciphers are filtered out causing the `No suitable cipher suites are enabled` exception to occur.

Protocols supported: AS2, AS3, AS4, ebXML, FTP, HSP, HTTP, OFTP, RNIF, SMTP

Possible values: `0` - `n` bits

Default value: `0`

SSL Minimum Protocol Version

Specifies the minimum protocol version allowed for all listening secure server ports (HTTP, OFTP, and, for Cleo VLTrader and Cleo Harmony applications, FTP and SMTP). SSL 3.0 is the default value for compatibility with clients that do not support the more recent TLS versions 1.0, 1.1, 1.2, and 1.3.

SSL 3.0 (default value) - refer to RFC6101

TLS 1.0 (SSL 3.1) - refer to RFC2246

TLS 1.1 (SSL 3.2) - refer to RFC4346

TLS 1.2 (SSL 3.3) - refer to RFC5246

TLS 1.3 - refer to RFC8446

Protocols supported: AS2, AS3, AS4, ebXML, FTP, HSP, HTTP, OFTP, RNIF, SMTP

SSL Use Record Splitting

Indicates whether to use 1/n-1 record splitting in CBC mode as a countermeasure against the Rizzo/Duong BEAST (Browser Exploit Against SSL/TLS) attack against the SSL 3.0 / TLS 1.0 protocol. Must be turned off if the SSL library on the other side of the connection does not support the feature.

Possible values: `On` or `Off`

Default value: `On`

Protocols supported: AS2, AS3, AS4, ebXML, FTP, HSP, HTTP, OFTP, RNIF, SMTP

Store Raw Received Message

When this property is selected, raw received messages, along with possible sent responses, will be saved in the protocol's received directory (that is, `AS2\received`, `AS3\received`, `AS4\sent+received`, `ebXML\sent+received`, `OFTP\received`, `RNIF\sent+received`, or `SMTP\received`) under the Cleo Harmony root path. These files may be useful in diagnosing problems, but it may be desirable to disable this setting when disk space needs to be conserved.

Protocols supported: AS2, AS3, AS4, ebXML, OFTP, RNIF, SMTP

Unknown Partner Message Action

Determines the desired action to be taken when a message is received by an unknown or undefined trading partner.

For AS2/AS3, the Cleo Harmony application determines valid trading relationships via the defined "AS2-To"/"AS3-To" and "AS2-From"/"AS3-From" headers configured at the Mailbox level.

For ebXML, the Cleo Harmony application determines valid trading relationships via the configured "CPA Id" at the host level.

For AS4, the VersaLex application determines trading relationships via the configured **PMode.Initiator.Party and PMode.Responder.Party**.

This setting may help filter out unwelcome messages.

Choose from the following actions:

- **Save Payload** - The incoming payload is stored in the lostandfound\ directory if the message can be successfully decrypted (when applicable). For AS2/AS3, if the sending system requested an MDN, an unsigned MDN is returned with an explanation of the error. **This is the default setting.**
- **Save Raw Message** - The raw received message is stored in the protocol's received directory as described for the **Store Raw Received Message** property (above). No payload is stored, even if the message can be successfully decrypted (when applicable). For AS2/AS3, if the sending system requested an MDN, an unsigned MDN is returned with an explanation of the error.
- **Ignore** - The sending system receives a valid response code without any explanation of the error, even if the sending system requested an MDN (for AS2/AS3). No message or payload is stored on the receiving system.
- **Reject** - Disconnect from the sending system before completing receipt of the entire message entity. No message or payload is stored on the receiving system.

Protocols supported: AS2, AS3, AS4, ebXML

Local Listener AS2 Service

Configure the AS2 service primarily at the parent Local and the trading partner AS2 remote hosts levels.

See Configuring a Local Listener for OFTP on page 755 and Specifying Local Listener advanced properties on page 759.

Configuring AS2 Service

1. Expand the **Local Listener** node in the tree pane and then click the **AS2** node.

2. Specify parameter values as appropriate.

   See Local Listener AS2 Service reference on page 768 for information about the parameters available.

3. Click **Apply**.

Local Listener AS2 Service reference

Resource Path

Defaults to `/as2`. Your trading partners must include this resource path in the URL when sending AS2 messages. You can change it at any time, but it must start with a forward slash (/) character. If you specify just a forward slash (/), the AS2 service is considered the default HTTP service, and any received message not matching any other HTTP service's resource path is automatically piped to the AS2 service. (This is primarily for compatibility with previous versions of the Cleo Harmony application, which did not make use of resource paths for incoming messages.)

My External Address

The IP address used to access your computer or server from the Internet. This is the address where the Cleo Harmony application is installed and running.

This can be either a fully qualified host name (recommended) or a static visible external IP address.

You can use the **Set Address** button to set your external IP address.

Contact your systems administrator if you do not know your external IP address or fully qualified host name.

Advanced Feature: When you want an asynchronous MDN and you are using inbound port mapping on your firewall, you can specify the port where asynchronous MDNs should be received in the **My External Address** field. Enter the value in the form, `address:port`, for example, `CLEO.DFICOMM.COM:80`. This allows the asynchronous MDN requests to set the correct external address:port without adding/enabling that port in the Local Listener.

Note: This entry will be overridden if you specify a non-zero **Async MDN Preferred Port** for the specific trading partner. See AS2 Host: Advanced Tab on page 152.

MDN Storage Folder

The folder where Message Disposition Notifications (MDNs) are stored. By default this directory is pre-defined to be a subdirectory under the Cleo Harmony directory tree. Click **…**, navigate to a new path and folder, and click **Apply**.

Generate Filename Preservation MDN Responses

Select the **Generate Filename Preservation MDN Responses** option if you choose to check for duplicates of the same file name received from a specific trading partner. When selected, duplicate file names received from a particular trading partner within a desired number of hours, specified with the **Retain Filename History** property (the default value is 24 hours), will generate either a warning or error disposition in the MDN returned to the trading partner, depending on the setting of the **Duplicate Filename Action**. See AS2 Host Configuration on page 148 for detailed information on the usage of the Filename Preservation feature.

Restarts Storage Folder

The **Restarts Storage Folder** is used as a temporary working directory for incoming files. If a trading partner requests a restart of a previous incomplete transfer, the file restart position is determined based on the temporary payload and corresponding property file in this directory. The temporary payload files are encrypted and the restart files are cleared once the transfer completes or 24 hours has passed. If the Cleo Harmony application is being synchronized, the **Restarts Storage Folder** should be set to a **shared location between all the synchronized VersaLexes** because restart requests could come to any Cleo Harmony instance.

Retain Message ID History

The number of days message ID history is retained for checking for and reporting duplicate messages (with the same Message-ID header value) from your trading partners. The default is 5 days.

Working with MDNs

A *message disposition notification* (MDN) is an acknowledgment sent in response to an AS2 message.

Use the **MDNs** tab to view MDNs received by remote hosts.

View the details of any particular MDN entry in the table by either right-clicking on a specific row and choosing **Display** from the pop-up menu, or by double-clicking on any row to display a detail window containing the contents of the MDN:

The Cleo Harmony, Cleo VLTrader, and Cleo LexiCom applications append tracking information to the MDN, including the Message Integrity Check (MIC) value it computed, the name of the file, and the date and subject of the message that was sent. It also includes information about the sender and recipient of the message and how the message was assembled, for example, whether it was signed, encrypted, compressed, and so on.

Use the **Copy** button to copy MDN information to the clipboard. Use the **Print** button to print MDN information. Alternatively, right-click an MDN entry and select **Print** from the menu.

Resending or canceling a pending message

When a message has been sent requesting an asynchronous MDN, its initial **Status** is **Pending**. It will remain in this status until either the asynchronous MDN is returned or the values of the Async Timeout and Async Resends have been exhausted. See Specifying Local Listener advanced properties on page 759.

You can resend or cancel MDN entries with a status of **Pending**.

1. Right-click the message you want to resend or cancel.
2. Choose one of the following:
   - **Resend Now** - resend the message to your trading partner. This can only be done before the asynchronous timeout has expired.
   - **Cancel** - remove the associated files in the `AS2\unsent` folder, change the status of the message to `User Cancelled`, and stop any additional resend attempts. Use this option when it is clear that the asynchronous MDN will not be returned.

Filtering the MDN list

Use the **Status** drop down menu to filter the MDN entries displayed. By default, the filter is set to **Any** and all MDNs are displayed. If no entries match the filter, no MDNs entries are displayed.

Archiving MDNs

You can manually archive MDN files from the **MDNs** tab. The Cleo Harmony, Cleo VLTrader, and Cleo LexiCom applications store archived MDN files as `mdn.zip` files in the `AS2\mdn\archive` directory.

1. Hold down the **Ctrl** key and click rows to select them. Alternatively, select a series of rows by holding down the **Shift** key and selecting the first and last row.
2. While still holding down the **Ctrl** or **Shift** key, right-click to display the menu.
3. Release the **Ctrl** or **Shift** key and select **Archive** from the menu.

   Note: For the web UI, it is particularly important to release the **Ctrl** or **Shift** key prior to making the menu selection, as keeping it depressed could invoke another browser tab.

   The files are stored in compressed/zip format in the `AS2\mdn\archive` directory. Files included in the archive are removed from the `AS2\mdn` directory and the MDNs are removed from the display.

   The Cleo Harmony, Cleo VLTrader, and Cleo LexiCom applications also automatically archive MDNs after a specified number has been received. Set this value in the **Archive Automatically After Maximum Receipts** field on the **Local Listener Advanced** tab. See Specifying Local Listener advanced properties on page 759.

Local Listener AS3 Service

Configure the AS3 service to send and receive secure EDIINT messages through the FTP protocol.

Configuring AS3 Service

1. Expand the Local Listener node in the tree pane and then click the AS3 node.
2. Specify parameter values as appropriate.

   See Local Listener AS3 Service reference on page 770 for information about the parameters available.
3. Click **Apply**.

Local Listener AS3 Service reference

My External Address

The IP address used to access your computer or server from the Internet. This is the address where the Cleo Harmony application is installed and running.

This can be either a fully qualified host name (recommended) or a static visible external IP address.

You can use the **Set Address** button to set your external IP address.

Contact your systems administrator if you do not know your external IP address or fully qualified host name.

Alternatively, select the **Use 'My External Address' From AS2 Service** check box. The value from the AS2 Service panel will automatically be set in this field. This is the default setting.

Note: Since the External Address is only used by FTP Server, LexiCom users will always use the same External Address as defined for AS2 and will be able to change it.

MDN Storage Folder

The folder where Message Disposition Notifications (MDNs) are stored. By default this directory is pre-defined to be a subdirectory under the Cleo Harmony directory tree. Click **…**, navigate to a new path and folder, and click **Apply**.

Retain Message ID History

The number of days message ID history is retained for checking for and reporting duplicate messages (with the same Message-ID header value) from your trading partners. The default is 5 days.

Working with MDNs

You can view MDNs received by remote hosts using the **MDNs** tab.

To view the details of any particular MDN entry in the table, either right-click on a specific row and choose the **Display** option, or double-click on any row to get a detail window containing the contents of the MDN.

The Cleo Harmony application appends tracking information to the MDN, including the Message Integrity Check (MIC) value it computed and the name of the file and the date and subject of the message that was sent. It also includes information about the sender and recipient of the message and how the message was assembled, for example, whether it was signed, encrypted, compressed, and so on.

You can copy this information to the Windows clipboard by clicking **Copy** on the bottom of display window. You can then paste contents, for example, into a new document or an email message. You can also print this information to a networked printer by clicking **Print** on the bottom of the display window, or by selecting any one entry on the MDN display (shown in the previous diagram) and right-clicking it and selecting **Print** from the menu.

Local Listener AS4 Service

Configure the AS4 service to send and receive secure EDIINT messages through the FTP protocol.

Configuring AS4 Service

1. Expand the Local Listener node in the tree pane and then click the AS4 node.
2. Specify parameter values as appropriate.

   See Local Listener AS4 Service - AS4 Tab on page 771 for information about the parameters available.
3. Click **Apply**.

Local Listener AS4 Service - AS4 Tab

Resource path

Defaults to **/as4**. Your trading partners must include this resource path in the URL when sending AS4 messages. You can change it at any time, but it must start with a forward slash (/) character.

Receipts

Storage Folder

The folder where receipts are stored. By default this directory is pre-defined to be a subdirectory under the Cleo Harmony directory tree. Click **…**, navigate to a new path and folder, and click **Apply**.

Perform schema validation on incoming content

Enables schema validation on all AS4 incoming messages. Disable this if your trading partner is not sending compliant XML.

Default value is `true`.

Local Listener AS4 Service - Receipts Tab

The Receipts tab displays a table containing information from recent uploads of User Messages and their associated receipt status. One transaction is stored per row.

To display detailed information about a particular transaction, right-click a row and select **Display** from the menu. If the transaction is complete and a receipt was received, this operation displays the actual receipt. Otherwise, detailed tracking information from User Message INF file is displayed. This includes the `messageId`, the `host/mailbox`, and other useful information.

To manually archive completed transactions, right-click a row and select **Archive** from the menu.

Each row contains the following columns:

Last Activity

Date and time of the last activity related to the transaction.

File Sent

Path and name of the files sent as part of the transaction.

Host

The host from which the User Message was sent.

Mailbox

The mailbox from which the User Message was sent.

Status

Status of the message. Here are some examples of messages and their meanings:

SendingPayload

The User Message is currently being uploaded.

Error

The transaction ended in error.

Exception

The transaction ended with an exception.

Interrupted

The transaction was interrupted by the user.

WaitingForResponse

The User Message has been uploaded to the trading partner, and VersaLex is awaiting an HTTP response.

ReceiptExpected;ReceiptReceived

A receipt was expected (**PMode.ReceptionAwarenss** is `on`), and one was received.

ReceiptExpected;ReceiptNotReceived

A receipt was expected (**PMode.ReceptionAwarenss** is `on`), but one was not received.

ReceiptNotExpected;ReceiptReceived

A receipt was not expected (**PMode.ReceptionAwarenss** is `off`), but one was received.

ReceiptNotExpected;ReceiptNotReceived

A receipt was not expected (**PMode.ReceptionAwarenss** is `off`), and one was not received.

Local Listener ebXML Message Service

Configure your local listener to handle inbound ebXML messages.

Configuring ebXML Message Service

1. Expand the Local Listener node in the tree pane and then click the **ebXML Message Service** node.
2. On the **ebXML** tab in the content pane, specify parameter values as appropriate.

   See Local Listener ebXML Service reference on page 772 for information about the parameters available.
3. Click **Apply**.

Local Listener ebXML Service reference

Resource Path

Defaults to `/ebMS`. Your trading partners must include this resource path in the URL when sending ebXML messages. You can change it at any time, but it must start with a forward slash (/) character.

Acknowledgments: Storage Folder

The folder where Acknowledgments (Acks) are stored. By default this directory is pre-defined to be a subdirectory under the Cleo Harmony directory tree. Click **…**, navigate to a new path and folder, and click **Apply**.

Retain Message ID History

The number of days message ID history is retained for checking for and reporting duplicate messages (with the same Message-ID header value) from your trading partners. The default is 5 days.

Configuring ebXML CPA

A Collaboration Protocol Agreement (CPA) describes the relationship between two parties, typically you and your trading partner. Use the **CPA** tab to provide information about yourself for use in a CPA.

1. Expand the Local Listener node in the tree pane and then click the **ebXML Message Service** node.
2. Click the **CPA** tab in the content pane and specify parameter values as appropriate.

   See Local Listener ebXML CPA reference on page 773 for information about the parameters available.
3. Click **Apply**.

Local Listener ebXML CPA reference

My Party Id(s)

Identifies you to your trading partners. You can list more than one party IDs (URI, email address, DUNS number, etc.) If the type attribute is not included in a party ID, the value must be a URI. If necessary, your normal party ID can be overridden in the ebXML host and mailbox respectively for a specific trading partner.

My Role

Optional field that can help identify your authorized role (for example, buyer, seller, or dealer) usually using a URI. If necessary, your normal role can be overridden in the ebXML host and mailbox respectively for a specific trading partner.

Resource Path

Defaults to `/ebMS`. Your trading partners must include this resource path in the URL when sending ebXML messages. You can change it at any time, but it must start with a forward slash (/) character.

My Service(s)

Messages received from your trading partner must match these values. If you list more than one service, each one must be on its own line. If necessary, your normal services can be overridden in the ebXML mailbox for a specific trading partner.

My Action(s)

Messages received from your trading partner must match these values. If you list more than one action, each one must be on its own line. If necessary, your normal actions can be overridden in the ebXML mailbox for a specific trading partner.

Viewing ebXML acknowledgments

An ebXML acknowledgment is used by a message service handler to indicate that another message service handler has received a message.

1. Expand the Local Listener node in the tree pane and then click the **ebXML Message Service** node.
2. Click the **Ack** tab in the content pane.

   The **Acks** tab displays a list of acknowledgments in a tabular format.
3. Optionally, filter the list of acknowledgements. Select a value from the **Status** menu.

   The list displays acknowledgments whose status matches the value you selected.
4. Display detailed information about a particular acknowledgment. Right-click a row in the table to display a menu and select **Display**. Alternatively, double-click a row.

   The Cleo Harmony application displays the contents of the selected acknowledgment.

   If an acknowledgment has not (yet) been received, the Cleo Harmony application displays message tracking information, including the conversation, message, and CPA IDs, the message time-to-live, the host/mailbox, and the name and location of the file. If the message has errored out, the error code and description is also included.
5. Optionally, copy or print the acknowledgment.

   - **Copy**. You can then paste the contents of the acknowledgment into a new document or an email message, for example.
   - **Print**. Alternatively, you can right-click a row in the acknowledgments table and select **Print** from the drop down menu.

Local Listener fasp Service

Configure the fasp Service to integrate the Cleo Harmony and Cleo VLTrader applications with an Aspera Enterprise Server installation.

Configure this service to log unsolicited file transfers for inbound connections to the Aspera Enterprise Server.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

1. Expand the Local Listener node in the tree pane and then click the **fasp** node.
2. On the **fasp** tab in the content pane, specify parameter values as appropriate.

   See Local Listener fasp reference on page 774 for information about the parameters available.
3. Click **Apply**.

Local Listener fasp reference

Installation Folder

The location of the Aspera Enterprise Server. For Windows, the typical installation location is `C:\Program Files\Aspera\Enterprise Server`.

Management Port

The port the Cleo Harmony or Cleo VLTrader application uses to communicate with the Aspera Enterprise Server.

Unicode Support

Toggles support for files with Unicode filenames.

Local Listener HSP Service

The Cleo Harmony application includes an HSP server that allows HSP clients to send payloads using the HSP protocol.

Configuring Local Listener HSP Service

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

1. Expand the Local Listener node in the tree pane and then click the **HSP** node.
2. On the **HSP** tab in the content pane, specify parameter values as appropriate.

   See Local Listener HSP Service reference on page 774 for information about the parameters available.
3. Click **Apply**.

Local Listener HSP Service reference

Resource Path

Defaults to `/hsp`. Your trading partners must configure this resource path as the `Path` value in the **HSP Host > HTTP** tab. It can be changed at any time, but must start with a forward slash (/).

Local Listener HTTP Service

In addition to the AS2 and ebXML message service protocols (which are layered on top of HTTP and are peer-to-peer protocols), the Cleo Harmony and Cleo VLTrader applications also include an HTTP server that allows straight HTTP clients to send and receive payload.

Trading partners can use a web browser to manually trade with the Cleo Harmony or Cleo VLTrader application or an application (such as the Cleo LexiCom application) to automate trades with Cleo Harmony and Cleo VLTrader systems.

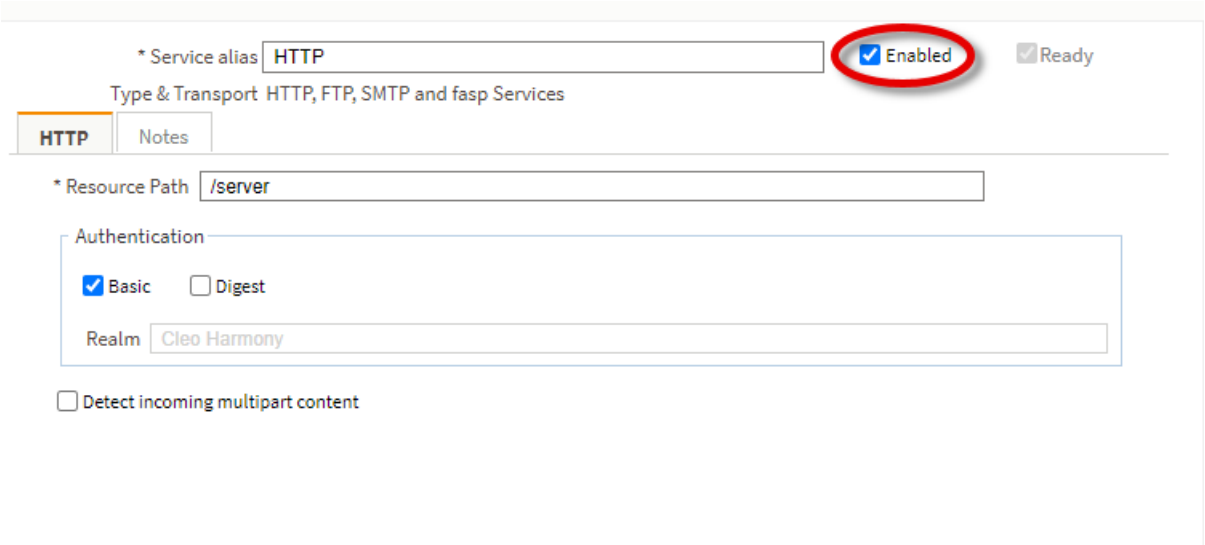
Configuring Local Listener HTTP Service

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

1. Expand the Local Listener node in the tree pane and then click the **HTTP** node.
2. On the **HTTP** tab in the content pane, specify parameter values as appropriate.

See Local Listener HTTP Service reference on page 775 for information about the parameters available.

Note: The HTTP node's Resource Path must be enabled in order to configure Automatic IP Blacklisting. Cleo VLProxy uses the HTTP Resource Path to update the blacklist. See Configuring a blacklist on page 886.



3. Click **Apply**.

Local Listener HTTP Service reference

Resource Path

Defaults to `/server`. Your trading partners must include this resource path in the URL when sending HTTP messages. You can change it at any time, but it must start with a forward slash (/) character.

Authentication

HTTP users can be identified to the Cleo Harmony and Cleo VLTrader applications using either WWW authentication or SSL client authentication. See Configuring HTTP for Local HTTP Mailbox on page 836. WWW authentication is enabled specifically for the HTTP service, while SSL client authentication is enabled for the HTTPs port. See Configuring a Local Listener for HTTP on page 750.

The Cleo Harmony and Cleo VLTrader applications support the **Basic** and/or **Digest Authentication** schemes and both are enabled by default. Normally, basic authentication is passed using an `Authorization: header`, but the Cleo Harmony and Cleo VLTrader applications also support basic authentication using `basicauth= parameter`. The parameter value is in the same format as normal basic authentication (username:password), but can be either clear text or base64-encoded. Please note that when **Digest Authentication** is enabled, password storage will not be as secure as the **Basic Authentication** passwords. With **Basic Authentication**, consider using HTTP/s only. When initially enabling **Digest Authentication**, you will need to update the passwords of the Local HTTP Users in order for the users to be able to log in.

Use the **Authentication Realm** to identify the Cleo Harmony or Cleo VLTrader server/service to the attached client during authentication. The default value is either `Cleo VLTrader` or `Cleo Harmony`, depending on your product.

Detect incoming multipart content

When you select **Detect incoming multipart content** and multiple files are sent to the server, the files are parsed and stored as individual elements. By default, this setting is not enabled and the content is stored as a single entity.

Local Listener RosettaNet Service

The **RossetaNet** tab contains the settings for configuring the RNIF listening service.

Configuring Local Listener RosettaNet Service

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

1. Expand the Local Listener node in the tree pane and then click the **RosettaNet** node.
2. On the **RosettaNet** tab in the content pane, specify parameter values as appropriate.

   See Local Listener RosettaNet Service reference on page 776 for information about the parameters available.
3. Click **Apply**.

Local Listener RosettaNet Service reference

Resource Path

Defaults to `/RNIF`. Your trading partners must include this resource path in the URL when sending RosettaNet messages. You can change it at any time, but it must start with a forward slash (/) character.

Business Identifier

Typically, a DUNS number. Identifies you to your trading partners. You can override this value for a particular trading partner in the mailbox **RosettaNet** tab.

Location Identifier

Optional. Identifies you to your trading partners. You can override this value for a particular trading partner in the mailbox.

Storage Folder

The folder in which Acknowledgments (Acks) are stored. Defaults to a subdirectory under the Cleo Harmony directory tree. You can click **…** to navigate to and choose a new folder. See Working with RosettaNet Acknowledgments on page 776

Retain Message ID History

The number of days the Cleo Harmony application keeps historical data about messages to use when checking for duplicate messages (with the same PIP instance ID header value) from your trading partners. See Working with RosettaNet PIPs on page 776

Working with RosettaNet PIPs

The **PIPs** tab shows the status of currently active and recently completed processes.

The processes in the list are ordered by start time with the oldest process first.

The **Status** column displays the process status. Possible values include **Active** (if currently active), or one of the completed states (**Complete**, **Cancelled**, or an error state)

- Use the **Status** drop-down menu to filter the PIP entries displayed. By default, the filter is set to `Any` and all PIPs are displayed. If no entries match the filter, no PIP entries are displayed.
- To cancel an active process, right-click an active PIP item and select **Cancel** from the drop-down menu.
- To view process details, double-click the process item (or select **Display** from the right-click context menu).

Filtering the PIP list

Use the **Status** drop-down menu to filter the PIP entries displayed. By default, the filter is set to **Any** and all PIP are displayed. If no entries match the filter, no PIP entries are displayed.

Working with RosettaNet Acknowledgments

The **PIPs** tab shows the status of currently active and recently completed processes.

1. The processes in the list are ordered by start time with the oldest process first.

   The **Status** column displays the process status, which will be **Active** if currently active, or one of the completed states (Complete, Cancelled, or an error state).
2. Use the **Status** drop down menu to filter the PIP entries displayed. By default, the filter is set to <Any> and all PIPs are displayed. If no entries match the filter, no PIP entries are displayed.
3. If necessary, cancel an active process. Right click on an active PIP item and select **Cancel** from the drop-down menu.
4. View process details. Double-click the process item or select **Display** from the right-click context menu.

Filtering the RNIF acknowledgment list

Use the **Status** drop-down menu to filter the acknowledgment entries displayed. By default, the filter is set to <Any> and all acknowledgments are displayed. If no entries match the filter, no acknowledgment entries are displayed.

Archiving RNIF acknowledgments

You can manually archive acknowledgment files from the **ACKs** tab. The Cleo Harmony application stores archived acknowledgment files as `ack.zip` file in the `RNIF\ack\archive` directory.

1. Hold down the **Ctrl** key and click the rows you wish to select. Alternatively, select a series of rows by holding down the **Shift** key and selecting the first and last row.
2. While still holding down the **Ctrl** or **Shift** key, right-click to display the menu.
3. Release the **Ctrl** or **Shift** key and select **Archive** from the menu.

   Note: For the web UI, it is particularly important to release the **Ctrl** or **Shift** key prior to making the menu selection, as keeping it depressed could bring up another browser tab.

   The files are stored in compressed/zip format in the `RNIF\ack\archive` directory. Files included in the archive are removed from the `RNIF\ack` directory and the ACK are removed from the display.

   The Cleo Harmony application also automatically archives ACKs after a specified number has been received. Set this value in the **Archive Automatically After Maximum Receipts** field on the Local Listener Advanced tab. See Specifying Local Listener advanced properties on page 759.

Local Listener Odette FTP Service

Configuring OFTP Service

1. Expand the Local Listener node in the tree pane and then click the **OFTP** node.
2. On the **OFTP** tab in the content pane, specify parameter values as appropriate.

   See Local Listener OFTP Service reference on page 777 for information about the parameters available.
3. Click **Apply**.

Local Listener OFTP Service reference

User ID

Password

Default assigned Odette FTP values.

Globally allow Incoming Destination (SFIDDEST) to differ from my User ID (SSIDCODE)

Allows any incoming destination value to be accepted always.

Globally allow Incoming Originator (SFIDORIG) to differ from partner User ID (SSIDCODE)

Allows any incoming originator value to be accepted always.

EERPs Storage Folder

The folder that stores End-to-End-Responses (EERPs) and Negative-End-Responses (NERPs). Defaults to subdirectory under the Cleo Harmony directory tree. You can click **…** to navigate to and choose a new folder.

Retain Message ID History

The number of days the Cleo Harmony application keeps historical data about messages to use when checking for duplicate messages from your trading partners. Default value is 5 days.

Restarts Temp Folder

A temporary working directory for incoming files. If a trading partner requests a restart of a previous incomplete transfer, the file restart position is determined based on the temporary payload and corresponding property file in this directory. The temporary payload files are encrypted, and the restart files are cleared when the transfer completes or 24 hours have passed. If the Cleo Harmony application is being synchronized, the Restarts Temp Folder should be set to a shared location between all the synchronized instances of the Cleo Harmony application because restart requests could come to any Cleo Harmony instance.

Working with OFTP EERPs

Use the **EERPs** tab to view received end responses.

View the details of any particular EERP or NERP entry in the table by either right clicking on a specific row and choosing the **Display** option, or by double-clicking on any row to get a detail window containing the contents of the end response.

If an end response has not (yet) been received, the Cleo Harmony application will display message tracking information, including the virtual filename, date/time, destination, originator, the host/mailbox, and the name and location of the file. If the message has errored out, the error code and description is also included.

This information can be copied to the Windows clipboard by clicking **Copy** at the bottom of display window. The contents can then be pasted, for example, into a new document or an email message. This information can also be printed to a networked printer by clicking the **Print** button on the bottom of the display window, or by selecting any one entry in the EERP table (shown in the previous diagram) and using the **Print** right-click menu option.

1. Click the **EERPs** tab to display a table of responses.
2. Right-click a row to display a drop down menu and select **Display**. Alternatively, double-click a row.

   The Cleo Harmony application displays the contents of the response.

   If an end response has not yet been received, the Cleo Harmony application displays message tracking information, including the virtual filename, date/time, destination, and originator, the host/mailbox, and the name and location of the file. If the message has errored out, the error code and description is also included.
3. If desired, copy or print the response.
   - **Copy**. You can then paste the contents of the response into a new document or an email message, for example.
   - **Print**. Alternatively, you can right-click a row in the response table and select **Print** from the drop down menu.

Filtering EERPs

Use the **Status** drop down menu to filter the EEPRs displayed. By default, the status filter is initially set to `Any` and all EEPRs are displayed. If no entries match the selected status, no EERPs are displayed.

Local Listener SMTP Service

The Cleo Harmony application will process an incoming SMTP MIME message as follows:

- If not a multipart message, the body of the message will be treated as a single file.
- Each part of a multipart message will be treated as a single file. Both inline and attachment disposition types are retained.
- If present, a preamble before the first part of a multipart message will be logged and then discarded. It will not be retained as a file.

Received multipart subtypes mixed, parallel, related, and nested multiparts will all be treated as simply one group of files. Multipart/alternative requires special consideration since duplicate, alternative representations of the same information may be included. Multipart/alternative will be processed as follows:

- If any attachment disposition types are present, these parts are all retained as a group of files and the rest of the multipart/alternative parts are discarded.
- Otherwise, if a text/plain content type is present, this part is retained as a single file and the rest of the multipart/alternative parts are discarded.
- Otherwise, the message data is rejected by the Cleo Harmony SMTP server.

Configuring SMTP Service

1. Expand the Local Listener node in the tree pane and then click the **SMTP** node.
2. On the **SMTP** tab in the content pane, specify parameter values as appropriate.

   See Local Listener SMTP Service reference on page 779 for information about the parameters available.
3. Click **Apply**.

Local Listener SMTP Service reference

My Identification

Domain

User Name

These values comprise your email address, that is `User Name@Domain`.

Acceptable additional incoming receiver usernames

Values recognized as valid `To` values by the Cleo Harmony SMTP server. For these `To` values, the `@Domain` portion must be the same as specified in the **Domain** field. Cleo Harmony and Cleo VLTrader applications only.

Return-Path

Optional - specify an email address or server to which you would like to send any responses, including bounced messages and error messages. The value must be specified as `User Name@Domain`. For the Cleo LexiCom application, the **Return-Path** must be entered to designate the server to receive any responses or error message. The value must be specified as **user@domain**.

Perform reverse DNS lookup

Cleo Harmony and Cleo VLTrader applications only. Select **Perform reverse DNS lookup** if you would like to verify the source domain name of an incoming email.

Allow VERIFY command

Cleo Harmony and Cleo VLTrader applications only. Deselect **Allow VERIFY command** if you do not want your trading partners to be able to specifically verify your email address.

Case sensitive usernames

Cleo Harmony and Cleo VLTrader applications only. Deselect **Case sensitive usernames** if you want to allow your trading partner's incoming email username verification to not be upper/lowercase dependent.

DSNs Storage Folder

Cleo Harmony and Cleo VLTrader applications only. If desired, change the location of the **DSNs Storage Folder**. This folder stores Delivery Status Notifications (DSNs). By default this directory is pre-defined to be a subdirectory under the Cleo Harmony directory tree. To change the location:

1. Click the **...** button.
2. Specify the new path using the directory chooser.
3. Click **Apply**.

Retain Message ID History

Cleo Harmony and Cleo VLTrader applications only. If desired, change the number of days to **Retain Message ID History**. The default is 5 days. This setting is used to check for duplicate messages from your trading partners.

Configuring inbound and outbound media types

Use the **Content** tab to specify acceptable inbound and outbound media types.

A media type can be wildcarded with asterisks (`*`) or question marks (`?`). Multiple media types can be separated by semi-colons (`;`) or commas (`,`) or entered on separate lines. Example values include:

- `*` – any payload media types acceptable
- `*/xml` – all payload media types with subtype `xml` acceptable
- `text/*;image/*` – all payload media types with content-type `text` or `image` acceptable
- `application/edi*` – all payload media types with content-type `application` and subtype starting with `edi` acceptable

To specify separate values for outbound versus inbound, deselect **Same as inbound**.

Working with DSNs

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

You can view received *delivery status notifications* (DSNs) on the **DSNs** tab.

View the details of any particular DSN entry in the table by either right-clicking on a specific row and choosing the **Display** option, or by double-clicking on any row to get a detail window containing the contents of the end response.

If a delivery status notification has not yet been received, the Cleo Harmony or Cleo VLTrader application displays message tracking information, including: the original message-ID, date, subject, and envelope-ID, the Cleo Harmony or Cleo VLTrader host/mailbox, the name and location of the files, and the original recipients. If the message has errored out, the status indicates timeout.

Click the **Copy** button on the bottom of display window to copy DSN information to the clipboard. Click **Print** on the bottom of the display window to print the DSN. Alternatively, right-click an entry in the DSN table and select **Print**.

Filtering the DSN list

Use the **Status** drop-down menu to filter the DSN entries displayed. By default, the filter is set to `Any` and all DSNs are displayed. If no entries match the filter, no entries are displayed.

Archiving DSNs

You can manually archive DSN files from the **DSNs** tab.

1. Hold down the **Ctrl** key and click the rows you want to select. Alternatively, select a series of rows by holding down the **Shift** key and selecting the first and last row.
2. While still holding down the **Ctrl** or **Shift** key, right-click to display the menu.

3. Release the **Ctrl** or **Shift** key and select **Archive** from the menu.

   Note: For the web UI, it is particularly important to release the **Ctrl** or **Shift** key prior to making the menu selection, as leaving it depressed could bring up another browser tab.

   The files are stored in compressed/zip format in the `SMTP\dsn\received\archive` directory. Files included in the archive are removed from the `SMTP\dsn\received` directory and the DSNs are removed from the display.

   The Cleo Harmony application also automatically archives DSNs after a specified number has been received. Set this value in the **Archive Automatically After Maximum Receipts** field on the **Local Listener Advanced** tab. See Specifying Local Listener advanced properties on page 759.

Local Listener Web Browser Service

If licensed, the web browser service is started automatically when the Cleo Harmony service/daemon is started. Through the service, you can access the Cleo Harmony UI or the Cleo VLNavigator UI using a web browser. The web browser service also allows you to access the Cleo VLTrader and Cleo Harmony web portal (see Configuring VLPortal Web Browser service on page 783). This section describes how to setup and configure web browser services. For information regarding the web UI user interface as it applies to both Cleo Harmony, and Cleo VLNavigator, see Using the Web Browser UI on page 34.

For information about current browser support, as well as the required minimum screen resolution, visit Cleo Technical Support and click the **System Requirements** link listed for under your product. Some of the uploading and downloading features within the browser services may require the client to turn off popup blocking.

If a native UI does not exist, you can use command line options to activate the local listener (if not already active) and to modify the HTTP port number.

```
Harmonyc -i "hosts/preconfigured/Local Listener.xml"
```

```
VLTraderc -i "hosts/preconfigured/Local Listener.xml"
```

```
LexiComc -i ".asp/preconfigured/Local Listener.xml"
```

```
Harmonyc -p "Local Listener" -t "<Host><HttpPort>80"
```

```
VLTraderc -p "Local Listener" -t "<Host><HttpPort>80"
```

```
LexiComc -p "Local Listener" -t "<Host><HttpPort>80"
```

The web browser service is not supported on the iSeries (AS/400) platform.

Configuring Cleo VersaLex web browser service

1. Expand the Local Listener node in the tree pane and then click the **Web Browser** node.
2. On the Cleo Harmony tab in the content pane, specify parameter values as appropriate.

   See Local Listener Cleo VersaLex Web Browser Service reference on page 782 for information about the parameters available.
3. Click **Apply**.

Local Listener Cleo VersaLex Web Browser Service reference

Cleo Harmony Resource Path

The check box activates and deactivates access to this resource. It is activated by default.

The default value of the path itself is the product name (for example, `/Harmony`). The path you specify must be included in the URL (for example, `http(s)://VersaLexComputerIP:http(s)Port//Harmony`) when accessing the web UI through a browser. You can change this value at any time, but it must begin with a forward slash (/) character.

If you include the parameter, `transfers`, in the URL (for example, `http(s)://VersaLexComputerIP:http(s)Port/VersaLexResourcePath?transfers`), today's transfer report is automatically displayed. This matches the functionality of the native UI VLStat program.

Access via VLProxy toggles access to the resource through the Cleo VLProxy application. It is selected by default.

Cleo VLNavigator Resource Path

The check box activates and deactivates access to this resource. It is activated by default.

The path you specify must be included in the URL (for example, `http(s)://VersaLexComputerIP:http(s)Port/VLNavigatorResourcePath`) when accessing the web UI through a browser. You can change this value at any time, but it must begin with a forward slash (/) character.

Access via VLProxy toggles access to the resource through Cleo VLProxy. It is selected by default.

Portal Resource Path

The check box activates and deactivates access to this resource. It is activated by default.

Your trading partners must include this resource path in the URL when accessing the Cleo Portal application through a web browser. You can change this value at any time, but it must begin with a forward slash (/) character.

You can customize some aspects of the appearance of the Cleo Portal page. See Customizing your Cleo Portal banner and login page graphics on page 911.

Users must connect on a secure port

Limit users to SSL connections only. When selected, users will be able to successfully authenticate access to the Cleo Harmony and Cleo VLNavigator applications only when an HTTP/s connection is used.

Note: For the Cleo Portal page, this check box is not applicable as the Cleo Portal page *requires* secured access. In fact, if a trading partner attempts to connect on an unsecured channel, the requests will be redirected to a secured channel. If a secured channel is not available, the trading partner will be denied access.

View Only Password

The password to allow view-only access to the Cleo Harmony application through a web browser. The default password is the product serial number. This password can be any combination of letters, numbers, or special characters, but cannot start with an asterisk (*).

Select **Default Mode** to set the default to view-only mode.

Cleo Harmony and Cleo VLTrader applications only: The view-only does not apply when a `VLNavigator` user group is assigned to this instance of the Cleo Harmony or application.

Edit Password

The password to allow full access to the Cleo Harmony application through a web browser. The default password is the product serial number. This password can be any combination of letters, numbers, or special characters, but cannot start with an asterisk (*).

Select **Default Mode** to set the default to edit mode.

Cleo Harmony and only: The edit password does not apply when a `VLNavigator` user group is assigned to this instance of the Cleo Harmony or application.

Default automatic refresh rate

The interval at which the browser session will automatically refresh. The value must be between 5 and 60 seconds. The default value is 15 seconds.

Zip all download files

Toggles compressing/zipping all exported files (for example, certificates) into an archive when downloading through the web UI.

About Default Portal Configuration

Before discussing web portal setup and editing, it is important to understand the default web portal configuration of the web portal provided for you by VersaLex.

VersaLex provides a single, standard portal called **Default Portal** with four standard web pages:

- VLPortal default home page (VersaLex Web Portal)
- Ad hoc file transfer page (Manual File Transfer)
- Transfer reporting page (File Transfer History)
- Help (VersaLex Web Portal Help)

Special rules apply to the **Default Portal**:

- It cannot be removed.
- Its portal ID cannot be modified.

Special rules apply to the standard pages within the **Default Portal**:

- VersaLex Web Portal: except for its page ID, this page can be modified, but it cannot be removed.
- Manual File Transfer and File Transfer History: except for their titles, these pages may not be modified or removed.
- VersaLex Web Portal Help: except for its page ID, this page can be modified, but it cannot be removed.

Web Portals can be displayed in any language(s) most commonly spoken by your users by including a language resource file for each desired language. See Internationalizing your web portals on page 790 for further details.

Configuring VLPortal Web Browser service

Note: This feature is being deprecated. For similar functionality, use Cleo Portal. See Cleo Portal on page 911 for more information.

1. Expand the Local Listener node in the tree pane and then click the **Web Browser** node.
2. On the Cleo Harmony tab in the content pane, specify parameter values as appropriate.

   See Local Listener VLPortal Web Browser Service reference on page 783 for information about the parameters available.
3. Click **Apply**.

Local Listener VLPortal Web Browser Service reference

Resource Path

The check box activates and deactivates access to this resource. Access is activated by default.

The default value of the path itself is the product name (for example, `/VLPortal`). The path you specify must be included in the URL (for example, `http(s)://VersaLexComputerIP:http(s)Port//Harmony`)

when accessing the Cleo VLPortal application through a browser. You can change this value at any time, but it must begin with a forward slash (/) character.

Access via VLProxy toggles access to the resource through the Cleo VLProxy application. It is selected by default.

Application Name

The name used by all your web portals. It is displayed as the title in the browser tab and as part of the titles in the web portal user dialogs. The default value is `VLPortal`.

Web Page Catalog

Displays the **VLPortal Web Page Catalog** dialog box. See Maintaining the VLPortal web page catalog on page 784.

Add custom link to user login page

A hyperlink included on the web portal login page. The value you specify must be a valid URL.

The check box activates and deactivates the feature. This option is deactivated by default.

See Providing access to the web portal on page 793.

You can specify the text describing the link by editing the value for the `VLPortalUI.CustomLink` property in the language-specific `VLPortal_xx.properties` file(s) stored under `webserver\VLPortal\internationalization` in the Cleo Harmony home directory.

Use reCAPTCHA

The check box activates and deactivates the feature. It is activated by default.

The value you specify is the number of failed attempts possible before reCAPTCHA is used. reCAPTCHA is an additional authentication level added for your trading partners when accessing the web portal to keep automated software from engaging in abusive activities on your site. This value defaults to `3`. To enable this feature for all login attempts, set it to `0`.

Web Portals

Displays the list of configured web portals. Each row in the table summarizes one web portal.

The **Portal ID** field specifies a unique identifier for the portal.

The **Language(s)** field specifies the ISO-639-1 language code(s) for the supported language(s) for this portal. English ('en') is provided by default with the Cleo Harmony application. An asterisk (*) next to any of the language codes means configuration of the web portal for that particular language has not been completed. Therefore, users selecting those language-specific portals are not able to access the incomplete web page(s). See Internationalizing your web portals on page 790 for detailed information.

The **Pages** field provides a list of web page IDs that are included with this portal. You can select only one row at a time. From each row's right-click menu, you can:

- **Edit** the web portal. See Editing or creating a web page on page 786.
- **Clone** the web portal. When you select this option, a dialog will be displayed allowing you to edit a new portal using the selected portal as a baseline. See Editing or creating a web page on page 786.
- **Remove** the web portal. If the portal you attempt to remove is referenced in an HTTP user host, you will be asked to confirm the removal. Note that **Default Portal** may not be removed.
- View the HTTP user hosts that reference the portal through the **Where Used...** option. See Viewing a web portal cross reference on page 789.

New Portal...

Create a new web portal from scratch. See Editing or creating a web page on page 786.

Maintaining the VLPortal web page catalog

1. Expand the Local Listener node in the tree pane and then click the **Web Browser** node.

2. On **VLPortal** tab, click **Web Page Catalog...**.

   The **VLPortal Web Page Catalog** dialog box appears.

3. The **Web Pages** table displays the list of current web pages. The **Page ID** field specifies a unique identifier for the page. The **Language(s)** field specifies the ISO 639-1 code(s) for the supported languages configured for this page. See Internationalizing your web portals on page 790 for more information. Only one row can be selected at a time. From each row's right-click menu, you can:

   - **Edit...** the web page. See Editing or creating a web page on page 786.
   - **Remove** the web page. If the page you attempt to remove is referenced within a current web portal, you are asked to confirm the removal. Note that the **File Transfer History**, **Manual File Transfer**, **Cleo Harmony Web Portal**, and **Cleo Harmony Web Portal Help** pages cannot be removed.
   - View the web portals that reference this page through the **Where Used...** option. See Viewing a web page cross reference on page 789.

4. Use **New Page...** to create a new web page from scratch. See Editing or creating a web page on page 786.

5. Use the **Import…** button to import new or modified language resource files to support languages other than English (provided by default with the Cleo Harmony product). After you import a new resource file, it will be displayed in the read-only **Language Resource Files** field. See Internationalizing your web portals on page 790 for further information.

Editing, cloning, or creating a web portal

When you select **Edit...** or **Clone…** from a row in the **Web Portals** table, or when the **New Portal...** button is selected from the **VLPortal** tab, the web portal editor is invoked.

Before discussing web portal editing, it is important to understand the default web portal configuration: the web portal provided for you by the Cleo Harmony application. See About Default Portal Configuration on page 783.

1. The **Portal ID** designates a unique identifier for this portal. This is used as a reference "key" in the **Associated web portal** menu of an HTTP user host (see Local HTTP Users Configuration on page 834).
2. The **Title** field allows you to specify a meaningful string, used primarily for organizing the portals. This value will not be displayed anywhere within the user portal experience.
3. The **Images** section allows you to customize the layout and design of the web portal framework.

   - The **Logo** defaults to `img/defaultlogo.jpg`. This image will be displayed in the upper left-hand corner of each web portal page. It can be changed to any customized image, for example, your company logo.
   - The **Banner** defaults to `img/banner.jpg`. This image will be displayed along the top of each web portal page. It can be changed to any customized image, for example, your company banner. A banner size of approximately 2000w by 84h pixels is recommended.
   - The **Menu** defaults to `img/navpic.jpg`. This image will be displayed just under the main menu, along the left border of each web portal page. It can be changed to any customized image.
   - Use **Import...** to import new graphic images that can subsequently be selected through the **Logo**, **Banner**, and **Menu** fields. All imported files are stored in `webserver\VLPortal\img\` under the Cleo Harmony home directory.

4. Set up the **Navigation Menu** table to establish the pages that should be included in the portal and the order in which they should be organized. Each row in the table represents a single web page. Only one row can be selected at a time. From each row's right-click menu, you can:

   - **Move Up** to move the page up in the menu list.
   - **Move Down** to move the page down in the menu list.
   - **Insert Above...** or **Insert Below...** to insert a new page above/below the current row. When this is selected, the following dialog will be displayed, allowing you to select a web page from the current web page catalog. See Maintaining the VLPortal web page catalog on page 784.

Note: The web page should be configured for all supported **Language(s)**, otherwise the web page will not be displayed for those language-specific users. See Internationalizing your web portals on page 790.

- **Edit...** to edit the selected page. See Editing or creating a web page on page 786.
- **Remove** to remove the selected web page from the navigation menu. This does not remove the page from the web page catalog; it simply removes the page from this portal's navigation menu. Note that all web portals must have at least one web page in their menu; therefore, the last page may not be removed. See Maintaining the VLPortal web page catalog on page 784.
- View the web portals that reference the selected page through the "Where Used..." option. See Viewing a web page cross reference on page 789.

5. Optional - Click **Metadata** to configure a metadata entry form for files the portal user uploads via the applet. See Configuring manual file transfer metadata on page 789.

To see how the fields specified on web portal editor map to an actual web portal layout, see the Sample web portal layout on page 792.

Editing or creating a web page

When you select **Edit** from a row in the **Web Pages** table in the **VLPortal Web Page Catalog** dialog box or in the **Insert Page** dialog box, or when you click **New Page** in the **VLPortal Web Page Catalog** dialog box, the web page editor is invoked.

Before discussing web page editing, it is important to understand the default web portal configuration: the web portal that is provided for you by the Cleo Harmony application. See About Default Portal Configuration on page 783.

Editing a base page

The **Manual File Transfer** and **File Transfer History** pages are referred to as *web portal base pages*. Only the page title and language can be changed for these two base web pages.

1. In the Web Page Catalog dialog box, right-click the web page you want to edit and select Edit from the drop down menu.

   A edit confirmation dialog box appears.
2. In the confirmation dialog box, click **Yes**.

   The **Edit Page** dialog box appears.

   Note: This dialog box is limited in scope for base pages. You can only modify values in the **Language** and **Title** fields.
3. Select a value from the **Language** drop down menu.

   The **Language** drop-down list contains the ISO-639-1 codes associated with language files located in the `webserver\VLPortal\internationalization` directory.
4. Enter a title for the base page in the **Title** field.

   The value you to specify is displayed in the portal navigation menu. It should be of a reasonable length for display within a browser, and it should be entered in the language associated with **Language** drop down menu. If more than one Language has been specified for a web page, deleting the **Title** text removes the value for the selected language. However, for the base pages, you must specify at least one language. See Internationalizing your web portals on page 790 for more information.
5. Optional - Click **Where Used** to display a cross reference of the web portals. See Viewing a web page cross reference on page 789.

Editing a custom or link page

If any page other than a base page is being edited, a full-page editor is displayed. In the editor dialog, choose between a **Custom** or **Link** type of page.

1. In the Web Page Catalog dialog box, right-click the web page you want to edit and select Edit from the drop down menu.

   A edit confirmation dialog box appears.
2. In the confirmation dialog box, click **Yes**.

   The **Edit Page** dialog box appears.

   Note: This dialog box is limited in scope for base pages. You can only modify values in the **Language** and **Title** fields.
3. Select a value from the **Language** drop down menu.

   The **Language** drop-down list contains the ISO-639-1 codes associated with language files located in the `webserver\VLPortal\internationalization` directory.
4. Enter a title for the base page in the **Title** field.

   The value you to specify is displayed in the portal navigation menu. It should be of a reasonable length for display within a browser, and it should be entered in the language associated with **Language** drop down menu. If more than one Language has been specified for a web page, deleting the **Title** text removes the value for the selected language. However, for the base pages, you must specify at least one language. See Internationalizing your web portals on page 790 for more information.
5. Select a page type. Choose one of the following:

   - Select **Custom** to modify your custom-built web page. These are pages that you have created **within** the Cleo Harmony product. For information about custom pages, see About custom pages on page 787.
   - Select **Link** to insert a link directly to any web page that has been built **outside** of the Cleo Harmony product. For information about link pages, see About link pages on page 788.
6. Optional - Click **Where Used** to display a cross reference of the web portals. See Viewing a web page cross reference on page 789.

About custom pages

Page ID

Designates a unique identifier for this page and once created, cannot be edited. It is used as a reference "key" in the web portal navigation menus. See Editing, cloning, or creating a web portal on page 785.

Language

Allows you to tailor the title and content of the custom page on a per-language basis. See Internationalizing your web portals on page 790.

Title

The title you specify is displayed in the portal navigation menu. It should be of a reasonable length for display within a browser. If multiple languages are supported, deleting the value in the **Title** field removes the custom web page for the selected language; however, at least one language must have a title.

If multiple languages are supported, deleting the value in the **Title** field removes the custom web page for the selected language; however, at least one language must have a title.

Section Table

Each row in the table in the main part of the dialog box contains the following columns

Section Text

Represented as heading text on the web page (HTML `<H2>` tag).

Line Break

If selected, represented as a blank line (HTML <BR> tag) on the web page **before** the following **Detail/Link Text**.

Detail/Link Text

Represented in one of two ways on the web page:

- If the **Link** field is empty, **Detail/Link Text** is represented as detailed text.
- If the **Link** field contains a hyperlink, **Detail/Link Text** is represented as an underlined link reference.

Link

Represents an actual hyperlink to be displayed in your custom page.

Use the right-click menu options to manipulate each row. A range of rows can be selected; however, this can only be done within the native UI. When manipulating a range of rows, the **Shift** key must be held down while selecting the right-click menu option. Note that the last row of the table will always be empty.

From each row's right-click menu, you can:

- **Edit Link...** to insert a link or edit the link on the selected row.
  - Select **None** to clear the link.
  - Select **URL** to enter a valid URL (for example, a link to your company's web site).
  - Select **Document** to select a document (for example, a PDF of documentation pertinent to your trading partner).
  - Use **Import...** to import new documents that can subsequently be selected through the **Document** field. All imported files are stored in `webserver\VLPortal\doc\` under the Cleo Harmony home directory.
- **Move Up** or **Move Down** to move the row(s) up or down in the ordering.
- **Insert Above** or **Insert Below** to insert a row above or below the current row.
- **Remove** to remove the selected row(s).

About link pages

Page ID

Designates a unique identifier for this page and once created, cannot be edited. It is used as a reference "key" in the web portal navigation menus. See Editing, cloning, or creating a web portal on page 785.

Language

Allows you to tailor the title and content of the page on a per-language basis. See Internationalizing your web portals on page 790.

Title

The title you specify is displayed in the portal navigation menu. It should be of a reasonable length for display within a browser. If multiple languages are supported, deleting the value in the **Title** field removes the custom web page for the selected language; however, at least one language must have a title.

If multiple languages are supported, deleting the value in the **Title** field removes the custom web page for the selected language; however, at least one language must have a title.

URL

HTML

Specify the target of your link.

URL

Select the radio button and specify a valid URL (for example, a link to your company's web site).

HTML

Select the radio button and specify a valid HTML page. Click **Import** to browse to an HTML page. Files you import are stored in `webserver\VLPortal\html\` under the Cleo Harmony home directory.

- If you choose the HTML option, any images referenced within the HTML file should be placed in `webserver\VLPortal\img\` under the Cleo Harmony home directory. This can be accomplished using the **Import...** button in the **VLPortal Images** dialog box.
- It is your responsibility to ensure that any content and style sheets are compatible with the web portal framework.

For information about how the fields specified on web page editor map to an actual web portal layout, see Sample web portal layout on page 792 .

Viewing a web portal cross reference

When **Where Used...** is selected from a row in the **Web Portals** table, the following dialog is displayed. This dialog identifies the HTTP user hosts that are using this particular web portal. The dialog is used for reference only; no manipulation can be performed from here. For information about how to change a web portal reference for an HTTP user host, see Local HTTP Users Configuration on page 834.

Viewing a web page cross reference

When **Where Used...** is selected from a row in the **Web Pages** table of the VLPortal Web Page Catalog, or **Where Used...** is selected from the Navigation Menu table of the web portal editor, or the **Where Used...** button is clicked in the web page editor, the following dialog is displayed. This dialog identifies the web portals that are including this particular web page. The dialog is used for reference only; no manipulation can be performed from here. For information about how to change a web page reference for a web portal, see Editing, cloning, or creating a web portal on page 785.

Configuring manual file transfer metadata

Configuring metadata allows you to build a form that the user is prompted to fill out when performing uploads from the **Manual File Transfer** page in VLPortal via the applet. The form input is inserted into an XML file that is uploaded inside a zipped archive along with the selected files.

1. From the Web Portal editor (Editing, cloning, or creating a web portal on page 785), click **Metadata**.

   The **Edit Portal Metadata** dialog box appears.

2. Enter information for the metadata file you want to create in the following fields:

   Filename

   Specify the name of the XML file to contain the user-supplied metadata that will accompany the uploaded files.

   Language

   Displays whatever alternative **Label** values have been supplied for the metadata items for the given language. See Internationalizing your web portals on page 790.

3. Add or edit metadata items from the Form Data list.

   If there are no existing metadata items in the Form Data list, click **New Item** to display the **New Metadata Item** dialog box.

   If there are metadata items in the Form Data list, right-click an item and select **Edit** to display the **Edit Metadata Item** dialog box.

   Note: The **New Metadata Item** and the **Edit Metadata Item** dialog boxes contain the same fields.

   a) Enter information about the metadata item in the dialog box.

Label

This label is displayed for this item in the selected language in the form the user is prompted to complete when uploading files. You select a language for the label and enter the label text.

Choices

Indicate the choices available to the user when they provide information about this item. If you provide choices, they are delimited by the '|' symbol. If the user can enter freeform text for the input, leave this field blank.

Element Identifier

The XML attribute for this item's corresponding element in the generated file.

Required

Indicate whether or not a selection/input is mandatory for this metadata item.

b) Click **OK**.

Your changes are saved and the **Edit Portal Metadata** dialog box appears.

4. Optional - Right-click an existing metadata item and select one of the following from the menu:
   - **Move Up** and **Move Down** to change the order in which corresponding fields appear in the form the user is prompted to complete when uploading the file(s).
   - **Edit** to edit the metadata item
   - **Remove** to remove the selected metadata item.
5. Click **OK** to save your changes and return to the **VLPortal** tab.

Internationalizing your web portals

The Cleo Harmony application includes default web portal language support for the English ('en') language; however, additional languages can be configured for the language(s) most commonly spoken by your users. All text displayed within the login page and the web portal base pages (**Manual File Transfer** and **File Transfer History**) is contained within a language-specific resource properties file stored under `webserver\VLPortal\internationalization` in the Cleo Harmony home directory.

The resource files must be specifically named in the format `VLPortal_xx.properties`, where `xx` corresponds to a valid **language code** . These codes must be in lower-case and must correspond to the two-letter "Alpha-2" codes for the specified language, as defined by ISO-639-1. You can find a full list of these codes at http://www.loc.gov/standards/iso639-2/php/English_list.php.

Note: The `VLPortal.properties` file found in the `webserver\VLPortal\internationalization` directory should not be modified. As changes are made to the Cleo Harmony application during product releases, this file could be updated and any changes you make to this file will be lost. Also note that when updates are made to this file (for example, additional field values or sections), those changes will need to be manually migrated into each of the language-specific resource files that you have previously configured.

Adding support for a new language to the base pages

To add support for a new language to the base pages:

1. Create a resource file for each language that you want to support. Use the `VLPortal.properties` file as a template for the desired language. For example, if you want to add web portal Spanish language support (that has the ISO-639-1 language code of 'es'), you would copy the `VLPortal.properties` file (from the `webserver\VLPortal\internationalization` directory) to `VLPortal_es.properties`.
2. Open this newly created properties file in a text editor and translate all the text after the '=' character into the desired language for each property provided in this file. In our example, we are translating to Spanish. Do not add a space after the '=' character.

Example:

The original English translation:

```
# Date Filters
# =============
TransferHistory.Today=today
TransferHistory.Yesterday=yesterday
TransferHistory.Now=now
TransferHistory.DayAgo=day ago
TransferHistory.DaysAgo=days ago
TransferHistory.WeekAgo=week ago
TransferHistory.WeeksAgo=weeks ago
TransferHistory.MonthAgo=month ago
TransferHistory.MonthsAgo=months ago
TransferHistory.YearAgo=year ago
TransferHistory.YearsAgo=years ago
```

The same properties translated to Spanish:

```
# Filtros de fecha
# =================
TransferHistory.Today=hoy
TransferHistory.Yesterday=ayer
TransferHistory.Now=ahora
TransferHistory.DayAgo=día atrás
TransferHistory.DaysAgo=días atrás
TransferHistory.WeekAgo=semana atrás
TransferHistory.WeeksAgo=semanas atrás
TransferHistory.MonthAgo=mes atrás
TransferHistory.MonthsAgo=meses atrás
TransferHistory.YearAgo=año atrás
TransferHistory.YearsAgo=años atrás
```

Note: Any lines preceded by one or more '#' characters is a comment and is ignored by the Cleo Harmony application. These lines are not required to be translated.

3. Import the translated resource file(s) into the Cleo Harmony application using the **Import…** button in the Maintaining the VLPortal web page catalog on page 784 dialog.

   Note: Do not copy the resource file(s) directly into the `webserver\VLPortal\internationalization` directory. In order for the resource file(s) to be properly registered in the Cleo Harmony application, they must be imported. This applies to newly created resource files or modified resource file. In all cases, the files must be imported rather than directly copied.

4. For each web page listed in the VLPortal Web Page Catalog, add an entry for the newly configured language. Right-click each web page entry and select **Edit…**.
   a) If a prompt appears showing the associated web portals and asking if you are sure you want to edit it, select **Yes**.
   b) From the **Language** drop-down selector in the upper-right corner, choose the newly imported language.
   c) Add the page title content in the appropriate language and click **OK**.

> **Note:** At a minimum, the above steps should be performed for the four baseline standard web pages (that is, Cleo Harmony Web Portal, Manual File Transfer, File Transfer History, and Cleo Harmony Web Portal Help). If any of these pages are missing a particular language variant, an asterisk (*) is displayed next to the language in the**Web Portals** table in the **VLPortal** tab.

See Configuring VLPortal Web Browser service on page 783.

5. Additionally, web portal users selecting this language will not be able to view the missing language variants. Further, if all the pages are missing, users will not be able to log into the web portal. When missing pages are encountered, a warning message is logged to the Cleo Harmony console each time the web portal user logs in.
6. If it is necessary to remove a page for a specific language variant and it is not the only language configured for that page:
   a) Edit the desired page.
   b) Select the language variant from the list.
   c) Clear the **Title** text and click **OK**.

      You are prompted to be sure you want to proceed.
   d) Click **Yes** to complete the process.

Adding support for a new language to the help documentation

The text for the web portal help is located in `webserver/web_docs/help/VLPortal`; it is called **VLPortal_Help.html**. You can add support for a new language to the help documentation.

1. Create a new HTML document from `VLPortal_Help.html`. For example, if creating a Spanish language document, create **VLPortal_Help_es.html**.
2. Open the new file in an HTML editor.
3. Translate all the text appropriately.

   If you want to update the screen images as well, use a screen capture application to capture images and name the images appropriately, for example, **VLPortalLayout_es.bmp**.
4. Within your HTML file, update all the image references to point to your newly created image files.
5. When finished editing your new HTML file, go to the VLPortal Web Page Catalog. Right-click on the **Cleo Harmony Web Page Help** entry and select **Edit…**.
   a) If a prompt appears, showing the associated web portals and asking if you are sure you wish to edit it, click **Yes**.
   b) From the **Language** menu in the upper-right corner, choose the desired language.
   c) Add the **Title** content in the appropriate language.

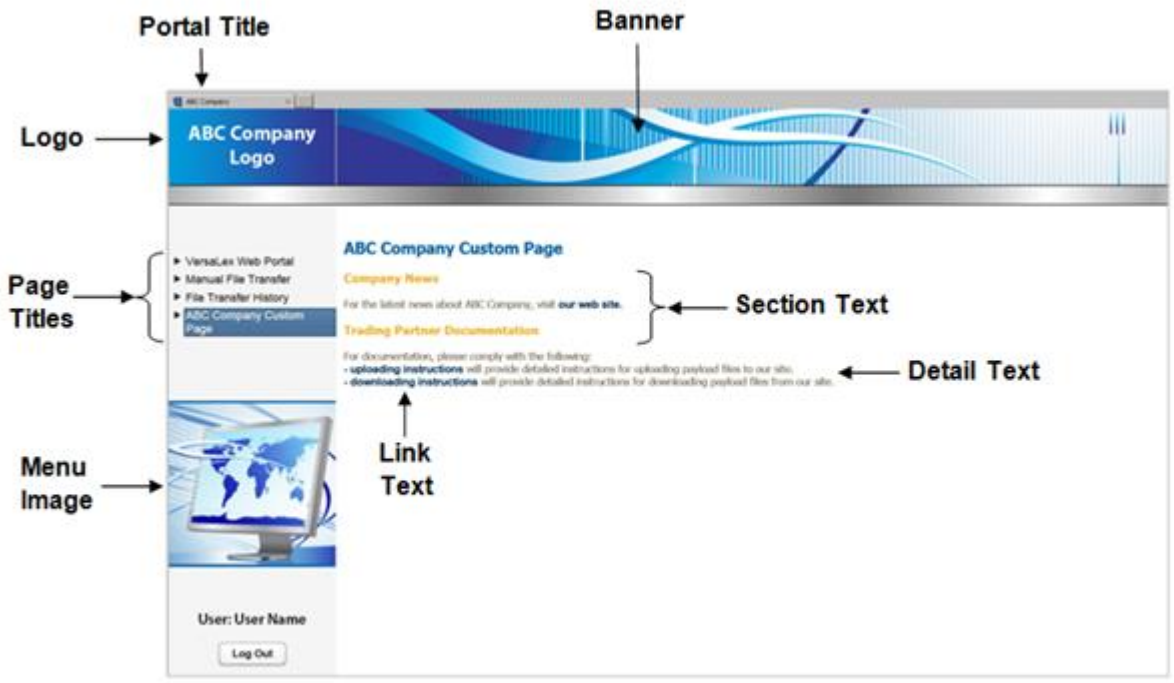
   See Editing or creating a web page on page 786 and Maintaining the VLPortal web page catalog on page 784.
6. Import you new HTML file.

   Click **Import**, select the new file as your linked file, and click **OK**.

   > **Note:** Do not copy HTML files directly into the `webserver\VLPortal\html` directory. In order for the HTML file to be properly registered in the Cleo Harmony application, it must be imported. This applies to a newly created HTML file or a modified HTML file. In all cases, the HTML files must be imported rather than directly copied.

Sample web portal layout

This example displays how a web portal configuration would appear in Internet Explorer.



Providing access to the web portal

Note: A custom web portal splash screen can be displayed by placing it in `webserver\VAADIN\cleo\images\custom` under the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom home directory. The filename must start with “splash.” (the word splash followed by a period). Supported formats include JPEG, GIF, and PNG. The image can be no larger than 525X340 pixels and no smaller than 250X100 pixels.

1. Before your trading partners can access the web portal, you must first establish a mailbox for each partner under the local HTTP users (see Local HTTP Users Configuration on page 834), and provide your partners with the proper URL (for example, `http(s)://VesraLexComputerIP:http(s)Port/VLPortalResourcePath`). Once these steps are followed, your trading partners can access the web portal by entering the specified URL into their browser. They will be prompted for a login.
2. The **User name** and **Password** are those that were established within the trading partner's mailbox under the local HTTP user.
3. To change a password, click **Options**.

   A password can be changed if:

   - the username's mailbox is not defined as an LDAP Usergroup and/or the username’s password has expired or
   - the username's mailbox is defined as an LDAP Usergroup, the LDAP Server Directory Type is "Active Directory," the LDAP Server Security Mode is not set to "None," and the user's password has not already expired.
4. The user can choose from the list of available languages from the **Language** drop-down list and view the web portal in their preferred language based on the resource files that have been configured and imported into the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application (see Internationalizing Your Portal).

5. If the option to select a custom link was configured in the **VLPortal** tab, a link will be included on the login page. (See Configuring VLPortal Web Browser service on page 783.) The text describing this link can be customized by editing the `VLPortalUI.CustomLink` property in the language-specific `VLPortal.properties` file(s) stored in `webserver\VLPortal\internationalization` under the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom home directory.
6. If reCAPTCHA authentication was enabled on the **VLPortal** tab, a dialog similar to the one shown below will also be displayed when the number of configured failed login attempts has been exceeded, or the number of failed login attempts was set to zero. See Configuring VLPortal Web Browser service on page 783.
7. After successfully logging in, the trading partner will be presented with the web portal home page in his desired language. The web portal associated with the user login is specified on the **Local HTTP User Host: Host HTTP** tab. See Configuring access for HTTP host users on page 835. The navigation within this portal is determined by the setup you established under the **VLPortal** tab. To understand the default (as-shipped) web portal configuration, see Configuring VLPortal Web Browser service on page 783.

Embedding web portal base pages into external web pages

It is possible to link directly to a web portal base page (**Manual File Transfer** or **File Transfer History**) from your own web pages. In order to access a base page in this manner, it is first necessary to log in, as discussed in Providing access to the web portal on page 793. The URL you provide will contain parameters to direct the display of the desired page(s).

Transfer Reporting page URL

The **Transfer Reporting** page is provided.

```
http(s)://VersaLexComputerIP:http(s)Port/VLPortalResourcePath?reportName=
 FileTransferHistory&external=true
```

Ad Hoc File Transfers

The **Ad Hoc File Transfers** page is provided.

```
http(s)://VersaLexComputerIP:http(s)Port/ VLPortalResourcePath?reportName=
 ManualFileTransfer&external=true
```

Transfer Reporting and Ad Hoc File Transfers

The **Transfer Reporting** and **Ad Hoc File Transfers** pages are provided, in the order specified, through a tabbed pane within a single page.

```
http(s)://VersaLexComputerIP:http(s)Port/  VLPortalResourcePath ?reportName=
 FileTransferHistory, ManualFileTransfer&external=true
```

Note: You should not provide multiple links to the base pages within the same web browser session. If you want to display multiple base pages, you should request all pages within one URL, using a comma-separated list as shown above.

Configuring Dashboards and System Monitor for web browser service

Cleo Dashboards and Cleo System Monitor are applications that are enabled from the **Dashboards/Monitor** tab in the Cleo VLNavigator application.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

1. Expand the Local Listener node in the tree pane and then click the **Web Browser** node.

2. On the **Dashboards/Monitor** tab in the content pane, specify parameter values as appropriate.

   See Local Listener Dashboard and System Monitor web browser service reference on page 795 for information about the parameters available.

3. Click **Apply**.

   Note: You must restart the Cleo Harmony or Cleo VLTrader service/daemon before you use Cleo Dashboards or Cleo System Monitor.

Local Listener Dashboard and System Monitor web browser service reference

Dashboards Resource Path

The check box activates and deactivates access to the Dashboards resource. Access is activated by default.

The default value of the path is `/VLDashboards`. Dashboards is a web UI-only application. You must include this resource path in the URL (for example, `http(s)://VersaLexComputerIP:http(s)Port/DashboardsResourcePath`) when accessing Dashboards through a browser. You can change this value at any time, but it must begin with a forward slash (/) character.

Access via VLProxy toggles access to the resource through Cleo VLProxy. It is selected by default.

System Monitor Resource Path

The check box activates and deactivates access to the Dashboards resource. Access is activated by default.

The default value of the path is `/VLMonitor`. System Monitor is a web UI-only application. You must include this resource path in the URL (for example, `http(s)://VersaLexComputerIP:http(s)Port/SystemMonitorResourcePath`) when accessing System Monitor through a browser. You can change this value at any time, but it must begin with a forward slash (/) character.

Access via VLProxy toggles access to the resource through Cleo VLProxy. It is selected by default.

Report Server

URL

RMI Port

Settings

The Report Server is a necessary component to Dashboards and System Monitor and the report server URL and RMI Port must be configured in order for Dashboards or System Monitor to function. Currently, Jinfonet's JReport Server is supported by the Cleo Harmony application. The Cleo JReport Server installer must be used, and the report server must be dedicated to Cleo Dashboards and System Monitor applications. HTTP-only is supported with the report server. The default server port is 8888 and the default RMI port is 1129. It is strongly recommended that the report server not be installed on the same computer as Cleo Harmony. Depending on report overhead and number of users, one report server can be set up to serve multiple instances of Cleo Harmony, or a separate report server can be dedicated to each Cleo Harmony. It is not recommended that the same report server be used across Cleo Harmony pools, as one report server instance cannot be used to serve different versions of Cleo Harmony.

Click **Settings** to display the report server log level setting and version.

Use the menu in the Options section select a Log Level for your reports.

Select **Normal** for everyday operation. Select **Verbose** in cases where debug logging has been requested by Cleo Support.

Configuring Cleo Unify for web browser service

Cleo Unify application is enabled from the Cleo VLNavigator **Unify** tab. See Cleo VLNavigator on page 917.

Note: This section applies to Cleo Harmony and Cleo VLTrader systems only.

1. Click **Local Listener > Web Browser** in the tree pane and then click the **Unify** tab.
2. Select the **Unify Resource Path** check box to enable access. The resource paths are not enabled by default.
3. Specify the path to the Cleo Unify resources.

   The default value is `/Unify`. Cleo Unify is a web UI-only, and users must include this resource path in the URL when the application through a web browser. For example, http://*VersaLexComputerIP*:*http(s)Port*/*Unify*)
4. (Optional) Clear the **Access via VLProxy** check box. It is selected by default, but you can clear it to disable access through Cleo VLProxy.
5. Click **Apply**.

Configuring graphics and fonts

If you are running the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application on a Unix platform, you might need to adjust graphics- and font-related properties if the application is reporting related problems. Running in **Headless mode** eliminates any possible dependencies on X11 or XVFB. When Headless mode is enabled (the default for new installs), the other graphics and font settings cannot be changed. The corresponding XML property name is `<Headlessmode>`.

1. Click the **Graphcis/Fonts** tab.
2. Clear the **Headless mode** check box to enable edit mode for the other graphics and fonts settings.
3. Select the **Mixed settings** check box to enable the properties below.

   Use platform graphics

   Property name: <*UsePlatformGraphics*>

   Description: Indicates to use native graphics environment rather than the application's virtual graphics environment

   Default value: `True` if Solaris; `False` otherwise

   Use X11 DISPLAY environment variable

   Property name*: *<NeedX11DisplayVariable>

   Description: If access to X-Window is needed for native graphics environment

   Default value: `True`

   Property name*: *<X11DisplayVariableValue>

   Description: X11 server number and screen number. If an X11 server is not available, it may be necessary to run `Xvfb`.

   Default value: `0.0`

   Include application fonts

   Property name: <*IncludeApplicationFonts*>

   Description: Includes webserver/AjaxSwing/lib/fonts in font path. Can only be False if <IncludeJreFonts> is True

   Default value: `True`

   Include JRE fonts

   Property name: <*IncludeJreFonts*>

   Description: Includes jre/lib/fonts in font path. Can only be False if <IncludeApplicationFonts> is True

   Default value: `True`

   Reverse order in font path

   Property name: <*ReverseOrderInFontPath*>

   Description: Reverses order of above directories in font path

Default value: False

Use application font properties

Property name: <*UseApplicationFontProperties*>

Description: Indicates to use application's font properties rather than JRE's

Default value: `True`, if Linux. `False` otherwise

Use platform font

Property name: <*UsePlatformFont*>

Description: Indicates to use native font rather than JRE's

Default value: `False`

Xvfb (X virtual frame buffer) is an X11 server that performs all graphical operations in memory (http://en.wikipedia.org/wiki/Xvfb). Xvfb implementations are available on Linux and Solaris. If needed, perhaps the easiest way to activate Xvfb is to start an Xvfb process just prior to starting the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application in the `Harmonyd`, `VLTraderd`, or `LexiComd` daemon script. The X11 server number and screen number are runtime parameters to `Xvfb`; the <*X11DisplayVariableValue*>

above would need to be set to the same server and screen numbers.

Note: If a native UI does not exist, you can use command line options to change any of the above settings. For example:

```
Harmonyc -p Local Listener\Web Browser -t
 <Service><IncludeApplicationFonts>False
```

```
VLTraderc -p Local Listener\Web Browser -t
 <Service><IncludeApplicationFonts>False
```

```
LexiComc -p Local Listener\Web Browser -t
 <Service><IncludeApplicationFonts>False
```

- When **Mixed settings** is selected, the graphics and text settings can be a mixture of the Cleo Harmony software's virtual environment and JVM runtime and operating system native environment.
- When **Application only settings** is selected, all of the graphics and font settings shift to only those provided by the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom software's virtual environment.
- When **Platform only settings** is selected, all of the graphics and font settings shift to only those provided by the JVM runtime and operating system native environment.

For both **Mixed settings** and **Platform only settings**, if the **Use X11 DISPLAY environment variable** check box is selected, you should ensure the server and screen number are properly set.

Configuring web browser service advanced properties

1. Click the **Advanced** tab.
2. Specify values for the following properties as needed.

Page Size

Use this option to specify the number of nodes on a page.

Changes to these settings in a web UI session are immediately applied to the session so that the optimal values can be determined - other active web UI sessions must explicitly refresh the tree (right-click in whitespace around tree). To match previous versions of the Cleo Harmony application when these settings were not configurable, set them as follows:

Top Level

Host Subfolders

The number of nodes displayed per page for top level and host subfolders trees.

Note: These settings apply to Cleo Harmony and Cleo VLTrader applications only

Within Hosts

The number of nodes displayed per page for the active and template hosts tree in the main window.

Certificates

The number of nodes displayed per page for the certificates tree in **Administration > Certificates** in the web UI or in **Tools > Certificate Manager** in the native UI.

Session Timeouts - Harmony/VLNavigator

These properties applies to the VersaLex and Cleo VLNavigator applications only.

Initial startup

The time allotted for launching a new web browser session. Default value: 120 seconds.

Waiting for response

The maximum time allowed waiting for server response to a browser request. Default value: 120 seconds.

Abnormal exit detection

The time allowed without a web UI ping before the session is shutdown by the server seconds. Default value: 60 seconds.

Session Timeouts - VLPortal

This property applies only to VLPortal.

Inactivity Timeout

The maximum time allowed while logged into the web portal without any user activity before the session is expired (default 600 seconds).

Note: If you have configured your portal users to use the applet, this value should be set large enough to cover the entire duration that a user may have an applet window active.

Response Headers

Additional response headers (primarily for required security headers) for the web UIs as a whole. Enter a new header on each line.

Possible headers include:

```
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: no-store
Content-Security-Policy: script-src 'self'
```

If you specify `X-Frame-Options`, for those web UIs where IFrames are used (for example, Cleo Harmony and Cleo VLTrader), a value of `DENY` is automatically changed to `SAMEORIGIN`.

If you specify `Content-Security-Policy`, for those web UIs where inline scripts are used(for example, Cleo Harmony and Cleo VLTrader), a `script-src` directive is added if not already present, and includes `'unsafe-inline'` and `'unsafe-eval'`. If the directive already exists, `'unsafe-inline'` and `'unsafe-eval'` are automatically inserted into directive.

Append `[Always]` to the end of any response header to be included in all web server responses, not just web UI responses. For example, `Content-Security-Policy: script-src 'self' [Always]` would result in this header (less the `[Always]` marker) being returned in an `/api` response.

Debug Settings

Append service debug to system debug file

Select the check box to log debug information into the Cleo Harmony system debug file.

Create individual client debug files

Select the check box to create a new HTML client debug file (stored in `logs\` under the Cleo Harmony home directory) for every JVM instance.

3. Click **Apply**.

Local Listener Web Service

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

A web service provides a platform-agnostic enterprise application integration (EAI) mechanism. The Cleo Harmony and Cleo VLTrader applications offer two web services: SOAP and REST.

Local Listener Web Service SOAP reference

There are two kinds of SOAP web services offered: a general purpose web service and a service designed specifically to work with TradeLink.

Resource Path

The check box activates and deactivates access to this resource. Access is activated by default.

The default value of the path itself is `/services`.

General Purpose web service

Used to initiate trading partner mailbox sends and receives through any Cleo Harmony or Cleo VLTrader protocol.

Similar to the Java `API IMailboxController` interface, the web service provides for `send`, `receive`, and `sendAndReceive` operations. A `delete` operation is also included for confirming receipt of a payload file after a `receive`. .

Password

Required by the web service. The password is immediately operational for any configured Cleo Harmony or Cleo VLTrader mailbox.

Available when you select **General Purpose web service**.

WSDL 1.2 compliant

Select to eliminate overloaded operations.

Available when you select **General Purpose web service**.

Use arrays

Indicates whether the host/mailbox should be specified in a string array rather than separate string arguments. When **WSDL 1.2 compliant** is not activated, **Use arrays** will default to activated.

TradeLink web serivce

Used to initiate trading partner mailbox sends and receives through any Cleo Harmony or Cleo VLTrader protocol.

Database Driver String

Connection String

Username

Password

Information required to connect to a TradeLink database. If you are not sure of these values, contact your TradeLink system administrator.

Allow web access to logs\ directory

Enables access to Cleo Harmony log files from within the web service activated, whether a general purpose web service or TradeLink.

Local Listener REST Service reference

The REST web service is a lightweight alternative to SOAP.

Resource Path

Select to activate the service.

Defaults to `/api`. It can be changed at any time, but must start with a forward slash (/).

Access-Control-Allow-Origin Response Header

Specify domains that can access resources in the **Resource Path**.

For example, to restrict access to the **Resource Path** to requests only from http://domain.example, specify `http://domain.example`

Specify an asterisk (*) to allow access from any domain or a regular expression to allow access from multiple, specific domains.

Disable Basic Access Authentication for REST API Requests

Select this option to disable users from accessing the REST API using the **HTTP Basic Access Authentication** method. Only **OAuth2.0** authentication is accepted.

Configuring Local Commands host

Use the Local Commands host for local commands only. With Local Commands hosts, there is no server, client, or protocol involved, nor any connection to another host. Local Commands mailboxes can have actions, but only operations that manipulate files within the local file system are provided. You can create multiple Local Commands hosts, schedule actions, and package files you have copied using an available packaging method, such as OpenPGP.

See Composing an action on page 89 and Local command reference on page 876 for more information.

1. Go to the **Templates** pane, right-click the Local Commands host, and select **Clone and Activate**. The Local Commands host is activated and added to the **Tree** pane.
2. On the **General** tab for the activated Local Commands local host, modify the default inbox and outbox directories, if necessary.

   You can select macro variables from the drop down lists. See Using Macro Variables for a list of the applicable macros (Default Host Directory context) and examples. For Cleo VLTrader and Cleo Harmony applications, see URI File System interface overview on page 955 for information about how to use a Cleo-provided or custom URI for the Inbox or Outbox. See Specifying default host directories on page 700 for information regarding the setup of system-level directories and custom directory macro variables.
3. On the **Advanced** tab, specify advanced host properties. The available properties within the Local Commands host **Advanced** tab are a subset of the properties described in Setting advanced host properties on page 89.
4. Specify mailbox packaging properties. Click the mailbox for the Local Commands host to display the **Packaging** tab.

The **Packaging** tab of the Local Commands host mailbox is used to encrypt and decrypt files that are involved in `LCOPY` commands within the Local Commands host.

5. Select one of the following options from the **Packaging** menu and then click **Configure**.

   - **OpenPGP** - a public/private key pair, established through a shared certificate, is used to perform the encryption/decryption, and digital signing is supported. See OpenPGP local packaging for Local Commands host reference on page 802.
   - **XML Encryption** - a public/private key pair, established through a shared certificate, is used to perform the encryption/decryption. See XML Encryption local packaging for Local Commands host reference on page 803.

   See Cryptographic Services on page 975 for general information regarding encryption and signing.

   Unlike the **Packaging** tab within other hosts that contains a Partner section and a Local section, the **Packaging** tab within the Local Commands host contains only the Local section, as there is no partner associated with a Local Commands host. See Setting up local packaging for Local Commands host on page 801. While reading the information about the Local section and its associated dialogs, it is important to be aware of the advanced properties that govern the details of the packaging selections. These properties are listed in the following table. See Setting advanced host properties on page 89 for more information.

OpenPGP Properties	XML Encryption Properties
PGP Compression Algorithm	XML Encryption Algorithm
PGP Encryption Algorithm	
PGP Hash Algorithm	
PGP Integrity Check	
PGP Signature Verification	
PGP V3 Signature	

The Local Commands host is used strictly for operations on local files. A default Copy **Action** is provided to move files from the inbox to the outbox. See Composing an action on page 89 and Local command reference on page 876 for more information.

Setting up local packaging for Local Commands host

Prior to setting up the **Local** section, you must create or acquire an encryption certificate to be used for local storage encryption, decryption, and signing. The **Local** section, along with the dialog boxes stemming from the **Configure** button, allows you to associate your signing/encryption certificate with this mailbox for packaging destination files and associate your signing/encryption certificate with this mailbox for un-packaging source files. Note that the certificates specified on this tab may reference the same certificate or two different certificates; this depends on your application.

Note: When you click **Configure**, either the **Configure OpenPGP Local Packaging** or **Configure XML Encryption Local Packaging** dialog box is displayed. It is important to understand that the **Encrypt**, **Decrypt**, and the certificate fields are *shared* between the two dialogs. This allows you to set up these fields once, and then simply use the **Packaging** selection on the **Local** section to toggle between packaging schemes.

Select an option from the **Packaging** drop-down menu. Choose from the following:

- **None**: local packaging is not active.
- **OpenPGP**: OpenPGP local packaging is active. See OpenPGP local packaging for Local Commands host reference on page 802 for information on setting up OpenPGP local packaging.

- **XML Encryption**: XML Encryption local packaging is active. See XML Encryption local packaging for Local Commands host reference on page 803 for information on setting up XML Encryption local packaging.

OpenPGP local packaging for Local Commands host reference

Encrypt

Enables you to sign and encrypt destination files. If you choose this option, you must also choose encryption options and you should enter both your trading partner's certificate and your user certificate as both might be necessary depending on other options you select. Note that the **Encrypt** and **Decrypt** options are mutually exclusive, as it is only practical to perform a single operation within an `LCOPY` command.

Decrypt

Enables you to verify signatures and decrypt source files. You should enter both your trading partner's certificate and your user certificate as both might be necessary depending on other options you select. Note that the **Encrypt** and **Decrypt** options are mutually exclusive, as it is only practical to perform a single operation within an `LCOPY` command.

Encryption/Signature Verification

Certificate

The CA certificate you want to use for encryption and signature verification. You can specify a certificate explicitly or click **Browse** to navigate to a certificate.

If multiple recipients are required, you can use the `SET` command to specify multiple certificates. The certificates are specified in the `SET` command using the '|' [pipe] character as a separator. For example,

```
SET mailbox.LocalPGPEncryptionCert=certs\companyA.cer  | certs
\personB.cer | certs\trunk.cer | certs\companyC.p7b
```

Decryption/Signing

Override Local Listener Certificate

Select the **Override Local Listener Certificate** check box enable the Certificate Alias and Password fields, where you can specify an certificate to use instead of the default signing certificate you specified for the Local Listener. See Configuring certificates for Local Listener on page 758.

Certificate Alias

The certificate you want to use for signing and decryption. You can specify a certificate alias explicitly or click **Browse** to navigate to a certificate.

Password

The password of the certificate's private key.

Encryption Options

You write a destination file to the file system with any combination of the following options (see Advanced system options on page 743 for information about associated advanced properties):

Encrypted

Encrypt using the **PGP Encryption Algorithm**.

Signed

Sign using the **PGP Hash Algorithm**.

Compressed

Compress using the **PGP Compression Algorithm**.

Armored (Base64)

Armor (Base64 encode) the data. Base64 encoding converts binary data to printable ASCII characters.

Encrypt to My Certificate

Allow **Signing/Decryption Certificate** and **Signature Verification/Encryption Certificate** to decrypt inbound encrypted files. The **Encrypted** check box must be selected to enable this option.

Decryption Options

Force Encryption

Force Signature

Allow Non-OpenPGP

Select one or more of these options to check all source files for the desired security level. An error is logged (and the file rejected) if the file is not packaged according to the corresponding security settings. If a setting is not selected, the file will not be checked for conformance with that security setting.

XML Encryption local packaging for Local Commands host reference

Encrypt

Enables you to encrypt destination files. Note that the **Encrypt** and **Decrypt** options are mutually exclusive, as it is only practical to perform a single operation within an `LCOPY` command.

Decrypt

Enables you to decrypt source files. Note that the **Encrypt** and **Decrypt** options are mutually exclusive, as it is only practical to perform a single operation within an `LCOPY` command.

Encryption Certificate

Certificate

The CA certificate you want to use for encryption and signature verification. You can specify a certificate explicitly or click **Browse** to navigate to a certificate.

Decryption Certificate

Override Local Listener Certificate

Select the **Override Local Listener Certificate** check box enable the Certificate Alias and Password fields, where you can specify a certificate to use instead of the default encryption certificate you specified for the Local Listener. See Configuring certificates for Local Listener on page 758.

Certificate Alias

The certificate you want to use for decryption. You can specify a certificate alias explicitly or click **Browse** to navigate to a certificate.

Password

The password of the certificate's private key.

Local Commands host advanced properties

Add Mailbox Alias Directory to Inbox

Appends a subdirectory at the end of the host's configured inbox directory. This allows files received through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Add Mailbox Alias Directory to Outbox

Appends a subdirectory at the end of the host's configured outbox directory. This allows files to be sent through different mailboxes to be kept separate.

Possible values: `On` or `Off`

Default value: `Off`

Allow Actions To Run Concurrently

Normally, actions and host actions within the same host are allowed to run concurrently. You can use this property to not allow actions and host actions to run concurrently.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Command Retries

If an error or exception occurs during a command, the number of times the command should be retried.

Note: Command Retries does not apply to exceptions related to TCP/IP or ISDN dial-up connections. This is because dial-up connections are managed by the framework so that they can be shared across actions.

Possible values: `0 - n`

Default value: `0`

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

`System Default`

```
Alphabetical
Date/Time Modified
```

Default value: `System Default`

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512
```

Default value: `System Default`

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: `On` or `Off`

Default value: `On`

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: `On` or `Off`

Default value: `On`

PGP V3 Signature

Retry Delay

The amount of time (in seconds) before a retry should be attempted.

Note: For AS4 hosts, this value is reflected as **read-only** through the `PMode.ReceptionAwareness.Retry.Period` setting.

Possible values: Any value greater than zero.

Default value: `60 seconds`

Terminate On Fail

If an error occurs during a command, stop the action.

Note:

Regarding non-`CHECK` commands: When `Terminate On Fail` is on, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and then the action stops. When `Terminate On Fail` is off, if a command fails, `Email On Fail` and `Execute On Fail`, if set, are processed, and the action continues.

Regarding `CHECK` commands: `Terminate On Fail` is only honored if the `ConditionsMet` parameter is set and the result of the `CHECK` is classified as `Error`. The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

Possible values: `On` or `Off`

Default value: `On`

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

`System Default`
`TripleDES`
`AES-128`
`AES-192`
`AES-256`

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

Configuring local FTP users

Note: This feature is being deprecated. For protocols other than AS3, use a Users host. See Users Host on page 516 for more information. For AS3, you can continue to use the FTP Users host and mailbox until further notice.

Note: This section applies to the Cleo VLTrader and Cleo Harmony applications only.

When you start your FTP server for the first time, no users are defined and therefore no access is granted to your server.

1. In the **Templates** pane, open the **Other** folder, and then clone and active the preconfigured **Local FTP Users** local host. See Activating a host from a template on page 77.
2. Specify default directories for all Local FTP users. See Configuring local FTP user directories on page 810.
3. Configure access for FTP users. See Configuring access for FTP host users on page 811.
4. Add a new mailbox to create a new FTP server login.

   You can either clone the default **myTradingPartner** mailbox or create a new mailbox.

   Local FTP user mailboxes can have actions, but unlike remote host/mailbox actions that perform remote host operations, local FTP user actions can only perform local host operations that manipulate files within the user's home directory. See Action Tab on page 828.

   FTP Users can be either generic FTP users, AS3 users, or LDAP users. See Configuring FTP for Local FTP Mailbox on page 812, Configuring AS3 for Local FTP Mailbox on page 813, and Configuring LDAP for Local FTP Mailbox on page 816, respectively.

You can create multiple Local FTP Users local hosts, which allows you to group users with the same host properties together. User names (for example, Local FTP user mailbox names) will remain unique across all Local FTP Users local hosts.

Configuring local FTP user directories

Use the **General** tab to specify default values for local FTP user directories.

1. Specify a **Default Root Directory**. By default, each FTP user's home directory is a subfolder under the directory you specify here. Click the **...** button to browse and select a directory. Alternatively, select a custom macro variable from the drop-down menu. See Using Macro Variables for a list of the applicable macros (Default Root Directory context). Once the change is applied, FTP users that are already configured to use the default root are switched over to the new default root.
2. Specify the paths and names of **Local User Subdirectories**. These directories are automatically created under each user's home directory. Each directory path specified should be a relative path.

   The configured inbox and outbox directories can be easily referenced in the mailbox `<collect>` and `<release>` actions by using the `%inbox%` and `%outbox%` macros, respectively. See Action Tab on page 828

   If the sentbox directory is configured, when the user retrieves a file from the configured outbox, the Cleo Harmony application places a user-accessible copy of the file in the sentbox directory. If the receivedbox directory is configured, when the user stores a file in the configured inbox (either directly or via RNFR/RNTO), the Cleo Harmony application also places a user-accessible copy of the file in the receivedbox directory.

   Note: Files of the same name are overwritten.

   The following are rules that apply to AS3/FTP mailboxes:

   - The default `inbox\` and `outbox\payload\` subdirectories are always used, regardless of the settings specified in the **Host** > **General** panel, because vendor AS3 send and receive "choreographies" are established and published for interoperability certification and cannot be altered.
   - Remote AS3 users must place all inbound payload files and MDNs in the `inbox\` subdirectory. Outbound payload files can only be received from the `outbox\payload` subdirectory; outbound MDNs can only be received from the `outbox\mdn`subdirectory.
   - Files placed in any other directory or subdirectory are not accessible by AS3 users and will not appear in any remote directory listings.

- The `sentbox` and `receivedbox` subdirectories are not created or used in AS3/FTP mailboxes regardless of the settings specified in the **Host** > **General** panel due to the above security restrictions placed on all AS3 users.
- In addition to the **Inbox**, **Outbox**, **Sentbox** and **Receivedbox** folders, additional folders can be specified in the **Others** field. Multiple paths can be added to **Others** separated by commas, semi-colons or carriage returns. Note that all paths must be relative and may not include reserved macro variables (for example, `%mailbox%`).

3. The **Archive Directories** allow for a copy of the sent and received files to be saved in an additional location that, in most cases, is not accessible by the user. Unlike the `sentbox` and `receivedbox` configured under the **Local User Subdirectories**, you can configure these directories to point to a network location by clicking the **...** button; or you can select a custom macro variable from the drop-down list. See Using macro variables on page 59 for a list of the applicable macros (**Default Local User Archive Directory** context). See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

   If desired, the `%mailbox%` macro may be used as part of these directory definitions to filter files for non-LDAP users into separate subdirectories. Files written to these directories are retained with unique file names and will be archived if the Sent/Received Box Archive System Option has been enabled. See Specifying default host directories on page 700

Configuring access for FTP host users

Use the FTP tab to configure access for FTP host users. Specify values for the following fields:

Acceptable inbound file patterns

Specify patterns that files must match to be permitted inbound. Patterns can include wildcards and regular expressions. See Using wildcards and regular expressions on page 69. If you specify multiple file patterns, separate them with semi-colons (;) or commas (,). Alternatively, enter them on separate lines.

The following are examples of valid patterns:

- `*` – any file pattern
- `*.*` – file must have an extension
- `*.edi;*.xml` – only `.edi` and `.xml` extensions acceptable (case sensitive)
- `[(?i).*\.(edi|xml)]` – only `.edi` and `.xml` extensions acceptable (case insensitive)

Users have read-only access

Restricts FTP users to read-only access of files and directory listings in their home directory. Users with read-only access may only retrieve files or directory listings from their home directory.

When you select this option, the **Users can make/remove subdirectories** check box is disabled and any previously selected setting is cleared.

This setting does not apply to AS3 users, since retrieving files may also require subsequent uploads of MDN receipts.

Users can make/remove subdirectories

Enables FTP users to make and remove subdirectories within their home directory

This check box is disabled when you select the **Users have read-only access** option.

Users must connect on a secure port

Limits users to SSL connections only. When selected, users will able to successfully authenticate only when an FTP/s connection is used.

IP filter required

When you select the **IP filter required** check box, all mailboxes under this host require whitelist IP addresses to be entered. If no whitelist IP addresses are entered for a mailbox, that mailbox is set to `not ready`. For the mailboxes that have whitelist IP addresses entered, the mailbox user can log in to the mailbox only from the IP

addresses configured. If the **IP filter required** check box is cleared, whitelist IP addresses are not required and the mailbox user can log in from anywhere.

Password Policy

Defines the security requirements that will be enforced for all local users. By default, the **Password Policy** used by all mailbox users is globally defined via the **Enforce Password Policy** option on the **System Options > Other** tab. See Other system options on page 729.

To specify a different set of security restrictions for all mailbox users defined for a particular local user host: select the **Override System Level Settings** option, select the **Enforce Password Policy** option (if not already selected), click **Configure**, make the changes and click **Apply**. See Configuring password policies on page 55 for further information on the **Password Policy** options.

To disable **Password Policy** enforcement for all mailbox users defined for a particular local user host: select the **Override System Level Settings** option, clear the **Enforce Password Policy** option and click **Apply**.

Configuring FTP for Local FTP Mailbox

FTP Users can be either generic FTP users, AS3 users, or LDAP users.

Username

The mailbox alias. This value is used by your trading partner to log in to your FTP server. Specify a value not already in use.

Password

The password for the mailbox. This value is used by your trading partner to log in to your FTP server.

User Home Directory

Defaults to a username subdirectory under the default root directory defined on the **General** tab (see Configuring local FTP user directories on page 810). To override this path for this user only, clear the **Use Default Root \Username** check box and click the **...** button to change the home directory; or select a custom macro variable from the drop-down list. See Using macro variables on page 59 Using Macro Variables for a list of the applicable macros (Default Root Directory context).

Subdirectories

Click **Subdirectories** to display the **Local User Subdirectories** dialog box. This dialog box displays host-level settings (read-only) for the current folder configuration and allows you to specify additional folders at the mailbox level in the **Mailbox-level Settings** > **Others** field. You can add multiple paths (one path per line) in the **Others** field. All paths must be relative and cannot include reserved macro variables (for example, `%mailbox%`).

Pipe Incoming Payload

Allows for this trading partner to send to your FTP server and redirect, or pipe, the incoming payload out through a different protocol. If the transfer out to the pipe mailbox fails, the transfer into the local mailbox also fails.

AS3 User

Select the **AS3 User** check box to designate the user as an AS3 user and enable the **AS3 Mailbox: AS3** tab. See AS3 Mailbox on page 196.

LDAP Usergroup

Select the **LDAP Usergroup** check box to designate the mailbox as an LDAP user group mailbox and enable the Mailbox **LDAP** tab (see Configuring LDAP for Local FTP Mailbox on page 816. Many of the other fields on this tab are disabled when select the **LDAP Usergroup** check box. An LDAP user group mailbox has the following features:

- The mailbox no longer corresponds to a single user, but rather a group of users configured in an external directory server.

- In addition to authenticating usernames and passwords through the external directory server, you can select the **Use LDAP Home Directory** check box to use the directory service to provide user home directory paths. If this option is not selected, and the **Use Default Root\Username** check box is selected, the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application dynamically appends the username to the root directory by way of a `%username%` macro variable.

Unlock

This button is enabled when the user has too many failed log in attempts. Mouse over the **Unlock** button to display when the user will be unlocked automatically or you must unlock the user manually. Click **Unlock** and then click **Apply** to unlock the user.

Configuring AS3 for Local FTP Mailbox

The **AS3** tab is enabled when you select the **AS3 User** check box on the **FTP** tab. The **AS3** tab contains three tabs: **Headers** (see Local AS3 message headers reference on page 813), **AS3** (see Local AS3 settings reference on page 813), and **Certificates** (see Local AS3 certificates reference on page 815).

Local AS3 message headers reference

The **AS3** tab contains the configuration for the AS3 message headers.

AS3-From

The AS3 name that you will be using for this trading relationship.

AS3-To

Your trading partner's AS3 name.

Subject

Text you want to include in the header of all messages sent to this trading partner.

Content-type

Select the value appropriate from the menu for the files you want to send to this trading partner.

Alternatively, leave this field blank and allow the application to detect the `Content-Type` first based on the file content and then the file extension. Detectable values include:

- application/edifact
- application/edi-x12
- application/edi-tradacoms
- application/xml (text/xml)
- application/pdf
- application/msword
- application/x-msexcel
- application/rtf
- application/zip
- image/bmp
- image/gif
- image/tiff
- image/jpeg
- text/plain
- text/html
- video/mpg

Local AS3 settings reference

The AS3 tab contains three sections: **Request**, **MDN Receipt**, and **Inbound Message Security**.

Request

Encrypted

Signed

These fields allow you to specify the combination of attributes (with respect to S/MIME format) of the message you want to send to the remote AS3 client.

- Unsigned/unencrypted (neither the **Encrypted** nor **Signed** check boxes are selected)
- Signed (only the **Signed** check box is selected)
- Encrypted (only the **Encrypted** check box is selected)
- Signed / Encrypted (both the **Signed** and **Encrypted** check boxes are selected)

Receipt

Enables the MDN Receipt section, where you specify attributes related to a receipt for your message.

Encryption Algorithm

This field is enabled when you select the **Encrypted** check box. It allows you to choose an encryption algorithm for the message. The remote AS3 client must be able to decrypt the message using the algorithm you choose. For a non-Cleo Harmony AS3 client, it is important to verify the algorithms it is capable of handling **prior** to sending an encrypted message. The default encryption algorithm is **TripleDES**. See Cryptographic Services on page 975 for more information on choosing an encryption algorithm.

Key Algorithm

When **Encrypted** is selected, the **Key Algorithm** field is enabled and allows you to choose the algorithm to encrypt the content encryption key with the public key of your trading partner's encryption certificate. Your trading partner uses the private key of their encryption certificate to decrypt the content encryption key that is subsequently used to decrypt the content of the message.

Possible values:

- `RSA`(default)
- `RSAES-OEAP`

Signature Algorithm

When **Signed** is selected, the **Signature Algorithm** is used to encrypt the hash value of the signature with the private key of your signing certificate. Your trading partner uses the public key of your signing certificate to decrypt the hash value of the signature that authenticates you as the sender of the message. When **RSA** is selected, the selected **Hash/MIC Algorithm** is used to determine the appropriate signature algorithm, for example, `rsaEncryption`, `sha256WithRSAEncryption`, `sha384WithRSAEncryption` or `sha512WithRSAEncryption`. If **RSASSA-PSS** is selected, the combination of the private key of your signing certificate and the hash algorithm is used in conjunction with the RSASSA-PSS algorithm to secure the signature.

Possible values:

- `RSA` (default)
- `RSASSA-PSS`

Hash/MIC Algorithm

When **Signed** in the **Request** section is selected, the combination of the signature algorithm and the selected hash algorithm is used to secure the signature.

Note: If the RSASSA-PSS signature algorithm is used and the SHA-512 hash algorithm is selected, the strength of the signature algorithm of your signing certificate must be SHA256withRSA or better.

When the **Signed** option in the **MDN Receipt** section is selected, the selected **Hash/MIC Algorithm** is used to compute the independent Message Integrity Check (MIC) value that is returned in the MDN Receipt.

Possible values:

- `SHA-1` (default)
- `MD5` (cryptographically weak and should not be used unless no other Hash/MIC algorithm is available)
- `SHA-256`
- `SHA-384`
- `SHA-512`

Compress Content

Select this check box to enable ZLIB compression for the message.

Use compression to conserve bandwidth and improve security when sending large files.

MDN Receipt

When the **Receipt** check box is selected in the **Request** section, the fields in an MDN Receipt is enabled for editing. Otherwise, these fields will be disabled.

Signed

When you select the **Signed** check box, a hash is computed over the content of the sent message using the algorithm you select from the **Hash/MIC Algorithm** menu. The recipient returns the MDN with a digital signature and will compute an independent MIC value over the content of the message received (using the same MIC algorithm) and return this value as a Base64-encoded value in the human-readable portion of the MDN. When the MDN is received, the MIC you selected is compared against the received MIC. When the MIC values match, the sender is guaranteed that the message read by the recipient was identical to the message that came from the sender and not modified in any way.

Forward MDN to Email

Select this check box to forward a copy of the received MDN to recipient you specify in the **Email Address** field.

Synchronous

Asynchronous

Because an AS3 client must connect to your FTP server to send and receive messages, MDNs for AS3 can only be returned **Asynchronously** as part of a new FTP session. Depending on whether the user makes a clear or secure connection, MDNs will be returned either via FTP or FTPS.

Email Address

If you selected the **Forward MDN to Email** check box, specify the address to which the email should be sent.

Inbound Message Security

Enforce Encryption

Force Signature

Force MDN Signature

Select any combination of **Force Encryption**, **Force Signature** and **Force MDN Signature** options to configure inbound message security for this Local FTP User Mailbox. If a message is received but does agree with these settings, an error is logged and the message is rejected. If a given setting is not selected (which is the default), the message will not be checked for conformance with that security setting.

Local AS3 certificates reference

The **Certificates** tab allows you to associate both a trading partner's signing and encryption certificate(s) with this mailbox, and also override your own Local Listener's signing and encryption certificates.

Trading Partner's Certificates

Encryption Certificate

The certificate to be used for encrypting your trading partner's messages. Specify a value explicitly or click **Browse** to navigate to the certificate that matches the one you received from your trading partner.

Signing Certificate

The certificate to be used for validating incoming messages from your trading partner. Specify a value explicitly or click **Browse** to navigate to the certificate that matches the one you received from your trading partner.

By default, the Cleo Harmony application uses all the certificates in its certificate store to determine if the signature of the incoming data message is trusted. To limit validation to a specified signing certificate (that is, the incoming data message is required to be signed with only that certificate), select the Signing Certificate check box and browse for the certificate to be used for validating message signatures

Use encryption certificate

If your trading partner is using the same certificate for signing and encryption (which is the general practice among most trading partners), select the **Use encryption certificate** check box to automatically populate the **Signing Certificate** field with the same certificate selected in the **Encryption Certificate** field

My Certificates

By default, the certificates you configured on the **Certificates** tab of the **Local Listener** panel are the certificates used to sign messages sent to your trading partner and decrypt messages received from your trading partner. See Configuring certificates for Local Listener on page 758.

Override Local Listener Certificates

Select this check box to enable fields where you can specify alternate certificates for signing and decrypting messages with this particular trading partner. If you do override the default the certificates, remember to export and exchange these alternate certificates with your trading partner.

Configuring LDAP for Local FTP Mailbox

Use the **LDAP** tab to specify values to for this mailbox. The **LDAP** tab is enabled when you select the **LDAP Usergroup** check box on the **FTP** tab.

The values you specify on this tab supersede the values specified on the **LDAP Settings** or **LDAP Server** page.

Override System Settings

Select the **Override System Settings** check boxes to enable their related fields.

Base DN

The base organizational unit where the users are defined. Contact your directory administrator for the correct Base DN value. (The Base DN value entered here can be overridden in a local user host LDAP mailbox.)

The examples the table below show sample base organizational units for the supported directory types.

Directory Type	Example Base DN
Active Directory	`OU=Employees,DC=company,DC=com`
Apache Directory Services	`OU=Users,DC=example,DC=com`
Lotus Domino	`O=SCNotes`
Novell eDirectory	`O=Company Organization`
DirX	`ou=Users,o=Company`

Search filter

Optional. Used to limit the amount of information returned from the LDAP server when many users are defined. A more restrictive filter can be specified as a comma separated list. If necessary, contact your directory administrator to determine the appropriate attributes and values. You can override the value entered here in a local user host LDAP mailbox.

The following table contains example lists with sample attribute names and values.

Search Filter	Description
`department=EDI`	Limits the search to entries that have the attribute, `department`, with a value of `EDI`.
`department=EDI,group=administrators`	Limits the search to entries that must match two attributes. The user must be in the `EDI` department and in the `administrators` group.
`department=EDI,telephoneNumber=800*`	Limits search to EDI department members with a telephone number starting with `800`.
`objectclass=person`	Limit the search to entries that are people if the Base DN contains other entries (for example, computers) and people.
`!(userAccountControl:1.2.840.113556.1.4.803:=2)`	Excludes disabled accounts - in Active Directory, if an account is disabled, bit `0x02` in the `userAccountControl` attribute value is on. `1.2.840.113556.1.4.803` is the rule object ID (ruleOID) for the LDAP bitwise `AND` operator.

If the value to search in has any of the following special characters, they must be substituted in the Search Filter with the corresponding escape sequence.

ASCII character	Escape Sequence Substitute
*	\2a
(	\28
)	\29
,	\2c
\	\5c
NUL	\00
/	\2f

Extend Search Filter

Used to append rules to the default search system filter. This field is enabled regardless of the status of the **Override System Options** check boxes.

List

Used to display a list of users and their attributes matching the **Base DN** and **Search Filter**.

Local FTP users mailbox advanced properties

Use the **Advanced** tab to set advanced properties for the Mailbox.

Active Mode Source Data Port

Specifies the FTP server source data port for Active Mode FTP when set to a value > 0. Default value is 0 where the data port is unspecified. Some FTP clients may require a specific port number (for example, 20) be used for the server data port.

Allow Duplicate Incoming AS3 Message IDs

Ignores messages with duplicate message IDs and allows reprocessing of the message.

Automatically Delete Retrieved Outbox Files

When this option is selected, delete (remove) each file retrieved from the user's Outbox when the next FTP command is received from the client for a given FTP session. Files will only be deleted from the outbox (see Configuring local FTP user directories on page 810 Tab) after retrieval from the defined Outbox directory or its subdirectories. The delete confirmation response will be contained in a multi-line response (for example, 150-Retrieve of 'test.edi' confirmed…) for the next appropriate client command.

Possible values: `Selected` or `Unselected`.

Base64 Encode AS3 Content

Base64 is the encoding format used by Multi-purpose Internet Mail Extension (MIME) for transmitting non-text material over text-only communications channels. Base64 is based on a 65-character subset of US-ASCII, enabling 6 bits to be represented per printable character

Canonicalize Inbound AS3 Signed Content

When this option is selected, a canonicalizer is used to ensure that '\r' and '\n' characters always occur together as '\r\n'. This option may be used when the inbound signature hash verification fails and the trading partner is using OpenSSL to sign its messages.

Compression-Signing Order

When both signing and compression are enabled, this indicates which is applied first.

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Repetitive Listener Failures

When "Email On Fail" is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, an email alert will be sent when the failure is resolved. Failure resolution email alerts will not be sent for general Listener failures since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Repetitive Listener Failures

When `Execute On Fail` is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, the `Execute On Fail` command will be executed again when the failure is resolved. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure. Executions of the "Execute On Fail" command for resolution of general Listener failures will not be done since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0 - n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the mailbox should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not the Cleo Harmony or Cleo VLTrader application's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of the Cleo Harmony or Cleo VLTrader application is both the client and server (for example, a local looptest).

Possible values:

```
Incoming
Outgoing
Both
```

Ignore Exception After Quit

Indicates to ignore any I/O errors that occur when attempting to read the SMTP server response after issuing a `QUIT` command.

Possible values: `On` or `Off`

Default value: `Off`

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

Interim File Extension

When applicable, specifies the temporary filename extension that a trading partner's client software uses while transferring a file. For the transfer logging feature, the Cleo Harmony application sets the transfer status to `Interim Success` rather than `Success` when a transfer with a temporary filename extension is finished. Then, when the trading partner client software renames the file to strip off the temporary filename extension, the Cleo Harmony application inserts an additional `Success` entry into the transfer log with the resulting filename, thus marking the transfer as complete. The dot preceding the extension can be included in the configured value, but it is not required. If multiple temporary filename extensions are used, they can be separated by commas or semicolons.

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Concurrent FTP Logins

The total number of logins allowed at any one time for this user. With the default value of 0, the number of concurrent connections per user will be limited the Maximum Concurrent FTP Logins Per User setting. A value other than zero will override the Maximum Concurrent FTP Logins Per User setting for this user.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more

restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
```

`Twofish`

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

`System Default`
`MD2`
`MD5`
`RIPE-MD-160`
`SHA-1`
`SHA-256`
`SHA-384`
`SHA-512`

Default value: `System Default`

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: `On` or `Off`

Default value: `On`

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: `On` or `Off`

Default value: `On`

PGP V3 Signature

Retain Temporary Inbound Message Files

Leaves any files that are used while processing inbound messages in the `temp\` folder. The default action is to delete these files after processing has completed. These files can be helpful for problem diagnosis.

Note: Temp files are only created for large (> 2.3 meg) or compressed inbound messages.

RSA-OAEP Key Algorithm Parameter

Represents the type of mask generation and hash generation functions that are applied when the `RSAES-OAEP` key algorithm is in use. See RFC4055 for a further description of the mask and hash generation functions.

Possible values: `MGF1-SHA1`, `MGF1-SHA256` or `MGF1-SHA512`

Default value: `MGF1-SHA1`

Store AS3 Raw Sent Message

Saves the content of the FTP header and raw (unprocessed) message sent to the remote client. The files are stored in the as3\sent\ directory under the Cleo Harmony root path. These files may be useful in diagnosing problems, but should be disabled if disk space needs to be conserved.

Trigger At Upload Completion

When this property is not selected, the trigger is created when the next command is received after the file upload.

When this property is selected, the trigger is created when a file upload is completed (data channel is closed).

Note: For the FTP protocol, the end of file is signaled by the closure of the data channel. This makes it difficult to distinguish between successful and failed transfers accurately. Therefore, if this property is selected, it is possible that the trigger is created for an incomplete or failed transfer.

Note: There might be some use cases where a transfer is considered successful even if the client does not issue another command or log out. For example, if the client transfers a file and remains logged in until the next transfer (which could be several minutes later). In that use case, you should select the property.

Use AS3 Content Type for File Extension

By default, inbound messages that do not specifically contain the name of the target file to be saved are stored using the value of the Message-ID (of that message) with the `.file` extension. When this option is selected, inbound messages without a target file name specifier will be stored using the Message-ID and the appropriate file extension based on the Content Type of the message.

Use External IP Address In PASV Response

Indicates for passive (pasv) mode that the external rather than the local IP address should be included in data port response to the FTP client.

Use Folded Headers For Outbound Messages

Enables or disables automatic line wrapping of HTTP headers exceeding 76 characters. By default headers are not folded since some non-Cleo product remote hosts using Microsoft Internet Information Server (IIS) cannot handle folded headers properly. Unless your host has been pre-configured to enable folded headers, leave this setting cleared!

Possible values: `On` or `Off`

Default value: `Off`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
AES-128
AES-192
AES-256
```

Default value: `System Default`

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

Configuring mailbox packaging

Note: This section applies to all hosts, except the Local Commands host. For information about packaging for the Local Commands host, see Configuring Local Commands host on page 800.

Use the **Packaging** tab to configure encryption and decryption of payload files retrieved from the file system (or database payload repository) and stored to the file system (or database payload repository).

The **Packaging** tab consists of two sections: **Partner Packing** and **Local Packaging**. See Configuring partner mailbox packaging on page 80 and Configuring local mailbox packaging on page 83, respectively.

For each Partner and Local Packaging, there are two packaging schemes: **OpenPGP** and **XML Encryption**. Both schemes use a public/private key pair established through a shared certificate to perform encryption and decryption. The OpenPGP option also supports digital signing. See Cryptographic Services on page 975 for general information regarding encryption and signing.

There are certain advanced properties that govern the details of the packaging selections. These properties are listed in the following table. See Setting advanced host properties on page 89 for more information.

OpenPGP Properties	XML Encryption Properties
PGP Compression Algorithm	XML Encryption Algorithm
PGP Encryption Algorithm	
PGP Hash Algorithm	
PGP Integrity Check	

OpenPGP Properties	XML Encryption Properties
PGP Signature Verification	
PGP V3 Signature	

Configuring IP filtering for an FTP mailbox

Whitelist IP addresses are entered on the IP Filter tab of each local user mailbox. These IP addresses are the only addresses that will be allowed to log into the mailbox.

1. Go to the **IP Filter** tab for your FTP mailbox.
2. Click **New** to create a new entry or double-click an existing entry to edit it. Alternatively, you can right-click on the entry and select **Edit**.
3. Enter an IP address to be added to the whitelist.

   You can use both IPv4 and IPv6 addresses. IP addresses can be a single address or a range of addresses. The following are examples of valid IP addresses:

IP Address	Description
*	All IP addresses
10.11.12.13	Single IPv4 address matching 10.11.12.13
10.*	IPv4 addresses in the range 10.0.0.0-10.255.255.255
10.11.*	IPv4 addresses in the range 10.11.0.0-10.11.255.255
10.11.12.50-10.11.12.70	IPv4 addresses in the range 10.11.12.50-10.11.12.70
fe80::79ba:8815:4f62:e386	Single IPv6 address matching fe80::79ba:8815:4f62:e386
fe80::79ba:8815:4f62:e386-fe80::79ba:8815:4f62:ffff	IPv6 addresses in the range fe80::79ba:8815:4f62:e386-fe80::79ba:8815:4f62:ffff
fe80::79ba:8815:4f62:e386/90	IPv6 addresses matching the first 90 bits of address fe80::79ba:8815:4f62:e386

4. Optionally, remove an entry by right-clicking it and selecting **Remove**.

Action Tab

The FTP Server does not independently invoke send and receive actions, but rather acts on the actions of the connected client. Default `collect` and `release` actions are provided to allow the server to make sent and received files available for processing.

Collect Action

```
#Initialize inbound file
LDELETE recvfile.edit

#Merge all files received into recvfile.edit
LCOPY -DEL -APE %inbox%/* recvfile.edi
```

Release Action

```
#Release all not yet available files
```

```
LCOPY -DEL %outbox%/../* %outboxc%
```

See Composing an action on page 89 and Local command reference on page 876 for more information.

FTP Server Command Reference

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

The FTP Server allows users to log into the Cleo Harmony or Cleo VLTrader application and store and retrieve files using standard FTP (File Transfer Protocol) commands. A full description of the FTP commands is available in the RFC 959 specification. More detail on the FTP Security Extensions is available in RFC 2228.

The following FTP commands are accepted and processed by the Cleo Harmony or Cleo VLTrader FTP server.

Access Control Commands

Command	Description
USER <username>	Identifies the user to the FTP server. The <username> parameter is a string that must match one of the users previously entered into the Cleo Harmony or Cleo VLTrader application.
PASS <password>	Verifies the identity of the user, since only specified user should know the password. The <password> parameter is a string specifying the user's password. This command must be immediately preceded by the USER command.
PASS <password>/<newPassword>/<newPassword>/	Verifies the identity of the user and changes the user's password. The <password> parameter is a string specifying the user's current password and <newPassword> is a string specifying the user's new password. This command must be immediately preceded by the USER command. The password must follow the configured password policy or the login will be considered a failure.
ACCT <account>	Specifies the user's account. This command is not required, and has no effect on the logon process.
CWD <pathname>	Changes the current working directory to that specified by <pathname>. If <pathname> starts with a slash, the path is considered to be an absolute path. Otherwise, it is a path relative to the current working directory.
CDUP	Changes the current working directory to the parent of the current working directory. This can also be accomplished with the CWD command.
QUIT	Terminates the USER and closes the connection.

Transfer Parameter Commands

Command	Description
PORT <host-port>	This command and the <host-port> argument specify the data port to be used in data connection. The <host-port> argument is the concatenation of a 32-bit internet host address and a 16-bit TCP port address. This address information is broken into 8-bit fields and the value of each field is transmitted as a decimal number in character string representation. The fields are separated by commas. An example PORT command might be: PORT h1,h2,h3,h4,p1,p2 where h1 is the high order 8 bits of the internet host address. This address and port are created by the client side and the server connects to the client's data port.
PASV	Requests the server to "listen" on a data port and to wait for a connection. The response to this command includes the host and port address this server is listening on.
TYPE <type-code>	Specifies the data representation type. The <type-code> is either A (for ASCII) or I (for Image). Other values for <type-code> are not supported.
STRU <structure-code>	Specifies the structure of the transferred file. The <structure-code> is either F (for File) or R (for Record). Other values for <structure-code> are not supported. This command has no effect on the files stored.
MODE <mode-code>	Specifies the data transfer mode. Only S (for Stream) is supported.

Service Commands

Command	Description
RETR <pathname>	Causes the server to send the file specified by <pathname> from the server to the client on the data connection.
STOR <pathname>	Causes the server to accept the data transferred through the data connection and to store the data as a file with name <pathname> at the server site.
STOU	Causes the server to accept the data transferred through the data connection and to store the data as a file with a unique filename at the server site.

Command	Description
APPE <pathname>	Causes the server to accept the data transferred via the data connection and to store the data in a file specified by <pathname> at the server site. If the file specified in the pathname exists at the server site, then the data is appended to that file; otherwise, the file specified in the pathname is created at the server site.
RNFR <pathname>	Specifies the old pathname of the file/directory which is to be renamed. This command must be immediately followed by a "rename to" (RNTO) command specifying the new file pathname.
RNTO <pathname>	Specifies the new pathname of the file/directory specified in the immediately preceding "rename from" (RNFR) command. Together the two commands cause a file/directory to be renamed.
DELE <pathname>	Causes the file specified by <pathname> to be deleted at the server site.
RMD <pathname>	Causes the directory specified in <pathname> to be removed as a directory (if the pathname is absolute) or as a subdirectory of the current working directory (if the pathname is relative).
MKD <pathname>	Causes the directory specified in <pathname> to be created as a directory (if the pathname is absolute) or as a subdirectory of the current working directory (if the pathname is relative).
PWD	Causes the name of the current working directory to be returned in the reply.
LIST<pathname>	Causes a list to be sent from the server to the client. If <pathname> specifies a directory or other group of files, the server should transfer a list of files in the specified directory. If the pathname specifies a file then the server should send current information on the file. A missing <pathname> argument implies the user's current working or default directory. The details of the files are returned in Unix format not matter which platform the server is running on.
NLST <pathname>	Causes a directory listing to be sent from server to client. The <pathname> should specify a directory or other system-specific file group descriptor; a missing <pathname> argument implies the current directory. The server will return a stream of names of files and no other information. The data will be transferred over the data connection as valid pathname strings separated by <CRLF>. This command is intended to return information that can be used by a program to further process the files automatically.

Command	Description
SITE <string>	Used by the server to provide services specific to his system that are essential to file transfer but not sufficiently universal to be included as commands in the protocol. Currently, there are no available SITE commands.
SYST	Used by the client to determine the system type on which the server resides. If the system type is Windows, then a system type of WIN32 is returned. Otherwise, Unix is returned.
STAT <pathname>	Status (not available during Transfer) Causes a status response to be sent over the control connection in the form of a reply. Unlike the RFC 959 description of STAT, this command cannot be sent during a file transfer. However, this command can be sent between file transfers. If a <pathname> is specified, the command is analogous to the "list" command except that data is transferred over the control connection. If a wild-carded pathname is given, the server can respond with a list of file names and attributes associated with that pathname. If <pathname> is not given, the server returns general status information about the server FTP process. This includes current values of all transfer parameters.
HELP <string>	Causes the server to send helpful information regarding its implementation status over the control connection to the user. The command takes an optional argument (for example, any command name) and returns more specific information as a response.
NOOP	Does not affect any parameters or previously entered commands. It specifies no action other than that the server return an OK reply.

Security Extensions

Command	Description
AUTH <mechanism>	The <mechanism> parameter specifies a security mechanism. This command is only available on the FTP/s Explicit ports. • SSL or TLS-P protect the control/data channels • TLS or TLS-C clear the protection of the control/data channels It is suggested that AUTH SSL be specified for a secure connection and that this command would not be issued for the clear channel case.

Command	Description
PROT <level>	The <level> parameter specifies the Data Channel Protection Level. Values of C (for Clear) or P (for Private/Encrypted) are supported.
PBSZ <size>	Allows the FTP client and server to negotiate a maximum protected buffer size for the connection. A <size> of 0 (zero) is the only allowed size.
CCC	Sets a protected command channel to clear-text.

FTP Extensions

Command	Description

EPORT |<net-prt> <net-address>|<tcp-port>|	Allows for the specification of an extended address for the data connection. The network protocol field (<net-prt>) specifies format used for the **<net-address>** field. The <tcp-port> field specifies the client data port to use. A delimiter character (typically |) separates the fields. Example commands for IPv4 and IPv6 formats would be:
	IPv4:
	`EPRT |1|192.136.4.34|1964|`
	IPv6:
	`EPRT |2|1677::3:670:45AC:76B3|1959|`

MDTM <pathname>	Returns the file modification time of the file specified by <pathname>.
SIZE <pathname>	Returns the size, in bytes, of the file specified by <pathname>.
XMKD	Same as MKD.
XPWD	Same as PWD.
FEAT	Returns the list of supported extended commands (such as commands beyond those originally described in RFC 959).
OPTS	Allows optional command parameters to be set or reset. The Cleo Harmony and Cleo VLTrader applications currently do not offer any optional command parameters.

Command	Description
REST <position>	The REST command must be the last command issued before the data transfer command that is to cause a restarted, rather than a complete, file transfer. The <position> parameter specifies where the transfer is to be started. STREAM mode is supported (Block and Compressed are not).

Local HTTP Users Configuration

Note: This section applies to the Cleo VLTrader and Cleo Harmony applications only.

When starting your HTTP server for the first time, no users are defined and therefore no access is granted to your server. To initiate creation of HTTP users as oppposed to AS2 or ebMS peer-to-peer partners. See HTTP Service. First, activate the preconfigured "Local HTTP Users" local host. See Activating a host from a template on page 77. To create a new HTTP server login, clone the default "myTradingPartner" or another mailbox. Local HTTP user mailboxes can have actions, but unlike remote host/mailbox actions that perform remote host operations, local HTTP user actions can only perform local host operations that manipulate files within the user's home directory.

Multiple Local HTTP Users local hosts may be created allowing users to be grouped together with the same host properties; however, usernames (for example, Local HTTP user mailbox names) will remain unique across all Local HTTP Users local hosts.

Configuring Local HTTP User directories

1. Specify a **Default Root Directory**. By default, each HTTP user's home directory is a subfolder under the default root directory you specify here. Click **[...]** to browse and select a directory. Alternatively, select a custom macro variable from the drop-down menu. See Using macro variables on page 59 for a list of the applicable macros (Default Root Directory context). Once the change is applied, HTTP users already configured to use the default root are switched over to the new default root.
2. Specify the paths and names of **Local User Subdirectories**. These directories are automatically created under each user's home directory. Each directory path specified must be a relative path.

   The configured inbox and outbox directories can be easily referenced in the mailbox <collect> and <release> actions by use of the %inbox% and %outbox% macros, respectively.

   See Specifying default host directories on page 700 for more information.

   If the sentbox directory is configured, when the user retrieves a file from the configured outbox, the Cleo Harmony application places a user-accessible copy of the file in the sentbox directory. If the receivedbox directory is configured, when the user stores a file in the configured inbox, the Cleo Harmony application also places a user-accessible copy of the file in the receivedbox directory.

   Note: Files of the same name are overwritten.

   In addition to the **Inbox**, **Outbox**, **Sentbox** and **Receivedbox** folders, you can specify additional folders in the **Others** field. You can specify multiple paths (one path per line) in the **Others** field. Note that all paths must be relative and cannot include reserved macro variables (for example, %mailbox%).
3. The **Archive Directories** allow for a copy of the sent and received files to be saved in an additional location that, in most cases, is not accessible by the user. Unlike the sentbox and receivedbox configured under the **Local User Subdirectories**, these directories can be configured to point to a network location by clicking **[...]**; or a custom macro variable may be selected from the drop-down list. See Using macro variables on page 59 for a list of the applicable macros (Default Local User Archive Directory context). See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

You can use the `%mailbox%` macro as part of these directory definitions to filter files for non-LDAP users into separate subdirectories. Files written to these directories are retained with unique file names and are archived if the **Sent/Received Box Archive System Option** is enabled. See Advanced system options on page 743

Configuring access for HTTP host users

Use the **HTTP** tab to configure access for HTTP host users.

Acceptable inbound files patterns

Specify patterns that files that must match to be permitted inbound. Patterns can include wildcards and regular expressions. See Using wildcards and regular expressions on page 69. If specifying multiple file patterns, separate them with semi-colons (;) or commas (,). Alternatively, enter them on separate lines.

The following are examples of valid patterns:

- * = any file pattern
- *.* = file must have an extension
- *.edi;*.xml = only .edi and .xml extensions acceptable (case sensitive)
- [(?i).*\.(edi|xml)] = only .edi and .xml extensions acceptable (case insensitive)

Users have read-only access

Restricts HTTP users to read-only access of files and directory listings in their home directory. Users with read-only access may only retrieve files or directory listings from their home directory.

Users can overwrite files

Allows files uploaded to this host by HTTP users to overwrite existing files of the same name. When this option is disabled, existing files of the same filename are not overwritten. When this option is enabled, existing files of the same filename are overwritten.

Note: This check box is disabled when you select the **Users have read-only access** option.

Use default file name

Allows the incoming file to be given the name specified in its associated field. Use this option to override the file name specified by the sender. This feature is useful in situations where the received file name must be something other than its original file name. This field can also include any of the supported macros allowing for the incoming file to be named, for example, with a date-time stamp. See Using macro variables on page 59 (Destination File context) for a discussion of all applicable macros.

Note: This check box and field are automatically disabled when you select the **Users have read-only access** option.

Users must connect on a secure port

Limits users to SSL connections only. When selected, users will able to successfully authenticate only when an HTTP/s connection is used.

IP filter required

When you select the **IP filter required** check box, all mailboxes under this host require whitelist IP addresses to be entered. If no whitelist IP addresses are entered for a mailbox, that mailbox is set to “not ready”. If a mailbox has whitelist IP addresses entered, login to the mailbox is allowed only from the IP addresses configured. If a mailbox does not have any whitelist IP addresses entered, the mailbox user can login from anywhere.

If the **IP filter required** check box is cleared, whitelist IP addresses are not required and mailbox user can log in from anywhere.

Password Policy

Defines the security requirements that will be enforced for all local users. By default, the **Password Policy** used by all mailbox users is globally defined using the **Enforce Password Policy** option on the **System Options > Other** tab. See Other system options on page 729.

To specify a different set of security restrictions for all mailbox users defined for a particular local user host, select the **Override System Level Settings** option, select the **Enforce Password Policy** option (if not already selected), click **Configure…**, make the desired changes and click **Apply**. See Configuring password policies on page 55 for further information about Password Policy options.

To disable Password Policy enforcement for all mailbox users defined for a particular local user host, select the **Override System Level Settings** option, clear the **Enforce Password Policy** check box and click **Apply**.

Associated web portal

Designates the Portal ID of the web portal associated with this HTTP user host. Select **None** or a specific Portal ID from the drop-down list. For information on web portal setup, see Configuring VLPortal Web Browser service on page 783.

Portal Applets

If the **Portal Applets** check box is selected, manual file transfer uses applets to overcome limitations of certain browsers run by users. The **Applet transfer limit** sets the maximum number of simultaneous transfers an applet session can attempt to use to transfer a set of files and the **Users can zip uploads** option allows the user to compress the files being uploaded into a single zip file. If **Use metadata** is selected, then the metadata configured for the portal will be used to prompt the portal user for additional information. For information on web portal metadata setup, see Configuring manual file transfer metadata on page 789.

Users can view transfers for all mailboxes associated at the Trading Partner level

Select this check box to give users the option of including other mailboxes associated with the Trading Partner(s) that the users' mailbox is associated with in the File Transfer History table.

Configuring HTTP for Local HTTP Mailbox

Username

The mailbox alias. This value is used by your trading partner to log in to your HTTP server. Specify a value not already in use.

Password

The password for the mailbox. This value is used by your trading partner to log in to your HTTP server.

User SSL Client Authentication

Select this check box to enable public key-based SSL client authentication. Clear the check box to enable WWW authentication.

Certificate

If you select the **User SSL Client Authentication** check box, specify the certificate you want to use. You can click **Browse** to navigate to and select a certificate.

User Home Directory

Defaults to a username subdirectory under the default root directory defined on the **General** tab (see Configuring Local HTTP User directories on page 834). To override this path for this user only, clear the **Use Default Root \Username** check box and click the **...** button to change the home directory; or select a custom macro variable from the drop-down list. See Using macro variables on page 59 Using Macro Variables for a list of the applicable macros (Default Root Directory context).

LDAP Usergroup

Select the **LDAP Usergroup** check box to designate the mailbox as an LDAP user group mailbox and enable the Mailbox LDAP Tab (see Configuring LDAP for Local HTTP Mailbox on page 837. Many of the other

fields on this tab are disabled as they are no longer applicable. An LDAP user group mailbox has the following features:

- The mailbox no longer corresponds to a single user, but rather a group of users configured in an external directory server.
- In addition to authenticating usernames and passwords through the external directory server, user home directory paths can also be provided by the directory service, if necessary, by selecting **Use LDAP Home Directory**. If this option is not selected, and **Use Default Root\Username** is selected, the Cleo Harmony application dynamically appends the username to the root directory by way of a `%username%` macro variable.

Unlock

This button is enabled when the user has too many failed log in attempts. Mouse over the **Unlock** button to display when the user will be unlocked automatically or you must unlock the user manually. Click **Unlock** and then click **Apply** to unlock the user.

Subdirectories

Click **Subdirectories** to display the **Local User Subdirectories** dialog box. This dialog box displays host-level settings (read-only) for the current folder configuration and allows you to specify additional folders at the mailbox level in the **Mailbox-level Settings** > **Others** field. You can add multiple paths (one path per line) in the **Others** field. All paths must be relative and cannot include reserved macro variables (for example, `%mailbox%`).

Pipe Incoming Payload

Allows for this trading partner to send to your HTTP server and redirect, or pipe, the incoming payload out through a different protocol. If the transfer out to the pipe mailbox fails, the transfer into the local mailbox also fails.

Associate to Primary Mailbox

Indicates an alternate host\mailbox location for payload transfers with this trading partner. Even if the primary mailbox is specified, all transfers are still classified under the local HTTP user host\mailbox (and not the primary host\mailbox).

Configuring LDAP for Local HTTP Mailbox

Use the **LDAP** tab to specify values to for this mailbox. The **LDAP** tab is enabled when you select the **LDAP Usergroup** check box on the **HTTP** tab.

The values you specify on this tab supersede the values specified on the **LDAP Settings** or **LDAP Server** page.

Override System Settings

Select the **Override System Settings** check boxes to enable their related fields.

Base DN

The base organizational unit where the users are defined. Contact your directory administrator for the correct Base DN value. (The Base DN value entered here can be overridden in a local user host LDAP mailbox.)

The examples the table below show sample base organizational units for the supported directory types.

Directory Type	Example Base DN
Active Directory	`OU=Employees,DC=company,DC=com`
Apache Directory Services	`OU=Users,DC=example,DC=com`
Lotus Domino	`O=SCNotes`
Novell eDirectory	`O=Company Organization`

Directory Type	Example Base DN
DirX	`ou=Users,o=Company`

Search filter

Optional. Used to limit the amount of information returned from the LDAP server when many users are defined. A more restrictive filter can be specified as a comma separated list. If necessary, contact your directory administrator to determine the appropriate attributes and values. You can override the value entered here in a local user host LDAP mailbox.

The following table contains example lists with sample attribute names and values.

Search Filter	Description
`department=EDI`	Limits the search to entries that have the attribute, `department`, with a value of `EDI`.
`department=EDI,group=administrators`	Limits the search to entries that must match two attributes. The user must be in the `EDI` department and in the `administrators` group.
`department=EDI,telephoneNumber=800*`	Limits search to EDI department members with a telephone number starting with `800`.
`objectclass=person`	Limit the search to entries that are people if the Base DN contains other entries (for example, computers) and people.
`!(userAccountControl:1.2.840.113556.1.4.803:=2)`	Excludes disabled accounts - in Active Directory, if an account is disabled, bit `0x02` in the `userAccountControl` attribute value is on. `1.2.840.113556.1.4.803` is the rule object ID (ruleOID) for the LDAP bitwise `AND` operator.

If the value to search in has any of the following special characters, they must be substituted in the Search Filter with the corresponding escape sequence.

ASCII character	Escape Sequence Substitute
*	\2a
(	\28
)	\29
,	\2c
\	\5c
NUL	\00

ASCII character	Escape Sequence Substitute
/	\2f

Extend Search Filter

Used to append rules to the default search system filter. This field is enabled regardless of the status of the **Override System Options** check boxes.

List

Used to display a list of users and their attributes matching the **Base DN** and **Search Filter**.

Configuring IP Filter for Local HTTP Mailbox

Whitelist IP addresses are entered on the IP Filter tab of each local user mailbox. These IP addresses are the only addresses that will be allowed to log into the mailbox.

1. Go to the **IP Filter** tab for your HTTP mailbox.
2. Click **New** to create a new entry, or double-click an existing entry to edit it. Alternatively, you can right-click on the entry and select **Edit**.
3. Enter an IP address to be added to the whitelist.

   You can use both IPv4 and IPv6 addresses. IP addresses can be a single address or a range of addresses. The following are examples of valid IP addresses:

IP Address	Description
*	All IP addresses
10.11.12.13	Single IPv4 address matching 10.11.12.13
10.*	IPv4 addresses in the range 10.0.0.0-10.255.255.255
10.11.*	IPv4 addresses in the range 10.11.0.0-10.11.255.255
10.11.12.50-10.11.12.70	IPv4 addresses in the range 10.11.12.50-10.11.12.70
fe80::79ba:8815:4f62:e386	Single IPv6 address matching fe80::79ba:8815:4f62:e386
fe80::79ba:8815:4f62:e386-fe80::79ba:8815:4f62:ffff	IPv6 addresses in the range fe80::79ba:8815:4f62:e386-fe80::79ba:8815:4f62:ffff
fe80::79ba:8815:4f62:e386/90	IPv6 addresses matching the first 90 bits of address fe80::79ba:8815:4f62:e386

4. If necessary, remove an entry by right-clicking it and selecting **Remove**.

Local HTTP Mailbox Advanced Properties

See Setting advanced host properties on page 89 for information aobut how to use and set properties supported in all protocols. Additional available properties specific to Local HTTP Users include:

Client Type

Indicates a specific HTTP client that requires special processing of the inbound message. The default value is **no** specified client type.

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Repetitive Listener Failures

When "Email On Fail" is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, an email alert will be sent when the failure is resolved. Failure resolution email alerts will not be sent for general Listener failures since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On`

`Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Repetitive Listener Failures

When `Execute On Fail` is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, the `Execute On Fail` command will be executed again when the failure is resolved. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure. Executions of the "Execute On Fail" command for resolution of general Listener failures will not be done since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)

`\f` - form feed
`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0 - n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the mailbox should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not the Cleo Harmony or Cleo VLTrader application's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of the Cleo Harmony or Cleo VLTrader application is both the client and server (for example, a local looptest).

Possible values:

`Incoming`

`Outgoing`
`Both`

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
DES
AES-128
AES-192
AES-256
Twofish
```

Default value: `System Default`

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512
```

Default value: `System Default`

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: `On` or `Off`

Default value: `On`

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: `On` or `Off`

Default value: `On`

PGP V3 Signature

Unzip Use Path

Indicates whether or not zip entry paths should be used for `LCOPY -UNZIP` operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: `On` or `Off`

Default value: `On`

Wait For Execute On

Indicates whether execution should wait for processing to complete within an `Execute On Fail`, `Execute On Successful Copy`, `Execute On Successful Receive`, or `Execute On Successful Send` command. Note that this option does not apply to native AS400 execution.

Possible values: `On` or `Off`

Default value: `On`

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
AES-128
AES-192
AES-256
```

Default value: `System Default`

Zip Comment

Specifies the comment to be added to the zip archive file in `LCOPY -ZIP` operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for `LCOPY -ZIP` operations. If `System Default` is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

`System Default`
`9` - (Best Compression)
`8`
`7`
`6`
`5`
`4`
`3`
`2`
`1`
`0` - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for `LCOPY -ZIP -REC` operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (`*`) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: `On` or `Off`

Default value: `On`

Local HTTP Mailbox Packaging

See Configuring mailbox packaging on page 79 for information about payload file packaging.

Local HTTP Mailbox Action Commands

The HTTP Server does not independently invoke send and receive actions, but rather acts on the actions of the connected client. Default collect and release actions are provided to allow the server to make sent and received files available for processing.

Collect Action

```
#Initialize inbound file
LDELETE recvfile.edit

#Merge all files received into recvfile.edit
LCOPY -DEL -APE %inbox%/* recvfile.edi
```

Release Action

```
#Release all not yet available files
LCOPY -DEL %outbox%/../* %outbox%
```

See Composing an action on page 89 and Local command reference on page 876 for more information.

HTTP Server Command Reference

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

The HTTP Server allows users to log into the Cleo Harmony or Cleo VLTrader application and store and retrieve files using standard HTTP. A full description of the HTTP protocol can be found in the RFC 2616 specification.

The following HTTP methods and parameters are accepted and processed by the Cleo Harmony or Cleo VLTrader HTTP server (these methods and parameters are also captured in the preconfigured host, `Generic Cleo HTTPs`).

Purpose	HTTP Method	Parameters	Comments
Login	`POST`	request=connect0	Login can also occur via other requests, but if using `request=send` and `401 Unauthorized` is bounced back by Cleo Harmony or Cleo VLTrader, file content will be sent more than once.
Send	`POST`	request=send	Uploading inbound payload
Inbound		directory=	Optional parameter; defaults to `inbox/`
		filename=	Optional parameter; name of file being uploaded
Outbound Directory Listing	`POST`	request=list	Listing available outbound payload
		directory=	Optional parameter; defaults to `outbox/payload/`
Receive Outbound	`POST`	request=receive	Downloading outbound payload
		directory=	Optional parameter; defaults to `outbox/payload/`
		filename=	Name of file being requested for download
Delete Outbound	`POST`	request=delete	Deleting outbound payload
		directory=	Optional parameter; defaults to `outbox/payload`
		filename=	Name of file being deleted

The Cleo Harmony and Cleo VLTrader applications also support HTTP `PUT`, `GET`, and `DELETE` methods for sending payload, receiving directory listings and payload, and deleting payload respectively, but the `POST` methods are recommended. Following are captures of example HTTP requests and responses demonstrating the above methods. While the examples below only show parameters on the `POST` line, the Cleo Harmony and Cleo VLTrader applications do accept requests using the `application/x-www-form-urlencoded` and `multipart/form-data` Content-types.

Client initial connect request without authorization

```
POST /server?request=connect HTTP/1.1
Host: test.cleo.com:5080
```

```
Connection: Keep-Alive, TE
TE: trailers, deflate, gzip, compress
User-Agent: RPT-HTTPClient/0.3-3I (Windows XP)
Content-length: 0
```

Cleo Harmony or Cleo VLTrader application response (unauthorized; both basic and digest Authentication is enabled)

```
HTTP/1.1 401 Unauthorized
Server: Cleo VLTrader/3.5 (Windows 2000)
Date: Tue, 22 May 2007 17:04:13 GMT
WWW-Authenticate: Basic realm="Cleo VLTrader"
WWW-Authenticate: Digest realm="Cleo VLTrader",domain="/
server",qop="auth",nonce="0qenmpn44",opaque="4b4c37373332"
Connection: close
Content-Type: text/html
Content-Length: 80
<html><head><title> Unauthorized</title></head><body> Unauthorized</body></
html>
```

Client connect request with digest authorization

```
POST /server?request=connect HTTP/1.1
Host: test.cleo.com:5080
Connection: TE
TE: trailers, deflate, gzip, compressUser-Agent: RPT-HTTPClient/0.3-3I
 (Windows XP)
Authorization: Digest realm="Cleo VLTrader",username="cleo",uri="/server
%3Frequest=connect",nonce="0qenmpn44",response="b4f7542bdedce937de6aa93078fcdf17",opaque
Content-length: 0
```

Cleo Harmony or Cleo VLTrader application response (authentication successful)

```
HTTP/1.1 200 OK
Server: Cleo VLTrader/3.5 (Windows 2000)
Date: Tue, 22 May 2007 17:04:18 GMT
Content-Length: 0
Set-cookie: jSessionId=3513ld61kg8bt; path=/
Connection: keep-alive
```

Client send (upload) request

```
POST /server?request=send&directory=inbox%2F HTTP/1.1
Host: test.cleo.com:5080
Connection: TE
TE: trailers, deflate, gzip, compress
User-Agent: RPT-HTTPClient/0.3-3I (Windows XP)
Cookie: jSessionId=3513ld61kg8bt
Cookie2: $Version="1"
Authorization: Digest realm="Cleo VLTrader",username="cleo",uri=...
Content-type: application/octet-stream; name="test.edi"
Content-length: 1533
...payload...
```

Cleo Harmony or Cleo VLTrader application response (send successful)

```
HTTP/1.1 200 OK
```

```
Server: Cleo VLTrader/3.5 (Windows 2000)
Date: Tue, 22 May 2007 17:19:59 GMT
Content-Type: text/html
Content-Length: 84
Connection: keep-alive
<html><head><title>OK</title></head><body>File successfully uploaded.</
body></html>
```

Client list request

```
POST /server?request=list&directory=outbox%2Fpayload%2F HTTP/1.1
Host: test.cleo.com:5080
Connection: TE
TE: trailers, deflate, gzip, compress
User-Agent: RPT-HTTPClient/0.3-3I (Windows XP)
Cookie: jSessionId=3513ld61kg8bt
Cookie2: $Version="1"
Authorization: Digest realm="Cleo VLTrader",username="cleo",uri=...
Content-length: 0
```

Cleo Harmony or Cleo VLTrader application response (listing successful)

```
HTTP/1.1 200 OK
Server: Cleo VLTrader/3.5 (Windows 2000)
Date: Tue, 22 May 2007 17:04:18 GMT
Content-Type: text/html
Content-Length: 402
Connection: keep-alive
<head><title>'cleo' mailbox</title></head><body><pre><H2>Download</H2>Server
 directory: outbox/payload/<hr>
2007/05/03 08:43:17   1.497kB <A HREF="/server/outbox/payload/test.edi"
 >test.edi</A><br>
2007/05/22 08:32:46   4.491kB <A HREF="/server/outbox/payload/test2.edi"
 >test2.edi</A><br>
2007/05/22 08:33:28  28.444kB <A HREF="/server/outbox/payload/test3.edi"
 >test3.edi</A><br><hr></pre></body>
```

Client receive (download) request

```
POST /server?request=receive&directory=outbox%2Fpayload&filename=test.edi
 HTTP/1.1
Host: test.cleo.com:5080
Connection: TE
TE: trailers, deflate, gzip, compress
User-Agent: RPT-HTTPClient/0.3-3I (Windows XP)
Cookie: jSessionId=3513ld61kg8bt
Cookie2: $Version="1"
Authorization: Digest realm="Cleo VLTrader",username="cleo",uri=...
Content-length: 0
```

Cleo Harmony or Cleo VLTrader application response (receive successful)

```
HTTP/1.1 200 OK
Server: Cleo VLTrader/3.5 (Windows 2000)
Date: Tue, 22 May 2007 17:25:57 GMT
Content-Description: test.edi
Content-Disposition: attachment; filename="test.edi"
```

```
Transfer-Encoding: chunked
Content-Type: application/edi-x12; name="test.edi"
Connection: keep-alive
...chunked payload...
```

Client delete request

```
POST /server?request=delete&directory=outbox%2Fpayload&filename=test.edi
 HTTP/1.1
Host: test.cleo.com:5080
Connection: TE
TE: trailers, deflate, gzip, compress
User-Agent: RPT-HTTPClient/0.3-3I (Windows XP)
Cookie: jSessionId=3513ld61kg8bt
Cookie2: $Version="1"
Authorization: Digest realm="Cleo VLTrader",username="cleo",uri=...
Content-length: 0
```

Cleo Harmony or Cleo VLTrader application response (delete successful)

```
HTTP/1.1 200 OK
Server: Cleo VLTrader/3.5 (Windows 2000)
Date: Tue, 22 May 2007 17:25:58 GMT
Content-Length: 0
Connection: keep-alive
```

A web browser can also be used by a trading partner to manually trade with VerasLex's HTTP server. A trading partner would use the Cleo Harmony or Cleo VLTrader address and HTTP server resource path to start (for example, `https://test.cleo.com:6080/server`):

After logging in, a simple web page is displayed to allow uploading and downloading of files.

Note: For information about a more robust web portal interface, see Configuring VLPortal Web Browser service on page 783.

Local SSH FTP Users configuration

Note: This feature is being deprecated. For similar functionality, use a Users host. See Users Host on page 516 for more information.

Note: This section applies to the Cleo VLTrader and Cleo Harmony applications only.

When starting the SSH FTP server for the first time, no users are defined and therefore no access is granted to your server. To initiate creation of SSH FTP users, first activate the preconfigured Local SSH FTP Users local host. See Activating a host from a template on page 77. To create a new SSH FTP server login, **clone** the default "myTradingPartner" or another mailbox. Local SSH FTP user mailboxes can have actions, but unlike remote host/mailbox actions that perform remote host operations, local SSH FTP user actions can only perform local host operations that manipulate files within the user's home directory.

Multiple Local SSH FTP Users local hosts may be created allowing users to be grouped together with the same host properties; however, usernames (that is, Local SSH FTP user mailbox names) will remain unique across all Local SSH FTP Users local hosts.

Configuring local SSH FTP user directories

1. Specify a **Default Root Directory**. By default, each SSH FTP user's home directory is a subfolder under the default root directory specified here. Click **[...]** to browse and select a directory. Alternatively, select a custom

macro variable from the drop-down menu. See Using macro variables on page 59 for a list of the applicable macros (Default Root Directory context). Once the change is applied, SSH FTP users already configured to use the default root are switched over to the new default root.

2. Specify the paths and names of **Local User Subdirectories**. These directories are automatically created under each user's home directory. Each directory path specified must be a relative path.

   The configured inbox and outbox directories can be easily referenced in the mailbox `<collect>`and `<release>` actions by use of the `%inbox%` and `%outbox%` macros, respectively. See Configuring local FTP users on page 809.

   See Specifying default host directories on page 700 for more information.

   If the sentbox directory is configured, when the user retrieves a file from the configured outbox, the Cleo Harmony application places a user-accessible copy of the file in the sentbox directory. If the receivedbox directory is configured, when the user stores a file in the configured inbox, the Cleo Harmony application also places a user-accessible copy of the file in the receivedbox directory.

   Note: Files of the same name are overwritten.

   In addition to the **Inbox**, **Outbox**, **Sentbox** and **Receivedbox** folders, additional folders can be specified in the **Others** field. Multiple paths can be added (one path per line) in the **Others** field. Note that all paths must be relative and cannot include reserved macro variables (for example, `%mailbox%`).

3. The **Archive Directories** allow for a copy of the sent and received files to be saved in an additional location that, in most cases, is not accessible by the user. Unlike the sentbox and receivedbox configured under the **Local User Subdirectories**, these directories can be configured to point to a network location by clicking **[...]**; or a custom macro variable may be selected from the drop-down list. See Using macro variables on page 59 for information about applicable macros (Default Local User Archive Directory context). See Specifying default host directories on page 700 for information about setting up system-level directories and custom directory macro variables.

   You can use the `%mailbox%` macro as part of these directory definitions to filter files for non-LDAP users into separate subdirectories. Files written to these directories are retained with unique file names and are archived if the Sent/Received Box Archive System Option is enabled. See Other system options on page 729

Configuring access for SSH FTP host users

Use the **SSH FTP** tab to configure access for SSH FTP host users.

Acceptable inbound file patterns

Specify patterns that files must match to be permitted inbound. Patterns can include wildcards and regular expressions. See Using wildcards and regular expressions on page 69. If you specify multiple file patterns, separate them with semi-colons (;) or commas (,). Alternatively, enter them on separate lines.

The following are examples of valid patterns:

- * = any file pattern
- *.* = file must have an extension
- *.edi;*.xml = only .edi and .xml extensions acceptable (case sensitive)
- [(?i).*\.(edi|xml)] = only .edi and .xml extensions acceptable (case insensitive)

Users have read-only access

Restricts SSH FTP users to read-only access of files and directory listings in their home directory. Users with read-only access may only retrieve files or directory listings from their home directory.

When you select this option, the **Users can make/remove subdirectories** check box is disabled and any previously selected setting is cleared.

Users can make/remove subdirectories

Enables SSH FTP users to make and remove subdirectories within their home directory

This check box is disabled when you select the **Users have read-only access** option.

Users must connect on a secure port

Limits users to SSL connections only. When selected, users will able to successfully authenticate only when an FTP/s connection is used.

IP filter required

When you select the **IP filter required** check box, all mailboxes under this host require whitelist IP addresses to be entered. If no whitelist IP addresses are entered for a mailbox, that mailbox is set to `not ready`. For the mailboxes that have whitelist IP addresses entered, the mailbox user can log in to the mailbox only from the IP addresses configured. If the **IP filter required** check box is cleared, whitelist IP addresses are not required and the mailbox user can log in from anywhere.

Password Policy

Defines the security requirements that will be enforced for all local users. By default, the **Password Policy** used by all mailbox users is globally defined via the **Enforce Password Policy** option on the **System Options > Other** tab. See Other system options on page 729.

To specify a different set of security restrictions for all mailbox users defined for a particular local user host: select the **Override System Level Settings** option, select the **Enforce Password Policy** option (if not already selected), click **Configure**, make the changes and click **Apply**. See Configuring password policies on page 55 for further information on the **Password Policy** options.

To disable **Password Policy** enforcement for all mailbox users defined for a particular local user host: select the **Override System Level Settings** option, clear the **Enforce Password Policy** option and click **Apply**.

Field Name	Description
Acceptable inbound files patterns	Specified patterns files must match to be permitted inbound. Patterns can include wildcards and regular expressions. See Using wildcards and regular expressions on page 69. If you specify multiple file patterns, separate them with semi-colons (;) or commas (,). Alternatively, enter them on separate lines. The following are examples of valid patterns: • * = any file pattern • *.* = file must have an extension • *.edi;*.xml = only .edi and .xml extensions acceptable (case sensitive) • [(?i).*\.(edi|xml)] = only .edi and .xml extensions acceptable (case insensitive)
Users have read-only access	Restricts SSH FTP users to read-only access of files and directory listings in their home directory. Users with read-only access may only retrieve files or directory listings from their home directory.

Field Name	Description
IP filter required	When you select the **IP filter required** check box, all mailboxes under this host require whitelist IP addresses to be entered. If no whitelist IP addresses are entered for a mailbox, that mailbox is set to “not ready”. If a mailbox has whitelist IP addresses entered, login to the mailbox is allowed only from the IP addresses configured. If a mailbox does not have any whitelist IP addresses entered, the mailbox user can login from anywhere. If the **IP filter required** check box is cleared, whitelist IP addresses are not required and mailbox user can log in from anywhere.
Password Policy	Defines the security requirements that will be enforced for all local users. By default, the **Password Policy** used by all mailbox users is globally defined using the **Enforce Password Policy** option on the Other system options on page 729 tab. To specify a different set of security restrictions for all mailbox users defined for a particular local user host, select the **Override System Level Settings** option, select the **Enforce Password Policy** option (if not already selected), click **Configure**, make the desired changes and click **Apply**. See Enhanced Security for further information on the **Password Policy** options. To disable **Password Policy** enforcement for all mailbox users defined for a particular local user host, select the**Override System Level Settings** option, clear the **Enforce Password Policy** check box and click **Apply**.

Configuring SHH FTP for local SHH FTP mailbox

Username

The mailbox alias. This value is used by your trading partner to log in to your FTP server. Specify a value not already in use.

Password

The password for the mailbox. This value is used by your trading partner to log in to your FTP server.

Use Public Key Authentication

Select the check box to enable public key authentication and specify the name of the file containing the client's authentication certificate (the remote client certificate to be used for authentication). You can click **Browse** to navigate to and select the file you want to use.

Use Key From File

Select the check box to enable use of the client's SSH public key and specify the name of the file containing the key. You can click **Browse** to navigate to and select the file you want to use.

Note: The file you select could contain multiple keys in the supported formats (RFC 4716 and OpenSSH). A file with multiple keys can contain either RSA or DSA keys of different sizes. The two formats cannot be mixed within a file. Keys must be separated by an `LF` or `CRLF`.

LDAP Usergroup

Select the **LDAP Usergroup** check box to designate the mailbox as an LDAP user group mailbox and enable the Mailbox LDAP Tab (see Configuring LDAP for Local FTP Mailbox on page 816. Many of the other fields on this tab are disabled as are no longer applicable. An LDAP user group mailbox has the following features:

- The mailbox no longer corresponds to a single user, but rather a group of users configured in an external directory server.

- In addition to authenticating usernames and passwords through the external directory server, user home directory paths can also be provided by the directory service, if necessary, by selecting **Use LDAP Home Directory**. If this option is not selected, and **Use Default Root\Username** is selected, the Cleo Harmony application dynamically appends the username to the root directory by way of a `%username%` macro variable.

Unlock

This button is enabled when the user has too many failed log in attempts. Mouse over the **Unlock** button to display when the user will be unlocked automatically or you must unlock the user manually. Click **Unlock** and then click **Apply** to unlock the user.

User Home Directory

Defaults to a username subdirectory under the default root directory defined on the **General** tab (see Configuring local SSH FTP user directories on page 851). To override this path for this user only, clear the **Use Default Root\Username** check box and click the **...** button to change the home directory; or select a custom macro variable from the drop-down list. See Using macro variables on page 59 Using Macro Variables for a list of the applicable macros (Default Root Directory context).

Subdirectories

Click **Subdirectories** to display the **Local User Subdirectories** dialog box. This dialog box displays host-level settings (read-only) for the current folder configuration and allows you to specify additional folders at the mailbox level in the **Mailbox-level Settings** > **Others**

field. You can add multiple paths separated by commas, semi-colons, or carriage returns. All paths must be relative and cannot include reserved macro variables (for example, `%mailbox%`).

Pipe Incoming Payload

Allows for this trading partner to send to your FTP server and redirect, or pipe, the incoming payload out through a different protocol. If the transfer out to the pipe mailbox fails, the transfer into the local mailbox also fails.

1. The SSH FTP server supports either public key or password based authentications.

   a. **Password Authentication:** Enter the user's **Password**. You will be asked to confirm the password when applying (once applied, the displayed length of the masked password will not necessarily represent the actual password length).

   b. **Public Key Authentication using a CA Certificate:** Specify the name of the file containing the Client's Authentication Certificate (the remote client certificate to be used for authentication) by clicking **Browse**. Find the certificate that matches the one received from your trading partner and click **Select**.

   c. **Public Key Authentication using a SSH Public Key File:** Specify the name of the file containing the Client's SSH Public Key file by clicking **Browse**. Find the SSH Public Key file that matches the one received from your trading partner and click **Select**.

   Note: The file selected may contain multiple keys in the supported formats (RFC 4716 and OpenSSH). A file with multiple keys can contain either RSA or DSA keys of different sizes. The two formats cannot be mixed within a file. Keys must be separated by an LF or CRLF.

2. To designate the mailbox as an LDAP user group mailbox select the **LDAP Usergroup** check box. Selecting this check box will enable the **Mailbox LDAP** tab (see Configuring LDAP for Local HTTP Mailbox on page 837) and disable most of the fields above as they are no longer applicable. An LDAP user group mailbox has the following features:

   a. The mailbox no longer corresponds to a single user, but rather a group of users configured in an external directory server.

   b. In addition to authenticating usernames and passwords through the external directory server, user home directory paths can also be optionally provided by the directory service by selecting **Use LDAP Home Directory**. If this option is not selected, and **Use Default Root\Username** is selected, the Cleo Harmony

application will dynamically append the username to the root directory by way of a `%username%` macro variable.

3. If the user has too many failed login attempts, then **Unlock** will be enabled. Holding the mouse over **Unlock** will display when the user will be unlocked automatically or if it must manually be unlocked. Selecting **Unlock** and then **Apply** will unlock the user.

Configuring LDAP for local SSH FTP mailbox

Use the **LDAP** tab to specify values for this mailbox. The **LDAP** tab is enabled when you select the **LDAP Usergroup** check box on the **SSH FTP** tab.

The values you specify on this tab supersede the values specified on the **LDAP Settings** or **LDAP Server** page.

Override System Settings

Select the **Override System Settings** check boxes to enable their related fields.

Base DN

The base organizational unit where the users are defined. Contact your directory administrator for the correct Base DN value. (The Base DN value entered here can be overridden in a local user host LDAP mailbox.)

The examples the table below show sample base organizational units for the supported directory types.

Directory Type	Example Base DN
Active Directory	`OU=Employees,DC=company,DC=com`
Apache Directory Services	`OU=Users,DC=example,DC=com`
Lotus Domino	`O=SCNotes`
Novell eDirectory	`O=Company Organization`
DirX	`ou=Users,o=Company`

Search filter

Optional. Used to limit the amount of information returned from the LDAP server when many users are defined. A more restrictive filter can be specified as a comma separated list. If necessary, contact your directory administrator to determine the appropriate attributes and values. You can override the value entered here in a local user host LDAP mailbox.

The following table contains example lists with sample attribute names and values.

Search Filter	Description
`department=EDI`	Limits the search to entries that have the attribute, `department`, with a value of `EDI`.
`department=EDI,group=administrators`	Limits the search to entries that must match two attributes. The user must be in the `EDI` department and in the `administrators` group.
`department=EDI,telephoneNumber=800*`	Limits search to EDI department members with a telephone number starting with `800`.

Search Filter	Description
`objectclass=person`	Limit the search to entries that are people if the Base DN contains other entries (for example, computers) and people.
`!(userAccountControl:1.2.840.113556.1.4.803:=2)`	Excludes disabled accounts - in Active Directory, if an account is disabled, bit `0x02` in the `userAccountControl` attribute value is on. `1.2.840.113556.1.4.803` is the rule object ID (ruleOID) for the LDAP bitwise `AND` operator.

If the value to search in has any of the following special characters, they must be substituted in the Search Filter with the corresponding escape sequence.

ASCII character	Escape Sequence Substitute
*	\2a
(	\28
)	\29
,	\2c
\	\5c
NUL	\00
/	\2f

Extend Search Filter

Used to append rules to the default search system filter. This field is enabled regardless of the status of the **Override System Options** check boxes.

List

Used to display a list of users and their attributes matching the **Base DN** and **Search Filter**.

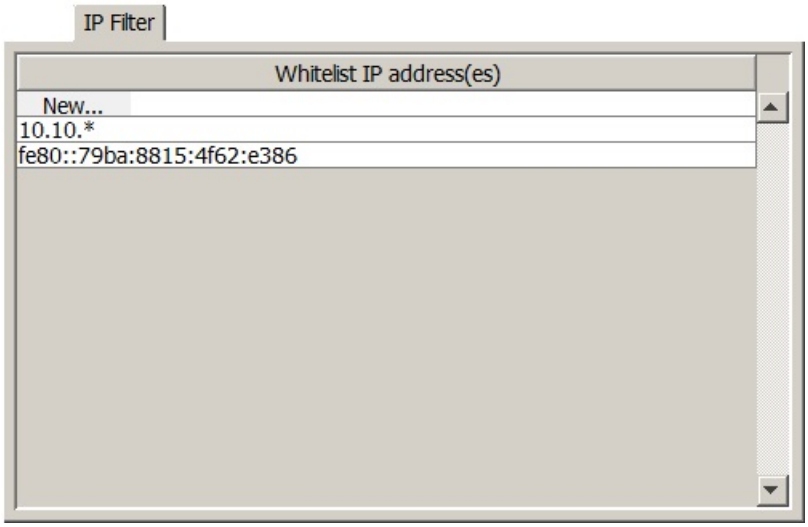
If necessary, **Override System Options** settings for **Base DN** and **Search Filter** (see LDAP server on page 691) in order to match the intended set of users for this mailbox. Or the **Extend Search Filter** can be used to append rules to the default system search filter.

Use the **List** button to list the users and their attributes matching the Base DN and Search Filter.

Configuring IP filter for local SSH FTP mailbox

Whitelist IP addresses are entered on the IP Filter tab of each local user mailbox. These IP addresses are the only addresses that will be allowed to log into the mailbox.

1. Go to the **IP Filter** tab for your SSH FTP mailbox.



2. Click **New** to create a new entry or double-click an existing entry to edit it. Alternatively, you can right-click on the entry and select **Edit**.
3. Enter an IP address to be added to the whitelist.

   You can use both IPv4 and IPv6 addresses. IP addresses can be a single address or a range of addresses. The following are examples of valid IP addresses:

IP Address	Description
*	All IP addresses
10.11.12.13	Single IPv4 address matching 10.11.12.13
10.*	IPv4 addresses in the range 10.0.0.0-10.255.255.255
10.11.*	IPv4 addresses in the range 10.11.0.0-10.11.255.255
10.11.12.50-10.11.12.70	IPv4 addresses in the range 10.11.12.50-10.11.12.70
fe80::79ba:8815:4f62:e386	Single IPv6 address matching fe80::79ba:8815:4f62:e386
fe80::79ba:8815:4f62:e386-fe80::79ba:8815:4f62:ffff	IPv6 addresses in the range fe80::79ba:8815:4f62:e386-fe80::79ba:8815:4f62:ffff
fe80::79ba:8815:4f62:e386/90	IPv6 addresses matching the first 90 bits of address fe80::79ba:8815:4f62:e386

4. If necessary, remove an entry by right-clicking it and selecting **Remove**.

Local SSH FTP mailbox advanced properties

See Setting advanced host properties on page 89 for information about how to use and set the properties supported in all protocols. Additional available properties specific to Local SSH FTP Users include:

Email On Check Conditions Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Check Conditions Not Met

Send an email notification after running a `CHECK` command where the overall conditions of the check are **not** met. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Fail

If an error occurs during a command, email the error condition. See Email/Execute Based on Results.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Flag

If a flagged event occurs, email the event. See Configuring email or execute based on results on page 57.

Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Possible values: Email addresses separated by commas (,), semicolons (;), or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Repetitive Action Failures

When "Email On Fail" is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. When the failure is resolved an email alert will be sent.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Repetitive Listener Failures

When "Email On Fail" is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses emailing of the same alert multiple times. If the same email alert continues to be suppressed after 24 hours, the suppressed email alert will be sent every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, an email alert will be sent when the failure is resolved. Failure resolution email alerts will not be sent for general Listener failures since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple emails if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Email On Successful Copy

Send an email notification after copying a file using `LCOPY`. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Receive

Send an email notification after successfully receiving a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Email On Successful Send

Send an email notification after successfully sending a file. See Configuring email or execute based on results on page 57.

Possible values: Email addresses separated by commas (,), semicolons (;) or colons (:). The first address should be an internal email address.

Default value:The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Met

After executing a `CHECK` command where the overall conditions are met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Note: Note that if multiple files contribute to the conditions being met, and one of the file macros is in the command (e.g., `%file%`), the system command will be executed repeatedly - once for each file.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Check Conditions Not Met

After executing a `CHECK` command where the overall conditions are *not* met, run a system command. See Configuring email or execute based on results on page 57.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Fail

If an error occurs during a command, run a system command. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Repetitive Action Failures

When `Execute On Fail` is enabled and the same failure occurs each time an action is run for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after a system restart if the failure occurs again. When the

failure is resolved, the `Execute On Fail` command will be executed again. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Repetitive Listener Failures

When `Execute On Fail` is enabled and the same failure occurs each time an inbound message is processed by the Listener for a specific host, leaving this option unchecked suppresses multiple executions of the `Execute On Fail` command. If suppression of execution of the command for this failure continues after 24 hours, the suppressed `Execute On Fail` command will be executed every 24 hours and after every system restart if the failure occurs again. If the failure can be associated with a specific host, the `Execute On Fail` command will be executed again when the failure is resolved. Users must account for this by including the %status% macro variable for the `Execute On Fail` command (see Using macro variables on page 59) and then checking for a success or failure. Executions of the "Execute On Fail" command for resolution of general Listener failures will not be done since it is not possible to determine that these types of failures have been resolved.

Note: This feature only suppresses multiple executions of the `Execute On Fail` command if the same failure occurs multiple times in a row. Suppression is not maintained across synchronized hosts.

Possible values: `On` or `Off`

Default value: `On`

Execute On Successful Copy

After successfully copying a file using `LCOPY`, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Receive

After successfully receiving a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Execute On Successful Send

After successfully sending a file, run a system command. This command may be used for post-processing the file. See Configuring email or execute based on results on page 57.

Possible values: System command to be executed.

Default value: The value specified for this property on the **Options > Advanced** panel (if set).

Fixed Record EOL Characters

End-of-line characters to be inserted and/or deleted.

Possible values: `0` to *n* characters.

Special character sequences:

`\r` - carriage return
`\n` - new line (linefeed)
`\f` - form feed

`\t` - horizontal tab
`\0` - null
`\\` - backslash

Fixed Record Incoming Delete EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to look for and delete EOL characters while receiving a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Incoming Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while receiving a file.

Fixed Record Incoming Delete EOL and Fixed Record Incoming Insert EOL are mutually exclusive properties.

Possible values: `On` or `Off`

Default value: `Off`

Fixed Record Length

The fixed record length after which end-of-line characters need to be inserted and/or deleted.

Possible values: `0 - n`

Default value: `0`

Fixed Record Outgoing Insert EOL

If Fixed Record EOL Characters has been specified and Fixed Record Length is greater than 0, indicates to insert EOL characters while sending a file.

Note: When using FTP ASCII mode, standard EOL characters may already be changing if transferring between Windows and Unix platforms.

Possible values: `On` or `Off`

Default value: `Off`

High Priority

Indicates whether incoming and/or outgoing transfers through the mailbox should be treated as high priority. When both high priority and regular priority transfers are active, the high priority transfers get a larger portion of the available bandwidth. Go to **Configure > Options > Other** to set the `High Priority Transfers Percentage Available Bandwidth` (defaults to 75). See Other system options on page 729 for more information.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Warning: If the trading partner's bandwidth (and not the Cleo Harmony or Cleo VLTrader application's) is limiting the transfer rate, then setting High Priority will not increase the transfer rate and will only result in potentially slowing down other Cleo Harmony or Cleo VLTrader transfers. Also, do not attempt to set High Priority Incoming or Outgoing on a host where the same instance of the Cleo Harmony or Cleo VLTrader application is both the client and server (for example, a local looptest).

Possible values:

`Incoming`
`Outgoing`

`Both`

Include Failure In Subject Of Email

When specified, the exception message will be included in the email that is generated on failure.

Note: If the exception message exceeds 256 characters, it will be truncated.

Possible values: `On` or `Off`

Default value: The value specified for this property on the **Options > Advanced** panel

Interim File Extension

When applicable, specifies the temporary filename extension that a trading partner's client software uses while transferring a file inbound (e.g. WinSCP .filepart). For the transfer logging feature, the Cleo Harmony application will set the transfer status to `Interim Success` rather than `Success` when a transfer with a temporary filename extension is finished. Then, when the trading partner client software renames the file using SFTP to strip off the temporary filename extension, the Cleo Harmony application will insert an additional `Success` entry into the transfer log with the resulting filename, thus marking the transfer as complete. The dot preceding the extension can be included in the configured value, but it is not required. If multiple temporary filename extensions are used, they can be separated by commas or semicolons.

LCOPY Archive

If specified, contains the directory for archiving `LCOPY` source files.

Possible values: Any local or shared directory. Macros can be used. See Using macro variables on page 59 (LCOPY Archive context).

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Log Individual LCOPY Results To Transfer Logging

When this option is enabled, a `<send>` and `<receive>` result is logged to the transfer log for each file copied.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `Off`

Macro Date Format

Specifies the date format to be used when the `%date%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Macro Time Format

Specifies the time format to be used when the `%time%` macro is used.

Possible values: See Using macro variables on page 59 for information about usage and possible date/time formats.

Default value: The value specified for this property on the **Options > Advanced** panel, if any.

Maximum Concurrent FTP Logins

The total number of logins allowed at any one time for this user. With the default value of 0, the number of concurrent connections per user will be limited by the Maximum Concurrent FTP Logins Per User setting. A value other than zero will override the Maximum Concurrent FTP Logins Per User setting for this user. See Specifying Local Listener advanced properties on page 759

Maximum Incoming Transfer Rate (kbytes/s)

Sets the maximum incoming transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The Maximum Incoming Transfer Rate system setting might also limit the transfer rates. The system Maximum Incoming Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers also affects individual transfer rates. See Advanced system options on page 743.

Possible values: `0 - n`

Default value: `0`

Maximum Outgoing Transfer Rate (kbytes/s)

Sets the maximum outgoing transfer rate in Kbytes (1024 bytes) per second for each mailbox or host. The default value of `0` does not limit the transfer rate. The system setting might also limit the transfer rates. The system Maximum Outgoing Transfer Rate value is used unless this setting is more restrictive. For simultaneous transfers, the number of active transfers will also affect individual transfer rates. See Advanced system options on page 743 for more information about Maximum Outgoing Transfer Rate.

Possible values: `0 - n`

Default value: `0`

Outbox Sort

Controls the order in which multiple files are transferred for a `PUT` command. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence. For `Alphabetical` ordering, the file extensions are not used to determine the sorted order unless they are needed to make the filenames unique.

Possible values:

```
System Default
Alphabetical
Date/Time Modified
```

Default value: `System Default`

PGP Compression Algorithm

Compression method used when OpenPGP packaging (with compression) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab is in effect.

Possible values:

```
System Default
ZIP
ZLIB
```

Default value: `System Default`

PGP Encryption Algorithm

Encryption method used when OpenPGP packaging (with encryption) is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. If `System Default` is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

```
System Default
TripleDES
Blowfish
CAST5
```

DES
AES-128
AES-192
AES-256
Twofish

Default value: System Default

PGP Hash Algorithm

Signing method used when OpenPGP packaging (with signing) is requested through the Configuring mailbox packaging on page 79. If System Default is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

System Default
MD2
MD5
RIPE-MD-160
SHA-1
SHA-256
SHA-384
SHA-512

Default value: System Default

PGP Integrity Check

When OpenPGP encrypting (see Configuring mailbox packaging on page 79), include an integrity check on encrypted data. Can be disabled for compatibility with certain OpenPGP implementation.

Possible values: On or Off

Default value: On

PGP Signature Verification

Indicates whether or not signed inbound PGP messages should be verified when inbound OpenPGP packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79. In general, this property should be enabled.

Possible values: On or Off

Default value: On

PGP V3 Signature

Unzip Use Path

Indicates whether or not zip entry paths should be used for LCOPY -UNZIP operations. When enabled, the entry's path is added to the destination path, unless the entry contains an absolute path. In this case, the absolute path is used in place of the destination path.

Possible values: On or Off

Default value: On

Wait For Execute On

Indicates whether execution should wait for processing to complete within an Execute On Fail, Execute On Successful Copy, Execute On Successful Receive, or Execute On Successful Send command. Note that this option does not apply to native AS400 execution.

Possible values: On or Off

Default value: On

XML Encryption Algorithm

The method used to encrypt/decrypt files when XML Encryption packaging is requested through the **Mailbox Packaging** tab. See Configuring mailbox packaging on page 79 . If System Default is specified, the value set on the **Configure > Options > Advanced** tab takes precedence.

Possible values:

System Default
TripleDES
AES-128
AES-192
AES-256

Default value: System Default

Zip Comment

Specifies the comment to be added to the zip archive file in LCOPY -ZIP operations.

Default value: The value specified for this property on the **Options > Advanced** panel, if set.

Zip Compression Level

Controls the level of compression for LCOPY -ZIP operations. If System Default is specified, the value set on the **Configure > Options > Advanced** takes precedence

Possible values:

System Default
9 - (Best Compression)
8
7
6
5
4
3
2
1
0 - (No Compression)

Default value: System Default

Zip Subdirectories Into Individual Zip Files

Indicates whether or not subdirectories should be bundled for LCOPY -ZIP -REC operations. When enabled, each first-level subdirectory (and all of its descendents) will be bundled together into an individual zip file. The name of this zip file may optionally reflect the subdirectory name if an asterisk (*) is placed in the destination path. Any files that are directly off the source root directory will not be copied.

Possible values: On or Off

Default value: On

Local SSH FTP mailbox packaging

See Configuring mailbox packaging on page 79 for information about payload file packaging.

Local SSH FTP mailbox action commands

The SSH FTP Server does not independently invoke send and receive actions, but rather acts on the actions of the connected client. Default collect and release actions are provided to allow the server to make sent and received files available for processing.

Collect Action

```
#Initialize inbound file
LDELETE recvfile.edit

#Merge all files received into recvfile.edit
LCOPY -DEL -APE %inbox%/* recvfile.edi
```

Release Action

```
#Release all not yet available files
LCOPY -DEL %outbox%/../* %outbox%
```

See Composing an action on page 89 and Local command reference on page 876 for more information.

SSH FTP Server command reference

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

The SSH FTP Server allows users to log into the Cleo Harmony application and store and retrieve files using standard SSH FTP (Secure Shell File Transfer Protocol) commands. A full description of the SSH FTP commands can be found in the Internet-Draft draft-ietf-secsh-filexfer-02.txt specification.

The following SSH FTP packet types are accepted and processed by the Cleo Harmony FTP server. The **id** field of each request or response has been omitted in the following descriptions. See SSH FTP file attributes on page 875 for information about the <ATTRS attrs> parameter used in some of the commands.

Command	Description
Requests from the Client to the SSH FTP Server	
`SSH_FXP_INIT` *<uint32 version>* *<optional extension data>*	Sent by the client when the transfer protocol starts. The client must be capable of supporting version 3 of the SSH FTP protocol. The server responds with a `SSH_FXP_VERSION` packet.
`SSH_FXP_VERSION` *<uint32 version>* *<optional extension data>*	Response to the SSH_FXP_INIT request.

Command	Description
SSH_FXP_OPEN <*string filename*> <*uint32 pflags*> <*ATTRS attrs*>	Files are opened or created when the client sends this message where filename field specifies the file name. The pflags field is a bitmask. The bits are defined as follows: SSH_FXF_READ 0x00000001 SSH_FXF_WRITE 0x00000002 SSH_FXF_APPEND 0x00000004 SSH_FXF_CREAT 0x00000008 SSH_FXF_TRUNC 0x00000010 SSH_FXF_EXCL 0x00000020 These have the following meanings: SSH_FXF_READ - Open the file for reading. SSH_FXF_WRITE - Open the file for writing. If both this and SSH_FXF_READ are specified, the file is opened for both reading and writing. SSH_FXF_APPEND - Force all writes to append data at the end of the file. SSH_FXF_CREAT - If this flag is specified, then a new file will be created if one does not already exist (if O_TRUNC is specified, the new file will be truncated to zero length if it previously exists). SSH_FXF_TRUNC - Forces an existing file with the same name to be truncated to zero length when creating a file by specifying SSH_FXF_CREAT. SSH_FXF_CREAT ***must*** also be specified if this flag is used. SSH_FXF_EXCL - Causes the request to fail if the named file already exists. SSH_FXF_CREAT ***must*** also be specified if this flag is used. The server response to this message will be either SSH_FXP_HANDLE (if successful) or SSH_FXP_STATUS (if the operation fails).
SSH_FXP_CLOSE <*string handle*>	A file is closed when the client sends this request. The server response to this request will be a SSH_FXP_STATUS message. The handle parameter is a handle previously returned in response to a SSH_FXP_OPEN or SSH_FXP_OPENDIR.

Command	Description
SSH_FXP_READ <*string handle*> <*uint64 offset*> <*uint32 len*>	Once a file has been opened, it can be read using the SSH_FXP_READ message. Only sequential offsets are supported, and repositioning within an open file is not allowed. In response to this request, the server will read as many bytes as it can from the file (up to 'len'), and return them in a SSH_FXP_DATA message. If an error occurs or EOF is encountered before reading any data, the server will respond with SSH_FXP_STATUS.
SSH_FXP_WRITE <*string handle*> <*uint64 offset*> <*uint32 len*> <*string data*>	When a file has been opened for writing, it can be written using the SSH_FXP_WRITE message. Only sequential offsets are supported and repositioning within an open file is not allowed. The server responds to a write request with a SSH_FXP_STATUS message.
SSH_FXP_LSTAT <*string path*>	Used to retrieve the attributes for a named file (identified by the 'path') while not following symbolic links. The server responds to this request with either SSH_FXP_ATTRS or SSH_FXP_STATUS.
SSH_FXP_FSTAT <*string path*>	SSH_FXP_FSTAT returns status information for an open file (identified by the file handle). The server responds to this request with SSH_FXP_ATTRS or SSH_FXP_STATUS.
SSH_FXP_SETSTAT <*string path*> <*ATTRS attrs*>	File attributes may be modified using the SSH_FXP_SETSTAT request where *path* specifies the file system object (for example, file or directory) whose attributes are to be modified, and *attrs* specifies the modifications to be made to its attributes. The server responds to this request with a SSH_FXP_STATUS message.
SSH_FXP_FSETSTAT <*string handle*> <*ATTRS attrs*>	File attributes on an open file may be modified using the SSH_FXP_FSETSTAT request where *handle* (***must*** be returned by SSH_FXP_OPEN) identifies the file whose attributes are to be modified, and 'attrs' specifies the modifications to be made to its attributes. The server responds to this request with a SSH_FXP_STATUS message.
SSH_FXP_OPENDIR <*string path*>	The SSH_FXP_OPENDIR opens a directory for reading where *path* is the path name of the directory to be listed (without any trailing slash). The server will respond to this request with either a SSH_FXP_HANDLE or a SSH_FXP_STATUS message.

Command	Description
SSH_FXP_READDIR <*string handle*>	Once the directory has been successfully opened, files (and directories) contained in it can be listed using SSH_FXP_READDIR requests. The server responds to this request with either a SSH_FXP_NAME or a SSH_FXP_STATUS message.
SSH_FXP_REMOVE <*string filename*>	Files can be removed using the SSH_FXP_REMOVE message where *filename* is the name of the file to be removed. The Server responds with a SSH_FXP_STATUS message.
SSH_FXP_MKDIR <*string path*> <*ATTRS attrs*>	New directories can be created using the SSH_FXP_MKDIR request where *path* and *attrs* specify the directory name and attributes. The server will respond to this request with a SSH_FXP_STATUS message.
SSH_FXP_RMDIR <*string path*>	Directories can be removed using the SSH_FXP_RMDIR request where *path* specifies the directory to be removed. The server responds to this request with a SSH_FXP_STATUS message.
SSH_FXP_REALPATH <*string path*>	The SSH_FXP_REALPATH request can be used to have the server canonicalize any given path name to an absolute path. The server will respond with a SSH_FXP_NAME packet containing only one name and a dummy attributes value. The name is the returned packet will be in canonical form. If an error occurs, the server may also respond with SSH_FXP_STATUS.
SSH_FXP_STAT <*string path*>	Used to retrieve the attributes for a named file identified by the *path*. SSH_FXP_STAT and SSH_FXP_LSTAT only differ in that SSH_FXP_STAT follows symbolic links on the server. The server responds to this request with either SSH_FXP_ATTRS or SSH_FXP_STATUS.
SSH_FXP_RENAME <*string oldpath*> <*string newpath*>	Files (and directories) can be renamed using the SSH_FXP_RENAME message where *oldpath* is the name of an existing file or directory, and *newpath* is the new name for the file or directory. The server will respond to this request with a SSH_FXP_STATUS message.
SSH_FXP_READLINK <*string path*>	The server does not support reading symbolic links. The server will respond with a SSH_FXP_STATUS error message.
SSH_FXP_SYMLINK <*string linkpath*> <*string targetpath*>	The server does not support creating symbolic links. The server will respond with a SSH_FXP_STATUS error message.
Responses from the SSH FTP Server to Client	

Command	Description
SSH_FXP_VERSION <*uint32 version*> <*optional extension data*>	Response to the SSH_FXP_INIT request. The server will respond supplying the lowest of its own (3) and the client's version number.
SSH_FXP_STATUS <*uint32 status*> <*string error*> <*string language*>	SSH_FXP_STATUS response is returned by the server in response to a client request where *status* indicates the result of the requested operation. The value SSH_FX_OK indicates success, and all other values indicate failure. SSH_FX_OK -Indicates successful completion of the operation. SSH_FX_EOF - indicates end-of-file condition; for SSH_FX_READ it means that no more data is available in the file, and for SSH_FX_READDIR it indicates that no more files are contained in the directory. SSH_FX_NO_SUCH_FILE - is returned when a reference is made to a file that should exist but does not. SSH_FX_PERMISSION_DENIED - is returned when the authenticated user does not have sufficient permissions to perform the operation. SSH_FX_FAILURE - is a generic catch-all error message; it should be returned if an error occurs for which there is no more specific error code defined. SSH_FX_BAD_MESSAGE - may be returned if a badly formatted packet or protocol incompatibility is detected. SSH_FX_NO_CONNECTION - is a pseudo-error that indicates the client has no connection to the server (it can only be generated locally by the client, and ***must not*** be returned by servers). SSH_FX_CONNECTION_LOST - is a pseudo-error that indicates the connection to the server has been lost (it can only be generated locally by the client, and ***must not*** be returned by servers). SSH_FX_OP_UNSUPPORTED - indicates that an attempt was made to perform an operation not supported for the server (it could be generated locally by the client if, for example, the version number exchange indicates that a required feature is not supported by the server, or it may be returned by the server if the server does not implement an operation).

Command	Description
SSH_FXP_HANDLE <*string handle*>	SSH_FXP_HANDLE is the server response to an SSH_FXP_OPEN or SSH_FXP_OPENDIR where *handle* is an arbitrary string that identifies an open file or directory on the server. The handle is opaque to the client; the client ***must not*** attempt to interpret or modify it in any way.
SSH_FXP_DATA <*string data*>	SSH_FXP_DATA is the server response to an SSH_FXP_READ where *data* is an arbitrary byte string containing the requested data. The data string may be at most the number of bytes requested in a SSH_FXP_READ request, but may also be shorter if end of file is reached or if the read is from something other than a regular file.
SSH_FXP_NAME <*uint32 count*> repeats count times: <*string filename*> <*string longname*> <*ATTRS attrs*>	*count* is the number of names returned in this response, and the remaining fields repeat *count* times (so that all three fields are first included for the first file, then for the second file, and so on). In the repeated SSH_FXP_ NAME is the server response to either a SSH_FXP_READDIR or SSH_FXP_REALPATH message where *filename* is a file name being returned (for SSH_FXP_READDIR, it will be a relative name within the directory, without any path components; for SSH_FXP_REALPATH it will be an absolute path name), *longname* is an expanded format for the file name, similar to what is returned by ls -l on Unix systems.
SSH_FXP_ATTRS <*ATTRS attrs*>	SSH_FXP_ATTRS is the server response for returning file attributes.

Cleo Harmony also supports HTTP PUT, GET, and DELETE methods for sending payload, receiving directory listings and payload, and deleting payload respectively, but the POST methods are recommended. Following are captures of example HTTP requests and responses demonstrating the above methods. While the examples below only show parameters on the POST line, Cleo Harmony does accept requests using the application/x-www-form-urlencoded and multipart/form-data Content-types.

Client initial connect request without authorization

```
POST /server?request=connect HTTP/1.1
Host: test.cleo.com:5080
Connection: Keep-Alive, TE
TE: trailers, deflate, gzip, compress
User-Agent: RPT-HTTPClient/0.3-3I (Windows XP)
Content-length: 0
```

Cleo Harmony response (unauthorized; both basic and digest Authentication is enabled)

```
HTTP/1.1 401 Unauthorized
Server: Cleo VLTrader/3.5 (Windows 2000)
Date: Tue, 22 May 2007 17:04:13 GMT
```

```
WWW-Authenticate: Basic realm="Cleo VLTrader"
WWW-Authenticate: Digest realm="Cleo VLTrader",domain="/
server",qop="auth",nonce="0qenmpn44",opaque="4b4c37373332"
Connection: close
Content-Type: text/html
Content-Length: 80
<html><head><title> Unauthorized</title></head><body> Unauthorized</body></
html>
```

Client connect request with digest authorization

```
POST /server?request=connect HTTP/1.1
Host: test.cleo.com:5080
Connection: TE
TE: trailers, deflate, gzip, compressUser-Agent: RPT-HTTPClient/0.3-3I
 (Windows XP)
Authorization: Digest realm="Cleo VLTrader",username="cleo",uri="/server
%3Frequest=connect",nonce="0qenmpn44",response="b4f7542bdedce937de6aa93078fcdf17",opaque
Content-length: 0
```

Cleo Harmony response (authentication successful)

```
HTTP/1.1 200 OK
Server: Cleo VLTrader/3.5 (Windows 2000)
Date: Tue, 22 May 2007 17:04:18 GMT
Content-Length: 0
Set-cookie: jSessionId=3513ld61kg8bt; path=/
Connection: keep-alive
```

Client send (upload) request

```
POST /server?request=send&directory=inbox%2F HTTP/1.1
Host: test.cleo.com:5080
Connection: TE
TE: trailers, deflate, gzip, compress
User-Agent: RPT-HTTPClient/0.3-3I (Windows XP)
Cookie: jSessionId=3513ld61kg8bt
Cookie2: $Version="1"
Authorization: Digest realm="Cleo VLTrader",username="cleo",uri=...
Content-type: application/octet-stream; name="test.edi"
Content-length: 1533
...payload...
```

Cleo Harmony response (send successful)

```
HTTP/1.1 200 OK
Server: Cleo VLTrader/3.5 (Windows 2000)
Date: Tue, 22 May 2007 17:19:59 GMT
Content-Type: text/html
Content-Length: 84
Connection: keep-alive
<html><head><title>OK</title></head><body>File successfully uploaded.</
body></html>
```

Client list request

```
POST /server?request=list&directory=outbox%2Fpayload%2F HTTP/1.1
Host: test.cleo.com:5080
Connection: TE
TE: trailers, deflate, gzip, compress
User-Agent: RPT-HTTPClient/0.3-3I (Windows XP)
Cookie: jSessionId=3513ld61kg8bt
Cookie2: $Version="1"
Authorization: Digest realm="Cleo VLTrader",username="cleo",uri=...
Content-length: 0
```

Cleo Harmony response (listing successful)

```
HTTP/1.1 200 OK
Server: Cleo VLTrader/3.5 (Windows 2000)
Date: Tue, 22 May 2007 17:04:18 GMT
Content-Type: text/html
Content-Length: 402
Connection: keep-alive
<head><title>'cleo' mailbox</title></head><body><pre><H2>Download</H2>Server
 directory: outbox/payload/<hr>
2007/05/03 08:43:17   1.497kB <A HREF="/server/outbox/payload/test.edi"
 >test.edi</A><br>
2007/05/22 08:32:46   4.491kB <A HREF="/server/outbox/payload/test2.edi"
 >test2.edi</A><br>
2007/05/22 08:33:28  28.444kB <A HREF="/server/outbox/payload/test3.edi"
 >test3.edi</A><br><hr></pre></body>
```

Client receive (download) request

```
POST /server?request=receive&directory=outbox%2Fpayload&filename=test.edi
 HTTP/1.1
Host: test.cleo.com:5080
Connection: TE
TE: trailers, deflate, gzip, compress
User-Agent: RPT-HTTPClient/0.3-3I (Windows XP)
Cookie: jSessionId=3513ld61kg8bt
Cookie2: $Version="1"
Authorization: Digest realm="Cleo VLTrader",username="cleo",uri=...
Content-length: 0
```

Cleo Harmony response (receive successful)

```
HTTP/1.1 200 OK
Server: Cleo VLTrader/3.5 (Windows 2000)
Date: Tue, 22 May 2007 17:25:57 GMT
Content-Description: test.edi
Content-Disposition: attachment; filename="test.edi"
Transfer-Encoding: chunked
Content-Type: application/edi-x12; name="test.edi"
Connection: keep-alive
...chunked payload...
```

Client delete request

```
POST /server?request=delete&directory=outbox%2Fpayload&filename=test.edi
 HTTP/1.1
Host: test.cleo.com:5080
Connection: TE
TE: trailers, deflate, gzip, compress
User-Agent: RPT-HTTPClient/0.3-3I (Windows XP)
Cookie: jSessionId=3513ld61kg8bt
Cookie2: $Version="1"
Authorization: Digest realm="Cleo VLTrader",username="cleo",uri=...
Content-length: 0
```

Cleo Harmony response (delete successful)

```
HTTP/1.1 200 OK
Server: Cleo VLTrader/3.5 (Windows 2000)
Date: Tue, 22 May 2007 17:25:58 GMT
Content-Length: 0
Connection: keep-alive
```

A web browser can also be used by a trading partner to manually trade with VerasLex's HTTP server. A trading partner would use the Cleo Harmony address and HTTP server resource path to start, for example, `https://test.cleo.com:6080/server`:

After logging in, a simple web page is displayed to allow uploading and downloading of files.

Note: For information about a more robust web portal interface, see Configuring VLPortal Web Browser service on page 783.

SSH FTP file attributes

The same encoding is used both when sending and returning file attributes from the server. When sending it to the server, the flags field specifies which attributes are included, and the server will use default values for the remaining attributes or will not modify the values of remaining attributes. When receiving attributes from the server, the flags specify which attributes are included in the returned data. The server normally returns all attributes known to it.

uint32	flags	
uint64	size	present only if flag SSH_FILEXFER_ATTR_SIZE
uint32	uid	present only if flag SSH_FILEXFER_ATTR_UIDGID
uint32	gid	present only if flag SSH_FILEXFER_ATTR_UIDGID
uint32	permissions	present only if flag SSH_FILEXFER_ATTR_PERMISSIONS
uint32	atime	present only if flag SSH_FILEXFER_ACMODTIME
uint32	mtime	present only if flag SSH_FILEXFER_ACMODTIME

uint32	extended_count	present only if flag SSH_FILEXFER_ATTR_EXTENDED
string	extended_type	
string	extended_data	...more extended data (extended_type - extended_data pairs), so that number of pairs equals extended_count

- **Flags** specify which of the fields are present. Those fields for which the corresponding flag is not set are not present and not included in the packet.
- The **size** field specifies the size of the file in bytes.
- The **uid** and **gid** fields contain numeric Unix-like user and group identifiers, respectively. The server only supports these fields on Unix systems.
- The **permissions** field contains a bit mask of file permissions as defined by posix. For non-Unix systems only the owner permissions are supported by the server.
- The **atime** and **mtime** contain the access and modification times of the files, respectively. They are represented as seconds from Jan 1, 1970 in UTC.
- The SSH_FILEXFER_ATTR_EXTENDED flag provides a general extension mechanism for vendor-specific extensions. This flag is not used by the server.

The flags bits are defined to have the following values:

SSH_FILEXFER_ATTR_SIZE	0x00000001
SSH_FILEXFER_ATTR_UIDGID	0x00000002
SSH_FILEXFER_ATTR_PERMISSIONS	0x00000004
SSH_FILEXFER_ATTR_ACMODTIME	0x00000008
SSH_FILEXFER_ATTR_EXTENDED	0x80000000

Local command reference

CHECK

See CHECK Command for information about this command.

comment

```
# text...
```

Lines in the action starting with a # character are considered comments and will be ignored when the action executes. Lines starting with # are generally used for documentation purposes.

LCOPY

Copy one or more files locally.

```
LCOPY -DEL -REC {-UNI|-APE} {-ZIP|-UNZ} "source" "destination"
```

-DEL

If the command is successful, delete the local file.

-REC

Recursively search all subdirectories.

You cannot use this option with the `-UNZ` option.

-UNI

Ensure the copied filename is unique.

-APE

Append copied file to existing destination file.

-ZIP

Zip all the files into one or more ZIP archive files, depending on the destination specified.

- Specify ZIP comment and compression level through **Zip Comment** and **Zip Compression Level** properties. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format. Visit http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html. The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Cryptographic Services on page 975.

-UNZ

Unzip the source file(s).

- All source files must be ZIP archive files.
- You cannot use this option with the `-REC` option.
- Use ZIP entry paths if **Unzip Use Path** is set. See Setting advanced host properties on page 89.
- The ZIP archive files created through the `LCOPY` command conform to the standard ZIP file format (reference http://docs.oracle.com/javase/6/docs/api/java/util/zip/package-summary.html). The ZIP file format should not be confused with other popular file compression/archive formats such as GZIP, TAR, RAR, etc. The `LCOPY` command works only with ZIP-formatted files. In addition to the Cleo Harmony application, there are many other software packages that can read/write ZIP-formatted files, for example, WinZip (Windows), File Roller (Linux), PKZIP and Info-ZIP (Windows/Linux/other Unix).
- In addition to standard ZIP-formatted archives, the Cleo Harmony application also supports password-based AES- encrypted ZIP files (128-bit, 192-bit, and 256-bit). See Encryption of Zip Files for more information on this capability.

`"source"`

Source path

- Path can be to a filename or to a directory
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.

- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*destination*"

Destination path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- You can use a single `*` within the destination path. In this context, it is not a wildcard. Rather, it is used to substitute a source file name or a source subdirectory name. When `*` is used in conjunction with both the `-REC` and `-ZIP` options, and `Zip Subdirectories Into Individual Zip Files` is enabled, then `*` is substituted with each first-level subdirectory name. When `*` is not used for bundling zipped subdirectories, then it is used as a shortcut for the `%sourcefilename%` or `%srcfilename%` macro. Only one `*` is allowed in the destination path. See Setting advanced host properties on page 89.
- When copying a file without the `-APE` option, or when copying a file with the `-APE` option where the destination file does not already exist, a temporary file name is used while the copy operation is taking place. This temporary file is placed in the destination directory. Its name begins with the product name and ends with `.tmp`. Once the copy completes successfully, the temporary file is renamed to the destination name.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LDELETE

Delete one or more files locally.

```
LDELETE "source"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.
- If you specify a relative path, the command uses the user's home directory.
- You can use `*` and `?`, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- Use of macro variables is supported. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

LREPLACE

Replace bytes in one or more files locally.

```
LREPLACE "source" Replace="input bytes" With="output bytes"
```

"*source*"

Source path.

- Path can be to a filename or to a directory.

- You can use * and ?, or a regular expression when you specify a filename. See Using wildcards and regular expressions on page 69 for additional information.
- If you specify a relative path, the command uses the default inbox.
- You can use macro variables. See Using macro variables on page 59 (Source File context) for a list of the applicable macros.
- If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"input bytes"

List of bytes to be replaced.

- Comma separated list of byte values (0-255).
- All bytes in comma-separated list must be found in the file in listed sequence in order to be replaced.

"output bytes"

List of bytes to be substituted for original `input bytes`.

- Comma separated list of byte values (0-255).
- If `With` parameter is omitted, then the `input bytes` are deleted from the file.

SCRIPT

See SCRIPT Command for information about this command.

SET

Change an action property value. The new value only affects the commands that **follow** the `SET`.

```
SET property=value
```

property = value

Action property and new value

- The property name must have no embedded spaces.
- The value specified remains in effect until it is set again or until the end of action.
- To reset property back to default value (host-level or system-level), specify

  ```
  SET property
  ```

  or

  ```
  SET property=
  ```

- To clear a string property, use the `CLEAR` command

SYSTEM

Execute a local system command.

```
SYSTEM "path"
```

"path"

Local command path with arguments.

- If you specify a relative path or no path, the command uses the Cleo Harmony home directory.
- See Using operating system commands in actions on page 93 for additional information

WAIT

Pause execution.

```
WAIT seconds
```

Seconds

Number of seconds to pause.

Clustering

You can cluster VersaLexes in your network using VersaLex Pools. The following section describes setting up and monitoring your VersaLex Pools.

Creating a VersaLex pool

1. Right-click **Systems** in the tree pane and select **New VersaLex Pool**.
   The **New VersaLex pool** dialog box appears.
2. Enter a unique VersaLex pool name and click **OK**.
3. The new pool is selected in the tree, and a shortened version of the **Add VersaLex** dialog box below is displayed. Only a VersaLex serial number and its connection information are needed. Once the VersaLex is added, any other VersaLexes synchronizing with the VersaLex are automatically added to the new pool. This feature can take a few seconds to load.
4. The pool can be subsequently renamed or hidden by right-clicking the pool in the tree pane and selecting **Rename** or **Hide**. Note that a hidden pool can be automatically revealed if a user group permission is added for that pool.

VersaLex pools

The **Systems** tree branch contains information regarding all the configured VersaLex pools. See Creating a VersaLex pool on page 880 for information about creating, renaming, or removing a VersaLex pool.

VersaLex Pool User Groups

The VersaLex Pool **User Groups** tab is view-only and shows which user groups have been granted access to this VersaLex pool. Use the **System Privileges** tab to grant access for each user group. See User Group: System Privileges Tab on page 930.

VersaLex Pool VersaLexes

The VersaLex Pool **VersaLexes** tab is view-only and shows the connection status of each VersaLex in this pool.

VersaLex Pool Transfers

The VersaLex Pool **Transfers** tab displays a graphic image of the total bytes transferred and includes additional statistics for each VersaLex in the pool for the time period specified by the Filter. A transfer report may be generated for each VersaLex by selecting **Details**.

Pre-requisite: Graphical viewing of transfers is only available for VersaLexes using Database Transfer Logging. See Transfers on page 895 and Logs on page 892. If any VersaLexes are using a database product that is different from the database used by the local VersaLex, those drivers must also be installed in the local lib/ext directory.

The option to view the **Details** for all the VersaLexes in the pool is also available when the following conditions are met:

1. All the VersaLexes in the pool have database transfer logging enabled. See Logs on page 892.
2. All the VersaLexes in the pool have Synchronized Hosts. See Synchronizing user configuration on multiple instances on page 888.
3. All the VersaLexes in the pool have either Synchronized System Options (see Synchronizing user configuration on multiple instances on page 888) or are all using the same database for Database Transfer Logging and have the same enablement and disablement options set for File Tracking. See Logs on page 892.

Saving or printing the graphs

To save or print a displayed graph or chart, right-click anywhere on the graph or chart to display a pop-up menu.

Choose **Save as** to display a file chooser allowing the graph or chart to be saved in PNG format.

Choose **Print** to print the graph or chart on the selected printer.

Configuring for a proxy

Two main types of firewalls exist: packet filtering firewalls and proxy servers. If a proxy server must be negotiated for a direct internet connection, the Cleo Harmony, Cleo VLTrader, and Cleo LexiCom applications support FTP, HTTP, and SMTP application-level proxies.

If you are unsure if you need to configure an HTTP proxy, check your browser to see if it is configured to use a proxy. See your browser's documentation for more information.

If you are still unsure of whether a proxy needs to be configured, contact your local network administrator.

An FTP proxy can only be used by FTP hosts and an SMTP proxy can only be used by SMTP hosts, while an HTTP proxy can be used by most of the host types. If all or most of your remote FTP hosts will be accessed thru the same proxy, consider specifying a Default FTP Forward Proxy. Likewise for FTP/s, HTTP, HTTP/s, and SMTP hosts. If necessary, the default forward proxy can be overridden within a specific host.

1. In the web UI, go to **Administration** > **Network** > **Proxies**. In the native UI, select **Configure** > **Proxies** in the menu bar.
2. Configure a new HTTP(/s) proxy that uses the Cleo VLProxy application.
   a) Click **New VLProxy**.
      A Cleo VLProxy configuration dialog box appears.
   b) Provide the information to configure the Cleo VLProxy instance and then click **OK**.
      See Cleo VLProxy configuration reference on page 882 for more information.
3. Configure an FTP proxy.
   a) Click **New FTP Proxy**.
      The **FTP Application-Level Proxy** dialog box appears.
   b) Provide the information to configure the new FTP proxy instance and then click **OK**.
      See FTP proxy configuration reference on page 884 for more information.
4. Configure an HTTP(/s) proxy that does not use Cleo VLProxy
   a) Click **New HTTP Proxy**.
      The **HTTP Application-Level Proxy** dialog box appears.
   b) Provide the information to configure the new HTTP proxy instance and then click **OK**.
      See HTTP proxy configuration reference on page 884 for more information.
5. Configure an SMTP proxy.
   a) Click **New SMTP Proxy**.
      The **SMTP Application-Level Proxy** dialog box appears.

b) Provide the information to configure the new SMTP proxy instance and then click **OK**.

See SMTP proxy configuration reference on page 885 for more information.

6. Configure a SOCKS proxy.

You can use a SOCKS proxy as a forward proxy for all remote hosts except fasp, MLLP, MQ Series, and SMTP.

a) Click **New SOCKS Proxy**.

The **SOCKS Application-Level Proxy** dialog box appears.

b) Provide the information to configure the new SOCKS proxy instance and then click **OK**.

See SOCKS proxy configuration reference on page 886 for more information.

7. Optional - Specify default forward proxies.

A default proxy is useful when all or most of your remote hosts for a given protocol use the same proxy. You can select a default proxy for FTP, FTP/s, HTTP, HTTP/s, and SMTP.

Select a forward proxy from the menu appropriate for the protocol. Each menu is populated proxies you have already configured.

8. Optional - Select an SMTP mail server from the **SMTP Mail Server**.

The **SMTP Mail Server** menu is populated with SMTP proxies you have already configured.

If the mail server requires SMTP authentication, select either plain or login authentication for the SMTP proxy to enable the username and password fields. See SMTP proxy configuration reference on page 885. If you are not sure of these values, contact your network administrator.

Note: The selected proxy authentication setting is ignored during authentication with the mail server. Instead, the authentication mechanism used is the first available authentication mechanism in the mail server.

If you select `None` in the **SMTP Mail Server** field, the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application will attempt to derive the SMTP mail server based on the destination email address.

Click **Test** to verify that the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application is able to successfully send email alerts whether the SMTP Mail Server has been defined or not.

9. Once configured, select the SMTP mail server from the list of available SMTP proxies:

An FTP proxy can only be used by FTP hosts and an SMTP proxy can only be used by SMTP hosts, while an HTTP proxy can be used by most of the host types. If all or most of your remote FTP hosts will be accessed thru the same proxy, then set the Default FTP Forward Proxy. Likewise for FTP/s, HTTP, HTTP/s, and SMTP hosts. If necessary, the default forward proxy can be overridden within a specific host.

Cleo VLProxy configuration reference

Provide values for these field to configure a Cleo VLProxy instance.

Proxy Server Address

Port #

Server address and port number to use for the Cleo VLProxy. These are required fields.

Forward proxy group

One or more instances of Cleo VLProxy grouped together for different purposes, for example, internal vs. external communications.

To create a new group, type the name of the group in the text box.

To select an existing group, pull down the menu and select a group.

Forward proxy backup only

Select this check box to specify this proxy as a backup for other proxies in the same group. The Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application will attempt to use an available backup Cleo VLProxy instance only if it is unable to use the primary forward Cleo VLProxy instance.

You cannot select the same proxy to be a backup and the default forward proxy at either the system or host level.

Forward proxy load balance

Select this check box to balance forward proxy requests across all the available instances of Cleo VLProxy based on the current number of connections to each. Any backup instances configured are included in the load balancing when the primary Cleo VLProxy in not available.

This field is only available when there are multiple instances of Cleo VLProxy configured in the same group.

Enable reverse proxying

Select this check box to use the reverse proxy feature of the Cleo VLProxy application for incoming HTTP messages.

If you select the **Enable reverse proxying** check box, the **Reverse forward connections** check box is enabled.

Reverse forward connections

Select this check box to indicate that all incoming reverse requests from the Cleo VLProxy application should use connections that originate from the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application forward to the Cleo VLProxy application. In other words, with this setting on, no inbound HTTP or HTTP/s port need be open through the firewall for incoming Cleo VLProxy requests. In fact, the HTTP and HTTP/s ports in the Local Listener can be disabled unless there is also local traffic coming directly to the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application.

The product establishes an available reverse connection pool with the Cleo VLProxy application, the size of which is based on the Local Listener **Incoming Connection Backlog Size** advanced property (see Specifying Local Listener advanced properties on page 759). When an incoming request uses one of the available connections, the pool is immediately replenished. If the request to the Cleo VLProxy application is over a secure port, the connection to the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application is converted to a secure port just prior to the incoming request starting. (**Note**: If **not** using **Reverse forward connections** and the request to the Cleo VLProxy application is over a secure port, the request from the Cleo VLProxy application into the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application uses a secure port if the Local Listener HTTP/s port is enabled.) While maintaining the available connection pool does add extra overhead, connections are established ahead of time; therefore, throughput with **Reverse forward connections** on or off should be comparable.

Selecting the **Reverse forward connections** check box also enables the **Proxy Connection(s)** portion of the dialog box.

Proxy Certificate(s)

SSL Certificate

Use Local Listener SSL Server Certificate(s)

Select this option to use the SSL certificate(s) configured in the Local Listener for both connections coming in through the Cleo VLProxy application and connections coming directly into the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application.

Select Proxy SSL Certificate

Password

Select this option to specify an SSL certificate and password to use for connections coming in through the Cleo VLProxy application. The SSL certificates configured in the Local Listener are used for connections coming directly into the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application. You can use different SSL certificates for each instance of the Cleo VLProxy application.

You can click **Browse** to navigate to and select a certificate.

SSH Certificate

Use Local Listener SSH Server Certificate

Select this option to use the SSH certificate configured in the Local Listener for both connections coming in through Cleo VLProxy and connections coming directly into Cleo Harmony, Cleo VLTrader, or Cleo LexiCom.

Select Proxy SSH Certificate

Password

Select this option to specify an SSH certificate and password to use for connections coming in through Cleo VLProxy. The SSL certificates configured in the Local Listener are used for connections coming directly into Cleo Harmony, Cleo VLTrader, or Cleo LexiCom.

You can click **Browse** to navigate to and select a certificate.

Use Proxy SSL Certificate

Select this check box to use the proxy SSL certificate specified in Cleo VLProxy for both SSL and SSH connectionsYou can use different SSH certificates for each Cleo VLProxy.

FTP proxy configuration reference

Provide values for these field to configure a FTP proxy.

Proxy Server Address

Port #

Server address and port number to use for the FTP proxy. These are required fields.

Commands

Template

The command necessary to negotiate through the proxy server to the remote FTP site. You can either enter them manually or select commands from the **Template** menu.

You can use the following keywords within the commands. When the commands are executed, the keywords are substituted for actual values.

- `%proxyuser` - proxy server logon username
- `%proxypass` - proxy server logon password
- `%host` - remote FTP site address
- `%user` - remote FTP logon username
- `%pass` - remote FTP logon password

Proxy Username

Password

If the proxy server requires authentication, provide a proxy username and password. If you are not sure of these values, contact your network administrator.

Click **OK** to save the FTP proxy.

HTTP proxy configuration reference

Provide values for these field to configure an HTTP proxy.

Proxy Server Address

Port #

Server address and port number to use for the HTTP proxy. These are required fields.

Proxy Authentication

Select the level of authentication to use for this proxy. If you specify a value other than **None**, specify values for **Username** and **Password**

Possible values: `None`, `Basic`, or `Digest`

Default value: `None`

Proxy Realm

Username

Password

If the proxy server requires authentication, provide a proxy username and password. If you are not sure of these values, contact your network administrator.

If the proxy server requires either basic or digest authentication, you must specify a proxy username and password. Optionally, specify a proxy realmIf you are not sure of these values, contact your network administrator.

SMTP proxy configuration reference

Provide values for these field to configure an SMTP proxy.

Proxy Server Address

Port #

Server address and port number to use for the SMTP proxy. These are required fields.

Proxy Authentication

Select the level of authentication to use for this proxy. If you specify a value other than **None**, specify values for **Username** and **Password**

Possible values: `None`, `Plain`, or `Login`

Default value: `None`

Proxy Realm

Username

Password

If the proxy server requires either plain or login authentication, you must specify a proxy username and password. Optionally, specify a proxy realm. If you are not sure of these values, contact your network administrator.

Use Start TLS

Select the check box to specify that the SMTP Proxy will send a `STARTTLS` command when the session is started.

Default value: Selected (True)

SSL Maximum Protocol Version

SSL Minimum Protocol Version

Specify minimum and maximum versions of SSL protocol (where the maximum value is the newest and minimum is the oldest) to use for the SMTP proxy to create a range of valid versions. The system will use any version inside the range you specify. You can specify a single version by entering the same value for both maximum and minimum versions.

SOCKS proxy configuration reference

Provide values for these field to configure a SOCKS proxy.

Proxy Server Address

Port #

Server address and port number to use for the SOCKS proxy. These are required fields.

Proxy Protocol Version

Select the protocol version required by the SOCKS server. Selecting `v5` enables the **Proxy Authentication** menu.

Possible values: `v4` or `v5`

Default value: `v4`

Proxy Authentication

If the server requires Username/Password authentication, select `Username/Password` to enable the **Username** and **Password** fields.

This menu is enabled when you select `v5` as the proxy protocol version.

Possible values: `None` or `Username/Password`

Default value: `None`

Configuring IP filtering

The Cleo Harmony application provides IP filtering that allows you to specify both a whitelist and a blacklist to control the IP addresses from which Cleo Harmony application users can log in.

Configuring a whitelist

A whitelist allows you to specify IP addresses from which users are allowed to log in. You specify whitelist IP addresses per local user mailbox by editing individual local user mailboxes. See Configuring IP filtering for an FTP mailbox on page 828, Configuring IP Filter for Local HTTP Mailbox on page 839, Configuring IP filter for local SSH FTP mailbox on page 857, and Users Mailbox: IP Filter on page 532.

Configuring a blacklist

A blacklist allows you to specify IP addresses that restrict access to the Cleo Harmony, Cleo VLTrader, and Cleo LexiCom applications through FTP/FTPs, SSH FTP/SSH FTPs, HTTP/HTTPs, along with general web UI access through the Cleo Harmony or Cleo VLTrader and Cleo VLNavigator applications.

It is important to understand that blacklist entries will take higher priority than whitelist entries. For example, if an IP is on both lists, access is denied from that IP. Set up blacklisting by specifying parameters for automated blacklist additions or by manually adding IP addresses to the blacklist. Configure your blacklist on the **Blacklist** tab on the **IP Filter** dialog box.

Note: If your architecture includes a load balancer placed in front of the Cleo Harmony, Cleo VLTrader, Cleo LexiCom or Cleo VLProxy application, and the IP address sent to the Cleo Harmony, Cleo VLTrader, Cleo LexiCom or Cleo VLProxy application is the address of the load balancer rather than the originating source, blacklisting could possibly result in blocking all traffic through the load balancer. If you are using a load balancer, consider using the load balancer's firewall capabilities to manage your blacklisting needs.

Note: If you are using Cleo VLProxy and want to configure Automatic IP Blacklisting, the Local Listener's HTTP node's Resource Path must be enabled. See Configuring Local Listener HTTP Service on page 774.

1. In the web UI, go to **Administration** > **Network** > **IP Filters**. In the native UI, go to **Tools** > **IP Filters**.

   The **IP Filters** page appears.
2. Click the **Blacklist** tab.

3. Do one or both of the following:
   - Configure Automatic IP Blacklisting

     If **Lock out IP** is enabled, after the specified number of failed login attempts within the specified number of seconds, the IP is blacklisted for the specified number of minutes. If the minutes are not specified (the field is left blank), the IP is blacklisted until manually removed by the user.

     Select **Blacklist REST API Requests** to trigger automatic IP blacklisting for failed REST API requests.
   - Manually add IP addresses to the blacklist
     a. Click **Add Blocked IP** to display the **New Blacklisted IP** dialog box.
     b. In the **IP** field, enter an IP address you want to block.
     c. In the **Until** field, choose **Forever** to deny access to the IP address permanently or **Never** to never let the IP address be blacklisted.

        The other fields in the dialog box are read-only.
     d. Click **OK**.
4. In the native UI, click **Close** to dismiss the **IP Filters** dialog box.

Reviewing the IP filter list

Extract the IP filter list for active hosts.

1. In the web UI, go to **Administration** > **Network** > **IP Filters**. In the native UI, select **Tools** > **IP Filters** in the menu bar.

   Each FTP, SSH FTP, and HTTP local user host is interrogated for its IP filter settings.

   Each mailbox within each local user host is listed along with its protocol, whether the mailbox is an LDAP mailbox, and its IP filter setting.
2. Optionally, click **Find** to search for a specific folder, host, mailbox, or IP address.
3. Optionally, click **Export** to export the whitelist as a `.csv`.

Reviewing TCP/IP port usage

Use the **TCP/IP Usage** report to review usage.

1. In the web UI, select **Administration** > **Network** > **Ports**. In the native UI, select **Tools** > **TCP/IP Port Usage** from the menu bar.

   The **TCP/IP Port Usage** page appears.

   Each active host whose connection type is Direct Internet Access or VPN is interrogated for name and IP address and inbound and outbound port usage.

   The information given is intended for the firewall administrator. Each host's TCP/IP protocol, address, and inbound and outbound port usage are listed. If an application proxy has been configured, it is also listed. The inbound ports can be adjusted within Cleo LexiCom, but modifications can affect server-side or AS2 trading partner configuration. The outbound ports are dictated by the server.

   For FTP, the command port and the data ports are distinguished in the report.

   - **FTP/s (Explicit)** vs. **FTP/s (Implicit)**
     - For **FTP/s (Explicit)**, the command port is initially clear text commands. The SSL handshake does not start until the client issues an AUTH SSL command and the server responds affirmatively, after which commands are encrypted.

    - For **FTP/s (Implicit)**, the SSL handshake starts immediately once the command port is opened, after which all commands are encrypted.
  - **Active (a.k.a. Port) Mode** vs. **Passive Mode**
    - In **passive** mode, the FTP server (host) picks a new data port dynamically for each transfer. If this is a well-known site, the known outbound data port range is listed; otherwise, `?-?` is shown and you will need to contact the server administrator for the range.
    - In **active** mode, the FTP client (LexiCom) picks a new inbound data port dynamically from the range listed for each transfer.

  For HTTP, commands and data are sent across the same port.
2. Optionally, click **Save As** to save the report as an HTML file.

For more information about specific hosts and specific firewalls, visit http://www.cleo.com/LexiCom/firewall/index.asp.

Synchronizing user configuration on multiple instances

You can synchronize user configuration on two or more instances of Cleo Harmony or Cleo VLTrader. Synchronization can involve a production system and one or more redundant backup systems, or it can involve distributed, non-redundant production systems. To allow for these different system scenarios, you can set up synchronization to include the entire set of user configuration data or a subset. Items available for synchronization include:

- Trading partner/CA certificates
- User certificates/private keys
- System options
- Proxy settings
- AS/400 configuration
- Windows/Unix folders configuration
- Schedule
- Routes
- Local Listener
- Hosts
- Trading Partners

Note: In the case of backup systems, synchronization is geared towards dedicated, hot backup systems. This feature is not conducive to a backup system that is also used as a standalone test system.

CAUTION: To avoid confusion, activate synchronization using the system containing the starting point of the files to be synchronized. This protects you from accidentally clearing configuration data. For example, when adding a synchronized backup to a production system, use the production system to activate synchronization.

For further protection, before activating synchronization use **File** > **Export** to backup user files. See Exporting user files on page 726.

1. In the web UI, go to **Administration** > **Network** > **Synchronization**. In the native UI, select **Configure** > **Synchronization** in the menu bar.

   The synchronization table appears. It always includes the active system (Cleo Harmony or Cleo VLTrader) indicated by a dot. This entry cannot be removed; right-click the entry and select **Edit** to modify the **Backup Only** setting for this system.
2. Add a system to be synchronized.

a) Click **Add VLTrader/Harmony**.

The Cleo Harmony Synchronization or Cleo VLTrader Synchronization dialog box appears.

b) Enter the serial number of the Cleo Harmony or Cleo VLTrader system to be synchronized and indicate whether it is a backup system.

A backup system should be configured as such. In fact, your license for the backup system might indicate `Backup Only`, which allows use as a backup system only. Backup systems are fully operational except for the following:

Note: While the production system is online, the scheduler can not be started on the backup system. If the schedule is marked to `Automatically run at startup`, the schedule will start up automatically on the backup system if the production system goes offline and will stop automatically when the production system comes back online. The same rules apply for the router and outbound database payload features.

c) Enter the system's computer name or address and the HTTP or HTTP/s port the Local Listener for that system is listening on (default is `HTTP 5080`). Cleo recommends specifying a Synchronization Port # on the HTTP tab for the Local Listener (see Configuring a Local Listener for HTTP on page 750) and configuring your firewall such that the port in question is accessible only to the instances of VersaLex you want to synchronize. (Note that firewall configuration must be done outside of VersaLex.) The Local Listener will automatically switch to using the Synchronization Port if one is configured. Otherwise, it will automatically switch to the HTTP/s port, if one is configured.

d) Optional – Add a **Group** to specify failover rules that designate how production/backup systems will respond when production systems go offline. This might be the case when, for example, you have separate configurations of production and backup servers in multiple data centers and want them to be organized in logical groups; or you have backup systems that are designated for disaster recovery and only want the backup systems to become active when all the production systems are offline. When groups are specified, the Cleo Harmony and Cleo VLTrader systems support either multiple production/backup groups or one all-production group and one all-backup group. See item 9, below, for a detailed description of the production/backup group and all-production/all-backup group failover rules.

e) Optional - Add an alias. If you provide an alias, it is included in the title bar of the product's main window. If the Cleo VLNavigator application is installed, you can set the alias to be included in the Cleo VLNavigator application's title bar by selecting the **VLNavigator Alias** check box.

f) Optional - enter some information in the **Location Note** field. For example, if you are using SNMP, enter a location note that can be used to describe the location.

g) Select items to synchronize. You can select items individually, click **All** to select them all, or click **None** to clear all selections.

Any combination of synchronized items is allowed, except for the following:

- routes cannot be shared across production systems
- trading partner/CA certificates and user certificates/private keys must be shared if hosts are being shared
- hosts must be shared if the schedule is being shared
- hosts must be shared across a production and backup system
- trading partners can only be synchronized if hosts are synchronized

Note: You can ensure that schedulers across systems in the cluster are synchronized by selecting the **Run Scheduler Automatically At Startup** option on the **Administration** > **System** > **Other** page. See Other system options on page 729.

3. Click **OK**.

The **Synchronization Username/Password entry** dialog box appears. Enter the user name and password for the system you are connecting to. The user you enter must have editable privileges to the system tree. Click **OK** to continue.

Another dialog box allows you to confirm that the existing user configuration on this system should be the starting point for both systems.

4. Click **Yes** to continue with synchronization.

   At this point, the systems connect and the synchronization parameters on the other side are automatically configured to match. If any network or port address translations (NAT or PAT) are being used between the two systems, the user might need to adjust the address and port of the automatically configured side for connecting back.

   When hosts are being synchronized, message IDs and receipts are also automatically synchronized for applicable protocols, including AS2/AS3, ebMS, OFTP and SMTP.

   - Sharing received message IDs ensures that duplicate messages can be detected from any of the synchronized instances of the product, not just the instance receiving the original message.
   - When a duplicate message ID is detected, sharing sent receipts allows the original receipt to be returned when dictated by the protocol.
   - Sharing received receipts ensures that the system that originally requested the receipt receives it. This allows message completion to be properly recorded and avoids the potential for false receipt timeouts and unnecessary resends of payload.
   - Sharing all sent and received receipts allows the full complement of receipts to be available and viewable on any of the synchronized systems.
   - Pending payload and receipt messages are NOT synchronized across systems, which means:
     - Resending payload messages when the asynchronous receipt timeout expires is not synchronized.
     - Resending asynchronous receipts that fail to be sent is not synchronized.

   Unlike configured synchronization items where the user must indicate which system contains the starting point, any recent messages IDs and receipts on either system are immediately shared when the synchronized systems are initialized. For systems already in production for some time, initial synchronization of message IDs and receipts may take an extended period (and this period may be CPU intensive on lower-end systems).

   The status displayed in the synchronization dialog box indicates what is currently being synchronized from this system to the other system. The status will also reflect when there is a connection error or a synchronization error. The status will eventually hold steady at `Waiting for sync requests` once initial synchronization has successfully completed.

5. Once initial synchronization is complete, you can modify synchronized items on any system and the update will be applied to the other instances of the product, regardless of where it was originally configured and regardless of whether it is a production or backup system. However, a warning dialog box is displayed whenever an update of a synchronized item is attempted from a backup system. Click **Yes** to continue.

   Modified items are immediately synchronized. If a synchronized system is currently down, then a modified item is queued for synchronization for when the system comes back online.

6. If errors occur, resolve them. Collisions can occur if users on two synchronized systems both update an item at the same time. If the same item is updated on both systems while the other system is offline, collisions will also occur when both systems are brought back online. An error message is generated and provides instructions to resolve the issue. Follow the instructions in the error message. A dialog box is displayed to allow you to continue.

7. In the dialog box, click **Just Resolve Errors** to display a dialog box where you can select the errors you want to resolve.

8. Select **Sync Now** check box for the errors you want to resolve and then click **OK**. The version of the file from this instance of the product is then synchronized with the other instance.

   Synchronization can also fail if the file being synchronized is somehow marked as read-only or if a host is being synchronized and the host is currently running. These failures must also be manually resolved.

9. If a synchronized system has been offline for an extended period of time, an error message might be displayed.

   If the still-online system is a backup system and the schedule is configured to run automatically, a warning might also be logged.

   You can configure the amount of time before failover in the native UI at **Configure** > **Options** > **Other** > **Synchronized Backup Failover** or in the web UI at **Administration** > **System** > **Other** > **Synchronized Backup Failover**. Failover defaults to 5 minutes. The connection failure exception is logged halfway through the failover wait period, so the connection failure is logged by default after 2.5 minutes, and failover occurs after 2.5 more minutes.

   - If there are multiple backup systems being synchronized with the production system, the schedule is automatically started on whichever online backup system has the lowest serial number. (If also configured, the router and outbound db payload features are also started.)
   - If there are multiple production systems synchronizing the schedule, the online production system with the lowest serial number is the "master" scheduler, and load balances scheduled actions across the other online productions systems. If a production system should go offline, an online backup system is added to the load balancing pool.
   - If all the production systems should go offline, the online backup system with the lowest serial number becomes the "master" scheduler. (If also configured, the outbound db payload feature also loads balances in a similar fashion.)
   - When failover groups are defined:
     - If the production/backup systems are grouped together, activation of backup systems are based on just the status of the active nodes *within the group* instead of the status of *all* active nodes. You can designate as many production/backup groups as needed.
     - If all production systems are grouped together and all backup systems are grouped together, the backup system(s) only become activated after all production systems are down/offline. The number of backup systems that become active is the same as the number ‘n’ of previously active production systems, that is, if you have synchronized more backup systems than production systems, only ‘n’ number of backup systems will become active. Only one all-production group and one all-backup group can be configured.

10. Should this become necessary, configuration items to be synchronized can be added or removed at any time. If making additions, it is recommended that this be done on the system containing the desired starting point of the configuration files being added. Go back to **Configure** > **Synchronization** in the native UI or **Administration** > **Network** > **Synchronization** in the web UI, right-click the serial number of the other instance, and select **Edit**. Then make the necessary modifications and click **OK**.

    If synchronization items were added, again you will be asked if the existing user configuration for the item added on this instance should be the starting point for both systems.

11. Synchronization with another instance can be temporarily disabled at any time by editing the configuration. When synchronization is re-enabled, if you chose to accumulate updates, any items modified while synchronization was disabled are immediately synchronized.

    Synchronization is automatically disabled should the product software versions become mismatched and automatically re-enabled once the versions are again aligned.

12. If synchronization between two systems becomes unnecessary, you can remove it by going to the **Synchronization** panel, right-clicking the serial number of the other instance, and selecting **Remove**

    Note: If more than two instances are being synced and one needs to be removed from synchronization, it is best to temporarily disable the sync relationship on each instance before removing (otherwise, depending on timing, the relationship can get automatically added back in shortly after being removed).

    CAUTION: For high throughput systems using a receipt protocol (AS2/3, ebMS, OFTP, SMTP), if one of the synchronized systems will be off-line for an extended period of time (for example, hardware being

repaired/replaced), it might be best to disable the synchronization configuration from the system still online until the offline system is again available. When disabling, be sure to choose to not accumulate updates and instead re-initialize later. Doing this will save the system still online from having to maintain a large synchronization queue and from having to delay archiving a large number of receipts.

Monitoring

The **Monitoring** settings allow you to choose the level of detail to monitor the logs, transfers, and data sent between the server and the trading partners of your Cleo Harmony, Cleo LexiCom, or Cleo VLTrader system. The **Monitoring** menus have standard options available as well as the ability to customize the level of detail shown. Access these by clicking **Administration** > **Monitoring** in the web UI. The following sections describe the different options available for monitoring data transfers on your system.

Logs

In the web UI, go to **Administration** > **Monitoring** > **Logs** in the menu bar. In the native UI, go to **Options** > **Messages**.

System Message Level

Indicates what level of detail messages should be shown in the messages pane.

Standard values pertain only to detail messages; customizing allows finer control of the level:

Possible values:

- `Essential - 0`
- `Low - 1`
- `Medium - 2`
- `High - 3`
- `Custom`

Default value: `High - 3`

System Log File

Indicates whether a system log file should be:

- continually appended to, or
- overwritten each time the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom software is started, or
- not created at all.

Possible values:

- `Append`
- `Overwrite`
- `None`

Default value: `Append`

Replicate Log Events in Cluster

Indicates whether any log event for any node in the cluster should be replicated across the cluster. The Cleo Harmony and Cleo VLTrader applications use a self-contained, distributed NoSQL database for this purpose. This option must be turned on for transfers and events information to be available through the REST API and, hence, the Cleo Portal and several of the newer UI reports (for example, Transfers and Logs).

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: `On` or `Off`

Default value: `On`

Note:

It is **strongly recommended that this switch remain `On`**, as reliance on the distributed NoSQL database will increase as new Cleo Harmony and Cleo VLTrader software features are introduced.

When transitioning this switch from `Off` to `On`, all users **should** log out and back in to view the new UI displays. Along with this, since the newer UI reports come strictly from data within the NoSQL database, it will take a while for historical data to collect.

When switching from `On` to `off`, all users **must** log out and back in to see up-to-date data for the event log and transfer report.

Compute CRC on transfers

Indicates whether a CRC-32 value should be computed on file transfers. If computed, a CRC value is recorded in the <Result> element of the system log file; and further, if database transfer logging is enabled, the CRC will be stored in the database as well.

Note: If special EOL processing is associated with the transfer (e.g., 'Fixed Record Outgoing Insert EOL' is on), CRC computations will take place after EOL processing on outbound payloads and before EOL processing on inbound payloads.

Note: This is a Cleo Harmony and Cleo VLTrader option.

Possible values: selected or unselected

Default value: unselected.

Log errors and warnings in System Event/Syslog File

This is a Cleo Harmony and Cleo VLTrader option.

When the 'Log errors' selection is enabled, indicates that all errors and exceptions will be logged in either the Windows Event Log or the Unix Syslog. In Unix, messages larger than the size of the Syslog record entry will be truncated.

Additionally, logging of warnings may be selected but requires that error logging has also been enabled.

When enabled, System Event logging will be done in addition to "Email On Fail". Suppression of repetitive messages used for emailing does not apply to System Event logging.

If you select either of these options and you are running Harmony or VLTrader as a daemon on systemd, you must make sure your Unit file contains the following:

```
[Service]
Type=simple
ExecStart=/root/Harmony/Harmonyc -s service
ExecStop=/root/Harmony/Harmonyc -s service,stop
```

In addition, if `stdout` and `stderr` are not being sent to `journald`, include the following:

```
StandardOutput=journal
StandardError=journal
```

For more information, see Starting as a daemon on systemd on page 52

Note: On newer versions of Linux and Unix Solaris 2.6+, it's possible that the remote Syslog capability was disabled and may require additional configuration. Refer to Knowledgebase # 2416 for further information.

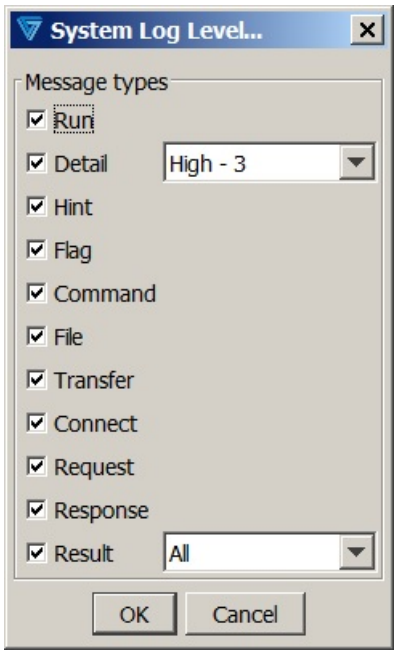
Possible values: selected or unselected

Default value: unselected

System Log Level

Indicates what level of messages should be logged to the system log file.

Standard values pertain only to detail messages; customizing allows finer control of the level:



Possible values:

- `Essential - 0`
- `Low - 1`
- `Medium - 2`
- `High - 3`
- `Custom`

Default value: `High - 3`

Automatically archive

Indicates whether the system log file should be automatically archived when it reaches the maximum size.

Possible values: selected or unselected

Default value: selected.

Archive daily or Archive weekly

In addition to archiving when it reaches the maximum size, indicates whether the system log file should be archived at the end of every day or every week (Sun-Sat).

Possible values: selected or unselected

Default value: unselected

Transfers

Note: This section applies to the Cleo VLTrader and Cleo Harmony applications only.

In the web UI, go to **Administration** > **Monitoring** > **Transfers**. In the native UI, click **Transfers** from the menu bar.

This panel is used to determine if and how transfers are recorded. The following describes the different parameters available. The **Database** and **XML File** sections are dimmed based on the Transfer Logging option you select.

Transfer Logging

Determines if Transfer Logging is enabled and whether a database or xml files are to be used.

Possible values: `Off`, `Database`, or `XML File`

Default value: `Off`

Transfer Database

The following fields are enabled when you select `Database` from the **Transfer Logging** menu.

Database

A menu from which you select the database to use for transfer logging.

Available databases are configured in the Databases tab. See Databases on page 722

Test Database Connection

Click this button to attempt to create a database connection using the selected database. The system will indicate success or failure.

Export Database Definition

Click this button to export SQL statements used to create the database tables for the specified Driver String and selected EDI and payload options to be exported to an SQL script file.

The file will contain all or most of the following DDL statements:

```
CREATE TABLE
ALTER TABLE
CREATE
CREATE TRIGGER
```

You can modify these statements (for example, use a specific table space or change/remove a trigger or foreign key), but the table names and columns must be left exactly as is. You can use the modified script to create a modified VersaLex database. If VersaLex itself has already created the standard database, you might need to add `DROP` statements to the beginning of the script.

Automatically purge logged transfers older than *n* day(s)

When enabled, VersaLex will purge the database every 8 hours of logged transfers older than the configured number of days.

Possible values: `Selected` or `Unselected`, plus a value for number of days greater than or equal to `1`

Default value: `Unselected`

Update Frequency

While the transfer is in-process, the frequency (in seconds) with which the database is updated with the current transfer bytes and seconds. Set this value to `0` to disable in-process updates.

Possible values: `0` or a value greater than or equal to `1`.

Default value: `1`

Track file content

Enables tracking feature where identifier and transactional data within EDI, XML and text files can be tracked. All tracked data is stored in additional database tables. See Transfer database fields on page 996.

Once enabled, click **Configure** to provide more information about tracking options. See File tracking on page 896.

Possible values: `Selected` or `Unselected`

Default value: `Unselected`

Use the database for incoming/outgoing payload

Extended transfer feature that uses the database as the payload repository rather than the file system.

Once enabled, click **Configure**. See Database payload on page 723

Possible values: `Selected` or `Unselected`

Default value: `Unselected`

Temporarily disable transfer database

While disabled, transfers are saved to disk and logged once the database is again available. This includes both base transfer and additional EDI log entries. You can set a limit to the number of transfer log entries to save while the database is unavailable. See *Maximum Saved Database Transfer Log Entries* in Other system options on page 729.

Possible values: `Selected` or `Unselected`

Default value: `Unselected`

Additional Serial Numbers

When using database transfer logging, transfers from other VersaLex installs can be added to transfer reports (see Viewing transfer status on page 637).

Possible values: Valid product serial numbers. You can enter multiple serial numbers separated by commas.

Transfer XML File

The following field is enabled when you select `XML File` from the **Transfer Logging** menu.

The files created by this option can be found in `..Harmony/logs/xfer%date%.xml`.

Number of days before archiving the XML log

Each day's transfers are logged to a separate file. This option defines the number of days before the transfer history is archived.

Possible values: Integers greater than `0` to represent whole day increments.

Default value: `3`

File tracking

When you select the **Track file content** check box and click **Configure file tracking** on the **Options** > **Transfers** tab, the **File Tracking Options** dialog box is displayed.

Use this dialog box as a starting point to configure all file tracking options. It consists of three sections: **Tracking Configuration**, **File Tracking List**, and **Properties**.

Tracking Configuration

Enable one or more of the three types of tracking available: EDI, XML, and text.

Track EDI content

When you select the **Track EDI content** check box on the **File Track Options** dialog box, EDI tracking is enabled and baseline EDI identifier information, such as interchanges and functional groups, are tracked. See EDI tracking fields on page 1000 for detailed information on the data collected in the database.

You can configure EDI tracking options without enabling tracking. Tracking will not actually occur unless the **Track EDI content** check box is selected.

To configure an EDI tracking entry, click **New EDI**. See New EDI on page .

To update an existing item, double-click it or right-click it and select **Edit**. See EDI tracking fields on page 1000.

Enable EDI functional acknowledgment tracking

Select this check box to track EDI-X12 and UN/EDIFACT pending functional acknowledgments. Once the functional acknowledgment is sent or received, the acknowledgment code is logged with the corresponding original transaction set.

Still track EDI inbound if error responding to the sender

Select this check box to continue logging incoming EDI information if the payload was successfully received but there was an error sending the asynchronous AS2 MDN or ebMS acknowledgment.

EDI Tracking Exclusions

Specify tracking exclusions directly in the field or select **Edit Exclusions** to select exclusions from a list. See *EDI Tracking Exclusions* in EDI tracking on page 898.

Track XML content

Select the check box to enable XML content tracking.

Unlike EDI tracking, where baseline content is tracked when you select the **Track EDI content** check box, for XML tracking you must add entries to the File Tracking List for any XML tracking to take place. See XML tracking fields on page 1003 for detailed information about the data collected in the database. For XML tracking, all data tracked - whether it be identifier data or transactional data - is stored solely in the `VLXMLExtractedData` table.

To configure an XML tracking entry, click **New XML**. See New XML on page .

To update an existing item, double-click it or right-click it and select **Edit**. See XML tracking fields on page 1003.

XML Tracking Exclusions

Specify tracking exclusions directly in the field or select **Edit Exclusions** to select exclusions from a list. See *XML Tracking Exclusions* in XML tracking on page 900.

Track text content

Select the check box to enable text tracking.

Unlike EDI tracking, where baseline content is tracked when you enable it, for text, you must add entries to the **File Tracking List** for *any* text tracking to take place. See Text Tracking Fields for detailed information on the data collected in the database. For text tracking, all data tracked -- whether it be identifier data or transactional data -- is stored solely in the `VLTextExtractedData` table.

Click **New Text** in the **File Tracking List** to configure new text tracking items. SeeNew Text on page .

To update an existing item, double-click it or right-click it and select **Edit**. See Text tracking fields on page 1004.

File Tracking List

A summary of all the reference information to be tracked. You can add new EDI, XML, and text items to track.

New EDI

Click **New EDI** to add a new EDI item to the **File Tracking List**. See *EDI Reference* in EDI tracking on page 898.

New XML

Click **New XML** to add a new XML item to the **File Tracking List**. See *XML Reference* in XML tracking on page 900.

New Text

Click **New Text** to add a new Text item to the **File Tracking List**. See Text tracking on page 902.

Properties

Reference 1 Display Name

Reference 2 Display Name

Optional - Specify the names to use in the transfer reports for the two storage areas designated for reference information. These names can then subsequently be seen in transfer report detail views, as seen through the **View Information** right-click option.

EDI tracking

EDI Tracking Exclusions

When you click **Edit Exclusions** for the **EDI Tracking Exclusion** field on the **File Tracking Options** dialog box, the **Edit EDI Exclusions** dialog box appears.

Choose from the following:

- **Exclude all non-production trading partner connections**
- **Exclude specific trading partner connections**: Select items from the list that correspond to the trading partners you want to exclude from tracking.
- **Exclude specific folders**: Select items from the list that correspond to the folders you want to exclude from tracking.
- **Exclude specific hosts\mailboxes\actions**: Select items from the list that correspond to the hosts, mailboxes, or actions you want to exclude from tracking.

All exclusions are considered independently. For example, assume you select **Exclude all non-production trading partner connections** and `newTradingPartner1` in the Trading Partners section and `AS2` in the hosts\mailboxes \actions section. With these selections, a file processed through the system will be excluded from tracking if its action is associated with the **AS2** host, or its action is associated with `newTradingPartner1`, or its action is associated with a non-production trading partner connection.

EDI Reference

The **New EDI Reference** dialog box is displayed when you click **New EDI** in the **File Tracking List** in the **File Tracking Options** dialog box. The **Edit EDI Reference** dialog box is displayed when you double-click an EDI item or right-click an EDI item and then select **Edit** in the **File Tracking List**.

In **New EDI Reference** or **Edit EDI Reference** dialog box, specify values for the following fields:

EDI Configuration

EDI Type

Transaction Type

Choose an type of EDI transaction and then a transaction type for which you want to specify a reference.

EDI types include ASC X12, EDIFACT or TRADACOMS.

The transaction types available depend on the EDI type you select.

Extract data on inbound transfers

Extract data on outbound transfers

Select these check boxes to track this reference on inbound and outbound transfers, respectively. You can select either or both.

Extract data only if segment

Select this check box to track this reference when the **segment**, **element**, and **subelement** meet the conditions you specify. If you select this check box, you must specify values for **segment** and **element**. The **subelement** is optional.

Identifier Data

The system automatically tracks identifier data, regardless of any other settings on the **Edit EDI Reference** dialog box. There are no settings or fields for you to configure.

Transactional Data

Specify one or more records in the **Transactional Data** table.

- **Insert a new row** - Click **New** to insert a new row in the table and display the **Extract Transactional Reference** dialog box with none of the fields populated.
- **Edit a row** - Right-click a row and select **Edit** or double-click a row to display the **Extract Transactional Reference** dialog box populated with data from the selected row.

See Extract Transactional Reference on page 899.

Extract Transactional Reference

The **Extract Transactional Reference** dialog box is displayed when you select an item to edit or you click **New** in the **Transactional Data** table. Edit or populate the following fields:

Extract segment

element

[subelement]

Identify a segment, element, and subelement you want to track.

Segment and **element** are required. **Subelement** is optional.

only if

element

[subelement]

Select this check box to track this reference when the **element** and **subelement** meet the conditions you specify. If you select this check box, you must specify a value for the **element** field. The **subelement** is optional.

Storage Location for Extracted Data

Specify where to store the collected reference data. Each reference collected will be separated by commas, and optionally preceded by the label, when it is displayed through the **View Information** right-click option under transfer reporting.

Reference 1

Reference2

Select the reference in which to store the data.

Reference Label

Optional: a label for the reference.

XML tracking

XML Tracking Exclusions

When you click **Edit Exclusions** for the **XML Tracking Exclusion** field on the **File Tracking Options** dialog box, the **Edit XML Exclusions** dialog box appears.

You can choose from the following:

- **Exclude all non-production trading partner connections**
- **Exclude specific trading partner connections**: Select items from the list that correspond to the trading partners you want to exclude from tracking.
- **Exclude specific folders**: Select items from the list that correspond to the folders you want to exclude from tracking.
- **Exclude specific hosts\mailboxes\actions**: Select items from the list that correspond to the hosts, mailboxes, or actions you want to exclude from tracking.

All exclusions are considered independently. For example, assume you select `Exclude all non-production trading partner connections`, and `newTradingPartner1` in the trading partners section and `AS2` in the hosts\mailboxes\actions section. With these selections, a file processed through the system will be excluded from tracking if its action is associated with the **AS2** host, or its action is associated with `newTradingPartner1`, or its action is associated with a non-production trading partner connection.

XML Reference

The **New XML Reference** dialog box is displayed when you click **New XML** in the **File Tracking List** in the **File Tracking Options** dialog box. The **Edit XML Reference** dialog box is displayed when you double-click an XML item or right-click an XML item and then select **Edit** in the **File Tracking List**.

In **New XML Reference** or **Edit XML Reference** dialog box, specify values for the following fields:

XML Configuration

Description

A unique description of this reference.

Extract data on inbound transfers

Extract data on outbound transfers

Select these check boxes to track this reference on inbound and outbound transfers, respectively. You can select either or both.

Identify XML files by

Define the means by which the tracking software should identify the XML files being considered.

Select either **root element** or **namespace** and provide a value for comparison.

Identifier Data

Unlike EDI tracking, where the identifier data is automatically tracked when EDI tracking is enabled, XML tracking requires the user to specify the paths to the desired identifier nodes. Fill in the node entries in the **Identifier Data** table to provide path information. Specify nodes in the following ways:

- using a proper XPath notation for the XML element or attribute. The subset of W3C characters that are supported are `A-Za-z0-9._/@\-`. See http://www.w3.org/TR/xpath for a complete description of XPath. For **Document Type** and **Document Date/Time** you can concatenate two XPaths together by using an ampersand (&) between the two XPath elements.

- using a string literal enclosed in double quotation marks. In this case, the tracking software merely passes the literal straight through for storage in the database.

Transactional Data

Specify one or more records in the **Transactional Data** table.

- **Insert a new row**: Click **New** to insert a new row in the table and display the **Extract Transactional Reference** dialog, with none of the fields populated.
- **Edit a row**: Right-click a row and select **Edit** or double-click a row to display the **Extract Transactional Reference** dialog, populated with data from the selected row.

See Extract Transactional Reference on page 899.

Extract Transactional Reference

The **Extract Transactional Reference** dialog box is displayed when you select an item to edit or you click **New** in the **Transactional Data** table. Edit or populate the following fields:

Extract node

Identify a node you want to track.

As you specify the node you want to track, observe these guidelines:

- The **root element** and the XPath strings should not contain namespace prefixes. The XPath strings will be matched regardless of the namespace prefix used in the XML payload.
- Based on the RNIF mailbox setting, **Incoming content format**, the configuration of **root element** and the XPath elements are affected. If the RNIF mailbox setting, **Incoming content format**, is set to:
  - **Original**: The root element and XPath elements should start with the root element of the XML payload.
  - **Wrapped XML**: The root element and XPath elements should start with the /pip/serviceContent/ followed by the root element of the XML payload.
  - **Wrapped CDATA**: Tracking cannot be performed.
  - **Wrapped BASE64**: Tracking cannot be performed.

only if node

Select this check box to apply a condition. If you select the check box, you must also specify a path and a value for comparison.

match ('=') fields

Select this check box to track this reference when the **element** and **subelement** meet the conditions you specify. If you select this check box, you must specify a value for the **element** field. The **subelement** is optional.

Storage Location for Extracted Data

Specify where to store the collected reference data. Each reference collected will be separated by commas, and optionally preceded by the label, when it is displayed through the **View Information** right-click option under transfer reporting.

Reference 1

Reference2

Select the reference in which to store the data.

Reference Label

Optional - a label for the reference.

Text tracking

Text Reference

Use the **Edit Text Reference** dialog box to enter a unique description describing this reference, specify whether you want to track this reference on inbound transfers, outbound transfers or both, and specify tracking inclusions.

Text Configuration

Description

A unique description of this reference.

Extract data on inbound transfers

Extract data on outbound transfers

Select these check boxes to track this reference on inbound and outbound transfers, respectively. You can select either or both.

Tracking Inclusions

Unlike EDI and XML tracking, where you can optionally specify items to be excluded from tracking, for text tracking, you specify items you want *included* in tracking. You must specify at least one inclusion. Also, unlike EDI and XML, where the exclusions are specified at global level, for text tracking, inclusions are specified *for each individual reference*.

Click **Edit Inclusions** to display a list where you can choose inclusions as follows:

- **Include all production trading partner connections**
- **Include specific trading partner connections** - Select items from the list that correspond to the trading partners you want to include in tracking.
- **Include specific folders** - Select items from the list that correspond to the folders you want to include intracking.
- **Include specific hosts\mailboxes\actions** - Select items from the list that correspond to the hosts, mailboxes, or actions you want to include in tracking.

Only track files named

Select the check box and specify a filename to which you want to limit tracking. You can use regular expressions and wildcards to specify a filename.

Lines

Within the **Lines** container:

- enter a **Fixed line length** or a **Variable line delimiter**. Line delimiters cam be either a single character or '\n' (newline) or '\\' (backslash).
- optionally specify **Number of header lines to skip before parsing**.

Fields

Within the **Fields** container

Choose whether fields will specified by character position (**Positional (n:m)**) or by field number (**Delimited by**). When fields are separated by a delimiter, the delimiter character may be either a single character or '\t' (tab).

Identifier Data

Unlike EDI, where the identifier data is automatically tracked when EDI tracking is engaged, for text you must specify the text fields you want to track. Right-click a row in the **Identifier Data** table and select **Edit** to display

a dialog box where you can enter information about the data to extract. Use the following fields to enter this information:

Extract Field

Enter information about the field in one of the following ways:

either or a string literal enclosed in two quotation marks.

- **Using proper syntax for field specification** - For positional fields, you must enter a string of the form `n:m` where `m` must be greater than or equal to `n`. For delimited fields, you must enter a single number. In all cases, whether you specify positional or delimited fields, all positions are *one-based*. That is, the first field or character of a line is specified as `1` and not `0`.
- **Using a string literal enclosed in two quotation marks** - If you key in a string literal, the other fields in the dialog box are disabled. This is because the tracking software merely passes the literal straight through for storage in the database.

only on line number

Select the radio button and specify the line number from which to extract the data. You cannot select both this radio button and the **only if field** radio button.

only if field

Select the radio button and specify criteria to select the field from which to extract the data. You cannot select both this radio button and the **only on line number** radio button.

Extract Transactional Reference

The **Extract Transactional Reference** dialog box is displayed when you select an item to edit or you click **New** in the **Transactional Data** table. Edit or populate the following fields:

Extract field

Identify a field you want to track.

only on line number

Select the radio button and specify the line number from which to extract the data. You cannot select both this radio button and the **only if field** radio button.

only if field

Select the radio button and specify criteria to select the field from which to extract the data. You cannot select both this radio button and the **only on line number** radio button.

Storage Location for Extracted Data

Specify where to store the collected reference data. Each reference collected will be separated by commas, and optionally preceded by the label, when it is displayed through the **View Information** right-click option under transfer reporting.

Reference 1

Reference2

Select the reference in which to store the data.

Reference Label

Optional - a label for the reference.

Polling

Note: This section applies to Cleo VLTrader and Cleo Harmony only.

In the web UI, go to **Administration** > **Monitoring** > **Polling**. In the native UI, go to **Options** > **Monitor** > **Polling**. The **Polling** sub-tab lists each polling category and interval:

Category	Description	Default Interval (seconds)
Actions History	Action result counts	15
Active Actions	Active actions and types	5
CPU	Overall CPU percentage usage	5
Database Payload	Database payload running status and active and backlog payload queue counts	5
Memory	Heap and perm gen space available and consumed	5
Operator Session	UI sessions and categories	5
Router	Router running status and active, disabled, and total number of routes	5
Scheduler	Scheduler running status and cycle time and active, disabled, and total number of scheduled actions	5
Server Port	Configured and listening server ports and active connection counts	5
Storage	VersaLex installation disk space used and total	30
Synchronization	For each VersaLex in the same pool, synchronization status and pending and unresolved synchronization error counts	15
System Queue	System log, transfer log, and operator audit trail queue used and maximum entry counts	5
System Transfer Rate	Overall system inbound/outbound transfer rates	5
Thread	Normal and deadlocked thread counts	5
Transfer Logging	Transfer logging DB connection	15
Unsolicited Status	Server session result counts	15
Uptime	VersaLex uptime counter	30
VL Proxy	VLProxy connection	15

System monitor polling intervals are configurable for a variety of reasons such as disk space optimization, System Monitor dashboard performance, CPU usage, and the minimum threshold check interval. The default configuration will be suitable for most cases so you should have little need to adjust any of these values.

When the System Monitor is enabled, a trade off exists when setting these intervals. A shorter polling interval uses more disk space but provides more granular data to the System Monitor dashboards and as such may provide better information to the system administrator. A longer polling interval consumes less disk space for the database but may provide better System Monitor dashboard performance on a slow system. A minimum polling interval of 5 seconds is enforced.

Thresholds

Note: This section applies to the Cleo VLTrader and Cleo Harmony applications only.

In the web UI, go to **Administration** > **Monitoring** > **Thresholds**. In the native UI, go to **Options** > **Monitor** > **Thresholds**. The **Thresholds** page lists each available threshold item, the threshold setting, the duration at the threshold value before considered an error condition, and whether or not an error should be logged and/or an SNMP alert delivered.

Account Lockout

A local user has been locked out due to too many failed login attempts.

Detection not subject to polling intervals. The **Log Error** check box is selected by default and cannot be cleared.

Attempted Invalid File Type

A user attempted to upload or rename a file not matching any values configured for 'Acceptable inbound file patterns' (FTP/SSH FTP Users) or 'Acceptable inbound media types' (HTTP users) and the request was rejected.

The **Log Error** check box is selected by default and cannot be cleared.

Blacklisted

An IP address has been blacklisted due to too many failed login attempts based on automatic IP blacklisting settings.

Detection not subject to polling intervals. The **Log Error** check box is selected by default and cannot be cleared.

Blocked By Blacklist

One or more connection attempts were made from IP addresses on the IP blacklist and the connections were closed.

Detection not subject to polling intervals. The **Log Error** check box is selected by default and cannot be cleared.

Blocked by Lockout

A local user whose account is locked attempted to log in and was blocked.

Detection not subject to polling intervals. The **Log Error** check box is selected by default and cannot be cleared.

Blocked By Whitelist

A local user attempted to log in from an IP address not on the IP whitelist and the login attempt was blocked.

Detection not subject to polling intervals. The **Log Error** check box is selected by default and cannot be cleared.

CPU Usage

Percentage of the overall, available CPU used by the Cleo Harmony or Cleo VLTrader service/daemon process.

Default value is 90% for 60 seconds.

Database Payload Backlog

Count of backlogged database payload entries.

Default value is 50 count for 30 seconds.

Deadlocked Threads

Any deadlocked threads within the Cleo Harmony or Cleo VLTrader service/daemon process.

Default value is not applicable.

Disk Storage Usage

Percentage of the available Cleo Harmony or Cleo VLTrader installation disk space used.

Default value is 90% for 30 seconds.

Exceeded Max Concurrent System Sessions

The maximum number of concurrent FTP users allowed at the system level has been exceeded and the login attempt was rejected.

Detection not subject to polling intervals. The **Log Error** check box is selected by default and cannot be cleared.

Exceeded Max Concurrent User Sessions

A Local User has exceeded their maximum concurrent logins and the login attempt was rejected.

Detection not subject to polling intervals. The **Log Error** check box is selected by default and cannot be cleared.

Heap Memory Usage

Percentage of the maximum heap space used by the Cleo Harmony or Cleo VLTrader service/daemon process.

Default value is 90% for 30 seconds.

Local Certificate Expired

The certificate used for Local Packaging has expired.

The **Log Error** check box is selected by default and cannot be cleared.

Operator Audit Trail Queue Backlog

Percentage of the maximum operator audit trail queue used by the Cleo Harmony or Cleo VLTrader service/daemon process.

Default value is 90% for 30 seconds.

Partner Certificate Expired

The certificate used for Partner Packaging has expired.

Detection not subject to polling intervals. The Log Error check box is selected by default and cannot be cleared.

Perm Gen Memory Usage

Percentage of the maximum perm gen space used by the Cleo Harmony or Cleo VLTrader service/daemon process.

Default value is 90% once.

Scheduler Cycle Time

Seconds for the (master) Cleo Harmony or Cleo VLTrader scheduler to cycle through the entire schedule.

Default value is 300 seconds once.

Server Port Listening

Any configured server port listening failures.

The **Log Error** check box is selected by default and cannot be cleared.

Synced VersaLex Connection

Any synced Cleo Harmony or Cleo VLTrader communication failures.

The **Log Error** check box is selected by default and cannot be cleared.

Synchronization Backlog

Count of backlogged synchronization items with another Cleo Harmony or Cleo VLTrader instance in the same pool.

Default value is 50 count for 60 seconds.

Synchronization Item(s) Unresolved

Any failures to synchronize changes to synced Cleo Harmony or Cleo VLTrader instance.

Default value is not applicable.

System Log Queue Backlog

Percentage of the maximum system log queue used by the Cleo Harmony or Cleo VLTrader service/daemon process.

Default value is 90% for 30 seconds.

Thread Usage

Count of the overall number of active Cleo Harmony or Cleo VLTrader service/daemon process threads.

Default value is 500 count for 30 seconds.

Transfer Failed

A file transfer failed. This could occur for many different reasons. See the Cleo Harmony or Cleo VLTrader system log for further details. Detection not subject to polling intervals.

The **Log Error** check box is selected by default and cannot be cleared.

The `Transfer Failed` event is only fired for transfers that fail while connecting to a Cleo Harmony or Cleo VLTrader FTP, SFTP, or /server (that is, plain HTTP/s) server. Notifications are not available for client-side or inbound AS2 transfer failures.

Transfer Log DB Connection

A transfer logging database connection failure.

The **Log Error** check box is selected by default and cannot be cleared.

Transfer Log Queue Backlog

Percentage of the maximum transfer log queue used by the Cleo Harmony or Cleo VLTrader service/daemon process.

Default value is 90% for 30 seconds.

VLProxy Connection

Any configured Cleo VLProxy communication failures.

The **Log Error** check box is selected by default and cannot be cleared.

SNMP agent

Note: This section applies to the Cleo VLTrader and Cleo Harmony applications only.

In the web UI, go to **Administration** > **Monitoring** > **SNMP Agent**. In the native UI, go to **Options** > **Monitor** > **SNMP Agent**. The **SNMP Agent** sub-tab allows you to configure an agent that provides a means to acquire information about the Cleo Harmony or Cleo VLTrader software's operation by polling and asynchronous notifications, via the SNMP protocol.

Enabled

Select this check box to activate the agent. Clear the check box to deactivate the agent.

Agent Listener Threads

Determines the number of concurrent request the agent can handle.

Engine ID

A hexadecimal value that uniquely identifies the agent for this Cleo Harmony or Cleo VLTrader instance. The product serial number is used as the administratively assigned textual identifier.

Contact

Optional. Provide a name for the person responsible for administering the agent.

Listening Ports

A list of ports on which the agent will answer polling requests and from which the agent will deliver notifications.

Click **New** to add a port.

Double-click an existing port to edit it.

Users

Allows you to activate and fill in credentials for an SNMPv1/2c (community) user or an SNMPv3 (USM) user. At least on active user is required.

Notifications

Click the button to display the **Notifications** dialog box, where you configure optional notification targets and their parameters. Notifications delivered correspond to the selected SNMP Alerts configured in the **Thresholds** panel.

Enabled

Select this check box in the Notifications dialog box to activate notifications for the selected targets. Clear the check box to deactivate notifications.

Aggregate

Select this check box to combine alerts statuses from all the selected SNMP Alerts into a single notification that summarizes the overall status instead of delivering unique notifications.

Notifications table

A list of notification targets. Click New to add a target. Double-click a target to edit it.

Export MIBs

Click the button to export private enterprise MIBs (implemented by the agent) to the desired file system location. The user can import the MIBs into an agent manager.

Note: In addition to the private enterprise MIBs, the manager will require the following standard SNMP MIBs, which are freely available online if they are not already imported:

- SNMP-FRAMEWORK-MIB
- SNMPv2-CONF
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPv2-TC.

Embedded database

Note: This section applies to the Cleo VLTrader and Cleo Harmony applications only.

In the web UI, go to **Administration** > **Monitoring** > **Embedded Database**. In the native UI, go to **Options** > **Monitor** > **Embedded Database**. The **Embedded Database** sub-tab allows for configuration of the Cleo Harmony or Cleo VLTrader local embedded H2 (www.h2database.com) relational database created for and used by the Cleo System Monitor application.

Database Port Number

The standard H2 SQL connection listening port. This is the port connected to by the Cleo System Monitor application for rendering system status.

Default value: `9092`

Web Server Port Number

The H2 web server portal. The H2 web portal can be accessed from a web browser using an URL of the form `http://CleoProductNameComputerIP:WebServerPortNumber`.

Default value: `8082`

View Only User Password

corresponds to the embedded database *viewonly* user. The viewonly user is used by the Cleo System Monitor SQL connection, and can also be used when accessing the H2 web server portal. Any Cleo System Monitor Dashboards that are open when a password change occurs will enter an error state. Logging out of the monitor and back in will correct this issue.

Purge Data After

The amount of system status history kept in the database (and available in Cleo System Monitor)

Default value: 14 days

Chapter

12

Cleo Portal

Configuring Cleo Portal

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

This section describes how to configure your Cleo Portal system.

You can:

- Provide admin users single-login access to both Cleo Portal and the Cleo Harmony or Cleo VLTrader applications.
- Customize the look and feel of Cleo Portal.

Customizing Cleo Portal

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

You can customize the look of your Cleo Portal by modifying its CSS and replacing certain background and logo graphics files displayed on the login page.

Customizing your Cleo Portal banner and login page graphics

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

You can modify the `custom.css` file to customize the look of your Cleo Portal banner and login page.

1. Navigate to *<installdir>*`/webserver/mftportal/styles/` and open `custom.css` in a text editor.
2. Modify the `custom.css` file as necessary.

   Include `#top-banner` items in the `custom.css` to affect the banner and `#Login` items to affect the login page graphics.

   For example, to specify `cloud-background.png` as the background image for the login page, copy the image to the webserver/mftportal/ directory and include the following in the custom.css file:

   ```
   #LogIn {
          background-image: url(../cloud-background.png);
   }
   ```

   Note: The URL is relative to `webserver/mftportal/styles`.

   See Cleo Portal CSS customization parameter reference on page 912 for information about styles you can customize.
3. Save your updates and refresh the Cleo Portal window to see your changes.

Note: If you re-run the installer, the `custom.css` file is reinstalled with the product and you must make your customizations again.

Cleo Portal CSS customization parameter reference

Use these selectors to control the style of the Cleo Portal.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

Note: Unless otherwise stated, changes to the height, width or text size of any element or attribute are not supported.

Top banner

#top-banner

Controls the style of the top navigation banner.

You can also reference `#top-banner` as `.navbar-default`.

#top-banner .banner-text a

Controls the default style of the navigation labels in the top navigation banner.

#top-banner .banner-text a:hover

Controls the hover style of the navigation labels in the top navigation banner.

#top-banner .banner-text a.active

Controls the style of the active navigation label in the top navigation banner.

#top-banner .banner-text a .icon

Controls the style of top navigation banner icons.

#top-banner .banner-text a.active .icon

Controls the style of the active navigation icon in the top navigation banner.

#top-banner .icon-avatar

Controls the style of the user avatar icon.

#top-banner .icon-avatar:hover

Controls the style of the user avatar icon on hover.

#top-banner .icon-avatar.open

Controls the style of the user avatar icon when user menu is open.

Log in page

#LogIn

Use the element to update the background color and/or image.

#LogIn .login-image

Use this element to update the corporate logo.

#btn-default[:hover, :active]

Use this element to update the **sign in** button.

Main masthead

app.portal .navbar-brand

Use this element to update the corporate logo on the main masthead. You will need to explicitly set the width. Maximum dimensions for a new logo is 200px X 65px.

.navbar-default

Use this element to update the background and border colors.

Buttons

.btn-primary[:active, :hover]

Use this element to update the background and border color of all buttons within Cleo Portal.

Background images

New images do not need to be placed within the Cleo Portal directory. You can place them anywhere on your server, a CDN, or anywhere that will provide a publicly accessible URL.

Setting Cleo Portal System Properties

You can set the following properties in your `conf/extended.properties` file to further customize your Cleo Portal experience.

external.ip.address

Set this property to customize URLs in Cleo Portal email links. For example, setting the property to `external.ip.address=my-company.com` would change outgoing URLs in Cleo Portal emails to `https://my-company.com/Portal/...`. Note that some protocols (excluding AS2) can use the `external.ip.address` property for various operations. The port properties will only ever be used by HTTP and HTTPs based protocols.

external.ip.address.http.port

Set this property to customize URLs in Cleo Portal email links if a different port than specified in the local listener is necessary. Port properties will only be used if the `external.ip.address` property is set. If both `http` and `https` ports are specified here, the `https` port will take precedence.

external.ip.address.https.port

Set this property to customize URLs in Cleo Portal email links if a different port than specified in the local listener is necessary. Port properties will only be used if the `external.ip.address` property is set. If both `http` and `https` ports are specified here, the `https` port will take precedence.

Setting up single-login access to Admin UI and Cleo Portal

You can configure your system to allow users to log in one time to access both the Web Admin UI and the Cleo Portal UI.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

Before you begin, you must have a secure port configured for your Local Listener (see Configuring a Local Listener for HTTP on page 750), a resource path for Cleo Portal set (see Local Listener Web Browser Service on page 781), and admin users available and enabled on your system (see Cleo VLNavigator User Tab on page 931.)

Once your system is properly configured, admin users can log in to Cleo Portal via HTTPs, enabling the drop-down menu used to toggle between User mode (Cleo Portal) and Admin mode (Cleo Harmony or Cleo VLTrader).

1. Set up a **VLNav** connector host.
   a) Go to **Hosts** > **Templates**.
   b) Open the **Generic** folder, right-click the **Generic VLNav** template, and select **Clone and Activate**.
      The **VLNav** host is added to the **Active** tab.
   c) Enter a name for your new VLNav connector in the **Host Alias** field.
   d) Click **Apply** to save your work.
2. Create a new Users host.
   a) If you do not already have an active **Users** host, go to the **Templates** tab, open the **Generic** folder, right-click the **Generic Users** template, and select **Clone and Activate**.
      The **Users** host is added to the **Active** tab.
   b) Right-click the **Users** host and select **New User Mailbox**.
      The **New User Mailbox** dialog box appears.
   c) Specify an alias for your mailbox and click **OK** to dismiss the dialog box and display the Login tab.
   d) On the Login tab, select `Connector Host` from the **Authentication** > **Type** field.
   e) Enter a value in the **Authentication** > **Authenticator** field.
      This value should be in the format `scheme:alias`, where the `scheme` is `VLNav` and the `alias` is host you created above.
   f) Optionally, click **List Users** to view a list of admin users who belong to this group.
   g) Click **Apply**.
3. Log in to Cleo Portal as one of the users you just configured.
   In the upper-right corner of the page, there is a pull-down menu you can use to toggle between User mode (Cleo Portal) and Admin mode (Cleo Harmony or Cleo VLTrader).

   Note: If you disable all protocols in the **Users Privileges** tab, an admin that logs into Cleo Portal is immediately redirected to the Web Admin UI and the toggle is not available.

For information about using SAML with Cleo Portal users, see SAML configuration on page 696.

Two-factor authentication

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

Two-factor authentication (TFA) is available for users. The two-factor authentication security option is available for users in the **Privileges** tab.

Note: Cleo Harmony only: if two-factor authentication is enabled, the user will not be able to use the Cleo Connector for Outlook.

First Time Registration:

The first time a user successfully logs in with TFA required, a notification appears with a username and password stating that an email has been sent to the registered email address with a link to complete the registration.

1. When the email arrives, click the link to navigate to the registration page. On this page, a wizard appears to help set up a client authenticator application. Choose a client authenticator application based on your system's needs. Recommended authenticator applications are Windows Authenticator, Google Authenticator for Android, and Google Authenticator for iOS, but any authenticator application that supports TOTP protocol will work.

   A QR code and text representation of the **shared key** are presented. These contain the same information. Either can be used to synchronize the client authentication application with Cleo Harmony and Cleo VLTrader.

2. Enter the information into the authenticator application and click **Next**.
3. The verification step allows the user to test that the authenticator application has been set up properly. To test the application, enter the username, password, and code from the client authenticator application. Click **Test**. Upon successful verification, a success message appears, and the **Finish** button is enabled.

The user can now log into the system using two-factor authentication. Navigate to the login page and follow the **Daily Use** instructions below.

Daily Use:

Enter the username and password and click **Log In**. A dialog box appears with a field labeled **TOTP Code** (time-based one-time password).

Enter the code received from the client authenticator application and click **Submit Code**.

If the code is valid, login is successful.

Resetting TOTP Key:

To the right of the input field in the **TOTP Code** dialog is a **Reset Key** link. Clicking this link will deactivate the user's current two-factor authentication setup, send a new registration email to the user's email address, and instruct the user to reregister at login. Follow the first time registration process outlined above to set up the authenticator again.

Enabling mixed mode authentication for Cleo Portal

You can allow Cleo Portal users to log in using SAML or local credentials.

Mixed mode authentication is enabled when both SAML and local logins are enabled. When mixed mode authentication is enabled, the Cleo Portal log in page displays a check box labeled **Use Company Login**, which allows the user to choose the SAML login.

When the user chooses to use SAML login, the **Username** and **Password** fields disappear and when the user clicks **Log in**, the SAML log in page is displayed.

When the user chooses not to use the company login, **Username** and **Password** fields are displayed, allowing the user to enter local login credentials.

1. Go to **Administration** > **Users** > **SAML**.
2. Select the **Enable SAML login for Cleo Portal users** check box and the **Allow local login for Cleo Portal users** check box.

   See SAML service provider reference on page 698 for more information about these parameters.
3. Click **Save**.

Cleo Portal users will be able to log in using either their company login (SAML) or their local credentials.

Note:

You can bypass the Cleo Portal log in page and go directly to your SAML log in by adding a query string parameter /Portal endpoint. The URL should be specified as '/Portal?sso=true'.

Copying items in Cleo Portal

You can copy files and folders in Cleo Portal using the **Copy selected item** button.

To copy an item:

1. Select the item(s) to be copied. The **Copy selected item** button in the button row is enabled.
2. Click **Copy selected item** to open the **Copy** dialog box.
3. Select a destination for the copied item. If necessary, you can rename the copied item in the **Item name** field.
4. Click **Copy**. The item is copied and, if applicable, the copied item is renamed.

Note: You can only rename a single copied item; you cannot rename a group of items. You cannot copy an item into its own folder.

Note: You can copy items between spaces (**Home**, **Shared with me**, and **Connections**).

Moving items in Cleo Portal

You can move files and folders in Cleo Portal using the **Move selected item** button.

To move an item:

1. Select the item(s) to be moved. The **Move selected item** button in the button row is enabled.
2. Click **Move selected item** to open the **Move** dialog box.
3. Select a destination for the moved item. You can also rename the item using the **Item Name** field.
4. Click **Move**. The item is moved and, if applicable, renamed.

Note: You cannot move an item into its own folder. You cannot *move* items between spaces (**Home**, **Shared with me**, and **Connections**), but you can *copy* items between spaces. See Copying items in Cleo Portal on page 915 for more information.

Renaming items in Cleo Portal

You can rename files and folders in Cleo Portal using the **Rename selected item** button.

To rename an item:

1. Select the item to be renamed. The **Rename selected item** button in the button row is enabled.
2. Click **Rename selected item** to open the **Rename** dialog box.
3. Type the new item name into the **Item Name** entry field and click **Rename**.
4. The renamed item appears in the list.

Note: You can only rename a single item; you cannot rename a group of items.

Note: If you attempt to rename the item with a name that is already in use in the target directory, a warning appears prompting you to either enter a different item name or overwrite the existing item.

Note: If you attempt to rename a shared item, you cannot give the item a name that is already in use in the item owner's directory.

Note: Attempting to change a file extension while renaming a file can make it become unusable.

Chapter

13

Cleo VLNavigator

The Cleo VLNavigator application is a Cleo Harmony and Cleo VLTrader add-on program for optional multiple Cleo Harmony and Cleo VLTrader user and application management. It facilitates:

- grouping Cleo Harmony and Cleo VLTrader items into *pools*
- defining user groups with specific Cleo VLNavigator, Cleo Harmony and Cleo VLTrader privileges
- creating individual user logins
- configuration of optional applications

For environments with multiple instances of the Cleo Harmony or Cleo VLTrader applications, the Cleo VLNavigator application can optionally be installed at each instance of Cleo Harmony or Cleo VLTrader software. If the instances of Cleo Harmony or Cleo VLTrader software are connected via synchronization, user groups or both, the Cleo VLNavigator applications will mirror each other much in the same way that fully-synchronized Cleo Harmony or Cleo VLTrader instances mirror one another.

The Cleo VLNavigator application is a component of the Cleo Harmony and Cleo VLTrader installers. The Cleo VLNavigator application does not have a corresponding service/daemon. Instead, it relies on the Cleo Harmony and Cleo VLTrader service/daemon, which must be running when the Cleo VLNavigator application is invoked.

Systems

The Cleo VLNavigator application allows multiple instances of the Cleo Harmony or Cleo VLTrader applications to be logically grouped into *pools*. Instances that synchronize at least one configuration item (for example, CA certificates, User certificates, Hosts, Schedule, and so on) must be in the same pool. Otherwise, disjointed Cleo Harmony or Cleo VLTrader instances can be placed in separate pools.

The installed Cleo Harmony or Cleo VLTrader instance and instances already synchronizing will automatically be placed in a default `mySystem` home pool when the Cleo VLNavigator application is first started. Additionally, any instances of the Cleo Harmony or Cleo VLTrader application reverse proxying through Cleo VLProxy software will be presented to the Cleo VLNavigator user for optional inclusion in a pool.

Synchronization can only be setup in Cleo VLNavigator for Cleo Harmony or Cleo VLTrader instances in the `home` pool, which contains the local Cleo Harmony or Cleo VLTrader instance. For instances outside of the home pool, synchronization must either be setup directly on the Cleo Harmony or Cleo VLTrader instances themselves or Cleo VLNavigator software must be installed on and invoked from at least one of the Cleo Harmony or Cleo VLTrader instances. For these additional pools, once the first instance is added, any other instance it is synchronized with will also be automatically added to the pool.

Pools, including the default `mySystem` home pool, can be named with any alias. The home pool must be renamed before another pool can be added. Cleo Harmony or Cleo VLTrader instances must be identified by their serial number, but can also have an additional, optional alias.

User groups are assigned access to either all instances within a pool or individual instances.

User groups

User privileges for both Cleo VLNavigator and Cleo Harmony or Cleo VLTrader applications are established using *user groups*. Within a user group, each privileged item is set to either no access, view-only, or editable. Cleo VLNavigator access is broken down into three privileges: the **Systems** tree, the **Users** tree, and the **Applications** tree. The **System** privileges match the list of configurable Cleo Harmony or Cleo VLTrader synchronization items (**CA certificates**, **User certificates**, **Hosts**, **Schedule**, etc).

A default **Administrators** group comes installed with full Cleo VLNavigator and Cleo Harmony or Cleo VLTrader privileges and cannot be modified. The Administrators group also cannot be renamed or deleted.

When the Cleo VLNavigator application is installed, by default the Cleo Harmony or Cleo VLTrader application does not require a login (except for the web UI). Once at least one user group is assigned to a specific Cleo Harmony or Cleo VLTrader instance or its pool, a login to that instance is required (and the existing web UI edit and view-only passwords are deactivated).

Users

A *user* can be a member of one and only one user group. A user consists of a username and password. It can also have an additional, optional alias.

A default administrator user within the Administrators user group comes installed. Its initial password is communicated by the installer, and should be modified as soon as possible. The administrator user cannot be renamed or deleted.

Optional Applications

Optional applications can be enabled or disabled at the user-group or user levels. Cleo VLNavigator software also allows for configuration of the optional applications.

Configuring the Cleo VLNavigator application

To configure the Cleo VLNavigator application, set up VersaLex Pools, Users, and optionally configure Applications. See VersaLex pools on page 880, Users on page 686, and Applications on page 660 for more information. Below are some quick steps to get you started with this application.

Creating a VersaLex pool

1. Right-click **Systems** in the tree pane and select **New VersaLex Pool**.
   The **New VersaLex pool** dialog box appears.
2. Enter a unique VersaLex pool name and click **OK**.
3. The new pool is selected in the tree, and a shortened version of the **Add VersaLex** dialog box below is displayed. Only a VersaLex serial number and its connection information are needed. Once the VersaLex is added, any other VersaLexes synchronizing with the VersaLex are automatically added to the new pool. This feature can take a few seconds to load.
4. The pool can be subsequently renamed or hidden by right-clicking the pool in the tree pane and selecting **Rename** or **Hide**. Note that a hidden pool can be automatically revealed if a user group permission is added for that pool.

Add a VersaLex

1. Right-click a Systems pool in the tree pane and select **Add VersaLex**.

The **Add VersaLex** dialog box appears. This is the same dialog box that is displayed in VersaLex when a synchronized VersaLex is first added.

2. Enter the serial number of the VersaLex being added, the system's computer name or address, and its HTTP or HTTP/s port. If the VersaLex you are adding is a backup system, select **High Availability Backup**. See Synchronizing user configuration on multiple instances on page 888 for more information about configuration options, particularly the list of synchronization items. If the VersaLex is being added to an empty pool, the synchronization items table is not applicable and is not displayed. Otherwise, at least one synchronization item is required.
3. Click **OK**.

   The Cleo VLNavigator application then attempts to connect to the added VersaLex instance and indicate whether the connection was successful or not.
4. If the VersaLex instance was added to a pool with other instances of VersaLex, an informational message appears to indicate that the new instance needs to be intialized from the "master" instance.

   The added VersaLex will be selected in the tree. The VersaLex can be subsequently renamed, edited, or removed by right-clicking the pool in the tree pane and selecting **Rename**, **Edit**, or **Remove**.

   The VersaLex can be moved to a different pool by right-clicking the pool in the tree pane and selecting **Move** or by clicking and dragging the VersaLex to a different pool.

View/Edit Trading Partners

If all the VersaLexes in the home pool are synchronizing Trading Partners, right-click the **Systems** home pool in the tree pane and select **Trading Partners** to display the **Trading Partner** table.

See Managing Trading Partners on page 631 for further details.

LDAP Configuration

This configuration is optional unless you intend to define LDAP Users who authenticate with an external directory service, such as Active Directory or Apache Directory Service, instead of VLNavigator.

1. Select **Users** in the tree pane and select the **LDAP Server** tab.
2. Enter the required user information. See Users LDAP Server for a description of this tab.
3. Click **Apply**.

Create a User Group

1. Right-click **Users** in the tree pane and select **New User Group** or right-click a **User Group** in the tree pane and select **Clone**.

   The **New User Group** dialog box appears.
2. In the **Alias** field, enter a unique user group alias.
3. On the **VLNavigator Privileges** tab and **System Privileges** tab, set Cleo VLNavigator and System privileges, respectively. See User Group VLNavigator Privileges on page 929 and User Group: System Privileges Tab on page 930 for more information.
4. On the **File Transfer Report** tab, set the **File Transfer** report. See User Group File Transfer Report Tab on page 930. Also enable the desired applications. See User Group Application Settings Tab on page 930.
5. Click **OK**.
   The new user group is selected in the tree.

The user group can be subsequently cloned, disabled, renamed, or removed by right-clicking the user group in the tree pane and selecting **Clone**, **Disable**, **Rename**, or **Remove**. Note that cloning makes a copy of the user group; the users within the group are not also copied.

Add a User

1. Right-click a user group in the tree pane and select **New User**.

   The **New User** dialog box appears.
2. Enter the required user information. See Cleo VLNavigator User Tab on page 931 for information about this tab.
3. Click **OK**.

   The new user is added to Cleo VLNavigator.

The user can be subsequently disabled, renamed or removed by right-clicking the user in the tree pane and selecting **Disable**, **Rename**, or **Remove**.

The user can be subsequently moved to a different user group by right-clicking the user (or multiple users) in the tree pane and selecting **Move** or by clicking and dragging the user to a different user group.

VersaLex pools

The **Systems** tree branch contains information regarding all the configured VersaLex pools. See Creating a VersaLex pool on page 880 for information about creating, renaming, or removing a VersaLex pool.

VersaLex Pool User Groups

The VersaLex Pool **User Groups** tab is view-only and shows which user groups have been granted access to this VersaLex pool. Use the **System Privileges** tab to grant access for each user group. See User Group: System Privileges Tab on page 930.

VersaLex Pool VersaLexes

The VersaLex Pool **VersaLexes** tab is view-only and shows the connection status of each VersaLex in this pool.

VersaLex Pool Transfers

The VersaLex Pool **Transfers** tab displays a graphic image of the total bytes transferred and includes additional statistics for each VersaLex in the pool for the time period specified by the Filter. A transfer report may be generated for each VersaLex by selecting **Details**.

Pre-requisite: Graphical viewing of transfers is only available for VersaLexes using Database Transfer Logging. See Transfers on page 895 and Logs on page 892. If any VersaLexes are using a database product that is different from the database used by the local VersaLex, those drivers must also be installed in the local lib/ext directory.

The option to view the **Details** for all the VersaLexes in the pool is also available when the following conditions are met:

1. All the VersaLexes in the pool have database transfer logging enabled. See Logs on page 892.
2. All the VersaLexes in the pool have Synchronized Hosts. See Synchronizing user configuration on multiple instances on page 888.
3. All the VersaLexes in the pool have either Synchronized System Options (see Synchronizing user configuration on multiple instances on page 888) or are all using the same database for Database Transfer Logging and have the same enablement and disablement options set for File Tracking. See Logs on page 892.

Saving or printing the graphs

To save or print a displayed graph or chart, right-click anywhere on the graph or chart to display a pop-up menu.

Choose **Save as** to display a file chooser allowing the graph or chart to be saved in PNG format.

Choose **Print** to print the graph or chart on the selected printer.

User Groups, Transfer Monitors, and System Counters

See Add a VersaLex on page 918 for information about adding, renaming, editing, moving, or removing an instance of the Cleo Harmony software.

About User Groups

The Cleo Harmony **User Groups** panel is view-only and shows which user groups have been granted access to this Cleo Harmony instance or its pool. Access is granted in each user group via the User Group: System Privileges Tab on page 930.

About Transfer Monitor

The Cleo Harmony Transfer Monitor panel displays a graphic image of either the **Bytes** or **Files** transferred (**Inbound**, **Outbound** or in **Both** directions) for each instance of Cleo Harmony software in the pool for the time period specified by the **Filter**. You can set the **Duration** for a period of hours using the pull-down values or by specifying any value between 1-48 hours. Additionally, values in the form `:MM` can be used to specify a period less than an hour. Pre-defined values are specified in the pull-down list, or any value between :01 and :59 may be specified. The graph will refresh automatically after every **Auto-Refresh Interval** (between 5 and 60 seconds) when the **End Date**/**End Time** is today/now.

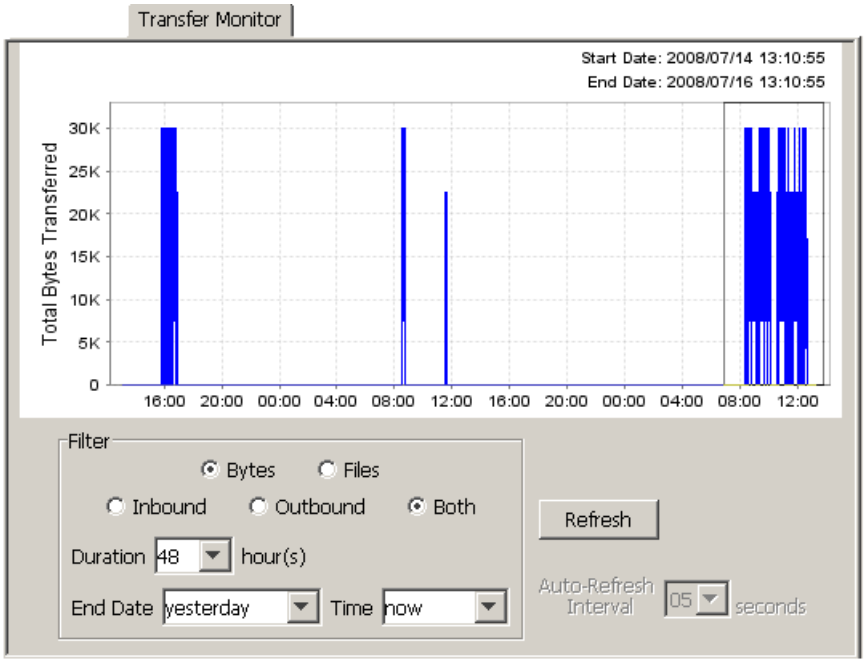
Note: Graphical monitoring of transfers data is only available for Cleo Harmony instances using Database Transfer Logging. See System on page 722. If any Cleo Harmony instances are using a database product that is different from the database used by the local Cleo Harmony application, those drivers must also be installed in the local lib/ext directory.

See Saving or printing the graphs on page 881 for information about saving or printing the graphical output.

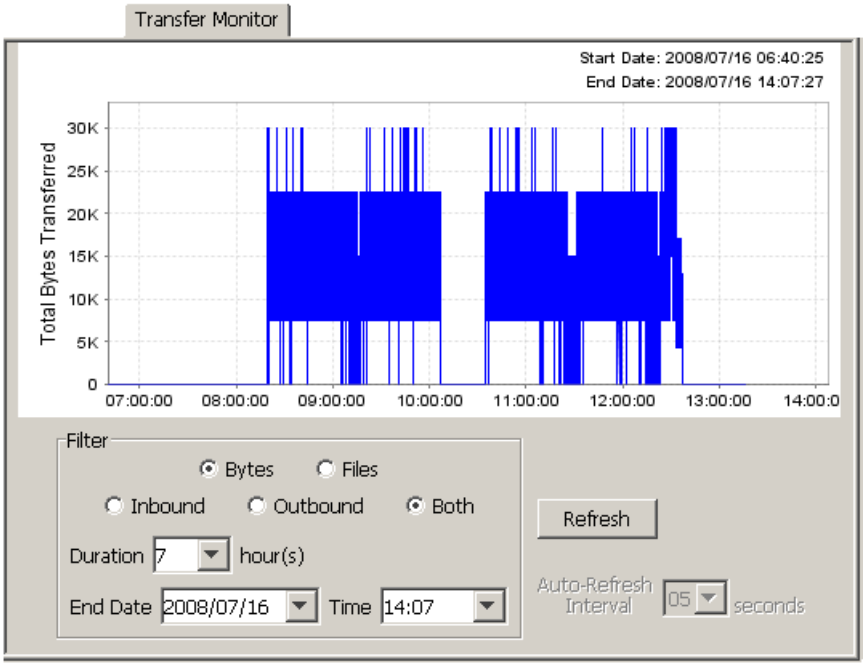
Getting Finer Granularity In Your Graphs

Cleo VLNavigator provides mechanisms for displaying finer granularity, especially when there are many data points within a specified time range. As mentioned in the previous section, durations of less than an hour can be specified to narrow the range of the plotted data points by optionally changing the **End Date** and/or **End Time**. Additionally, the data range can be zoomed in by dragging the mouse from left to right over a range of data points until the desired granularity is achieved.

In the following example, the range before 08:00 and after 12:00 has been selected (denoted by the gray box around the selected area):

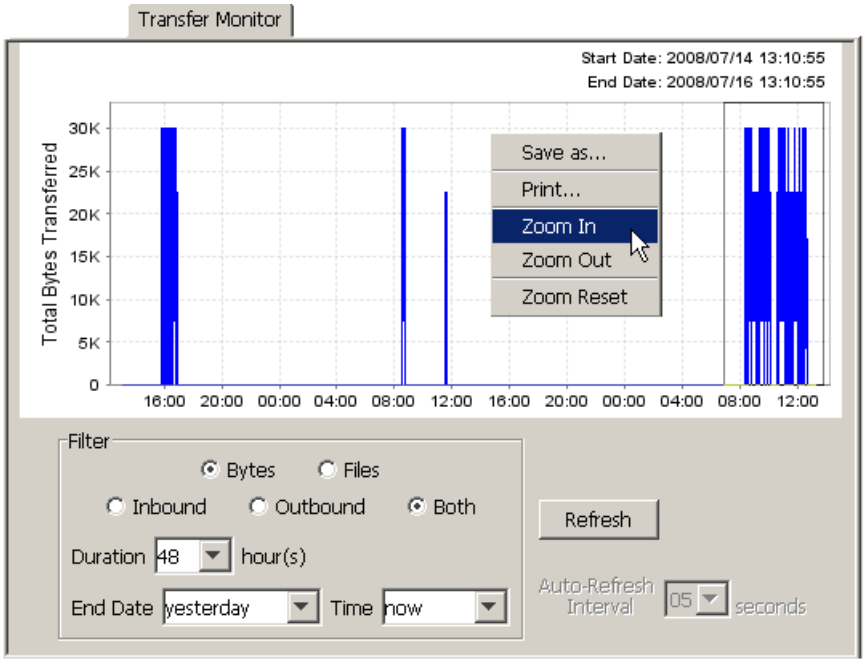


Then, the following updated graph is displayed:



This procedure can be done multiple times until the desired granularity is reached.

Another option for shrinking or expanding the displayed data set is to use the popup menu options available by right-clicking anywhere on the graph to **Zoom In**, **Zoom Out** or **Reset** the display back to the original graph:



Whatever method is chosen for zooming, **Refresh** will also reset the display to the original non-zoomed graph.

About System Counters

The VersaLex System Counters panel presents a graphical representation of the system counter data for the associated Cleo Harmony systems in the pool. The Cleo Harmony application keeps track of various system counters. These counters start accumulating from the first time Cleo Harmony software is invoked after product installation, and they continue accumulating while Cleo Harmony software is running. They are only reset when an overflow condition would occur. The following data are recorded:

- **From**: date/time the counter data were started
- **To**: date/time this display was last refreshed
- **Uptime**: percentage of time the Cleo Harmony application has been running between the from-date and to-date.
- The following transfer counters, grouped by protocol:
  - **Files In**
  - **Files Out**
  - **Total Files**
  - **Bytes In**
  - **Bytes Out**
  - **Total Bytes**

The pie chart shows a distribution of the transfer data by protocol. When viewing the chart, either the **Bytes** or **Files** transferred (**Inbound**, **Outbound** or in **Both** directions) can be displayed. **Refresh** is used to update the display in the case where new counter data are available (for example, a new transfer has occurred). See Saving or printing the graphs on page 881 for information about saving or printing the graphical output.

Users

The **Users** tree branch contains information about all configured user groups. Cleo VLNavigator supports authenticating users using its own database or using a directory service via LDAP. A non-LDAP user with

administrative privileges, such as the default administrator user, should be defined in case the LDAP server is not functional.

Note: If you have an Administrator user configured in Cleo VLNavigator and a Users host user configured in Cleo Harmony or Cleo VLTrader with the same username, you might experience issues logging in to your system with the Adminstrator user. To resolve possible issues, you can rename or remove the Users host user or change the configuration of the Users host user to use VLNav Connector Host authentication.

Configuring the Cleo VLNavigator LDAP server

Use the **LDAP Server** tab in Cleo VLNavigator to configure the LDAP server to authenticate internal administrators and operators of the Cleo VLNavigator and Cleo Harmony applications.

1. In Cleo VLNavigator, click the **Users** node in the tree view.

   The **LDAP Server** tab appears.
2. Select the **Enabled** check box to enable the fields on the tab.

   If the LDAP server is disabled (the **Enabled** check box is cleared), any LDAP users and the Default LDAP group, if it exists, are displayed in yellow to indicate the LDAP server is currently disabled and, therefore, all LDAP accounts are currently not usable.
3. Specify values for the fields in the **Server Configuration** section.

   See Cleo VLNavigator LDAP server configuration reference on page 687.
4. Specify values for the fields in the **Domain Configuration** section.
   a) Add servers to the list of active LDAP servers. Either retrieve LDAP service records or add them manually.
      - To retrieve LDAP service records, select the **Lookup** check box, specify a value in the **Domain** field, and click **Refresh**. LDAP service records found in the domain you specify are displayed in a table.
      - To add LDAP service records manually, clear the **Lookup** check box, and click the **New** button to display a dialog box in which you can enter information for a new record. When you are finished entering the information, click **OK** to dismiss the dialog box and display the new record in the table.

        Click **New** to add more new records as necessary.

        While the **Lookup** check box is cleared, you can right-click service records to edit them or remove them from the list.

   b) Specify values for **Base DN**, **Search Filter** and **Username Attribute**.

      See Cleo VLNavigator LDAP domain configuration reference on page 687 for information about the fields in the **Domain Configuration** section.
   c) Optional. Click **Advanced** to specify password expiration settings. The **Advanced** button is enabled only when you select `Active Directory` from the **Directory Type** menu. See Cleo VLNavigator LDAP server configuration reference on page 687.
   d) Click **Test** to test changes before they are applied. Enter an LDAP username and password. Changes to the **Server Configuration** panel are not applied until after a successful test login to the LDAP server.
5. Specify values for the fields in the **User Configuration** section.

   See Cleo VLNavigator LDAP user configuration reference on page 690.

Cleo VLNavigator LDAP server configuration reference

Enabled

Select the check box to enable LDAP connections to the configured server. Clear the check box to disable LDAP connections. When this check box is cleared, LDAP users are not able to log in.

Directory Type

The product used for the external LDAP directory service.

Possible values:

```
Active Directory
Apache Directory Services
Lotus Domino(IBM)
Novell eDirectory
DirX(Siemens)
```

Security Mode

If the directory server requires use SSL, specify a security mode. Otherwise, select `None`.

Possible values:

`None` - Information retrieved from the directory server will be clear-text.

`SSL` - Select when your servers support only SSL connections.

`StartTLS` - Select when your servers support SSL by use of the `StartTLS` command.

Cleo VLNavigator LDAP domain configuration reference

Lookup

Select the check box to use the value in the **Domain** field for retrieving SRV (Service) records for the LDAP service cluster.

Clear the check box to add records to the table manually.

Domain

The name of the domain from which you want to retrieve SRV records.

Click **Refresh** to refresh the information in the table using the value in the **Domain** field.

SRV record table

The SRV record table displays information about SRV records. Each row in the table represents one SRV record. Each row contains the following columns:

Enabled

Select this check box to use the record. Otherwise, the record is ignored.

Hostname

The target machine on which the LDAP service is running.

Port

The port used to connect to the LDAP service. Typically, the port `389` is used for non-secure (`None`) or StartTLS mode and `636` is used for SSL mode.

TTL

The `Time To Live` value defined as the time interval (in seconds) that the LDAP service record can be cached before the source of the information (for example, the domain) should again be consulted. A value of zero means that the LDAP record can only be used for the transaction in progress, and should not be cached. You can also use a value of zero for extremely volatile data.

Priority

The priority of the LDAP server. Attempts are made to contact LDAP servers with the lowest-numbered priority first. LDAP servers with the same priority are contacted in the order specified by the Weight field.

Possible values:`0-65535`

Weight

A server selection mechanism that specifies a relative weight for entries with the same priority. Larger weights are given a proportionately higher probability of being selected. Use a zero value when server selection is not required.

When there are records with weight values greater than zero, records weighted with a zero value will have a very small chance of being selected. When all priority and weight values are the same, the LDAP servers are selected in random order.

Possible values: `0-65535`

Base DN

The base organizational unit where the users are defined. Contact your directory administrator for the correct Base DN value. (The Base DN value entered here can be overridden in a local user host LDAP mailbox.)

The examples the table below show sample base organizational units for the supported directory types.

Directory Type	Example Base DN
Active Directory	`OU=Employees,DC=company,DC=com`
Apache Directory Services	`OU=Users,DC=example,DC=com`
Lotus Domino	`O=SCNotes`
Novell eDirectory	`O=Company Organization`
DirX	`ou=Users,o=Company`

Search filter

Optional. Used to limit the amount of information returned from the LDAP server when many users are defined. A more restrictive filter can be specified as a comma separated list. If necessary, contact your directory administrator to determine the appropriate attributes and values. You can override the value entered here in a local user host LDAP mailbox.

The following table contains example lists with sample attribute names and values.

Search Filter	Description
`department=EDI`	Limits the search to entries that have the attribute, `department`, with a value of `EDI`.
`department=EDI,group=administrators`	Limits the search to entries that must match two attributes. The user must be in the `EDI` department and in the `administrators` group.
`department=EDI,telephoneNumber=800*`	Limits search to EDI department members with a telephone number starting with `800`.
`objectclass=person`	Limit the search to entries that are people if the Base DN contains other entries (for example, computers) and people.

Search Filter	Description
`!(userAccountControl:1.2.840.113556.1.4.803:=2)`	Excludes disabled accounts - in Active Directory, if an account is disabled, bit `0x02` in the `userAccountControl` attribute value is on. `1.2.840.113556.1.4.803` is the rule object ID (ruleOID) for the LDAP bitwise `AND` operator.

If the value to search in has any of the following special characters, they must be substituted in the Search Filter with the corresponding escape sequence.

ASCII character	Escape Sequence Substitute
*	\2a
(	\28
)	\29
,	\2c
\	\5c
NUL	\00
/	\2f

Username Attribute

The **Username Attribute** is the directory attribute that matches the username entered when a login is required. The following table contains typical attribute names for the supported directory types.

Directory Type	Username Attribute
Active Directory	`sAMAccountName`
Apache Directory Services	`Uid`
Lotus Domino	`CN`
Novell eDirectory	`CN`
DirX	`cn`

LDAP Server Advanced Settings

The **LDAP Server Advanced Settings** dialog box displays when you click **Advanced** on the **LDAP Server** tab. Use this dialog box to specify values for password expiration checking.

Enable Password Expiration Checking

Select this check box to enable password expiration checking and the rest of the fields in the dialog box. Password expiration checking provides a daily email notification to the system administrator.

Warning Days Before Password Expiration

The range of days within which a notification is generated.

Daily Time Check

The time of day password expiration is checked.

To

The email address of the recipient of the daily password expiration check notification. You can specify multiple recipients. Separate email addresses by commas (,), semi-colons(;) or colons(:).

One or more individual users can also receive an email notification, if specified, when the **Security Mode** is not set to `None` and an email address is configured for the users (as part of his Active Directory settings). A Web Portal user whose password hasn't already expired is directed to the web link (see Providing access to the web portal on page 793) where they can change their password. Otherwise, they are directed to contact the system administrator for assistance in changing it.

Default value: The System Administrator email address defined in the **Options > Other** panel in the native UI or **Administration > System > Other** in the web UI.

From

The email address of the sender of the daily password expiration check notification. If this field contains multiple email addresses, only the first address is displayed.

Default value: The System Administrator email address defined in the **Options > Other** panel in the native UI or **Administration > System > Other** in the web UI.

Subject

String that appears in the Subject field of the daily password expiration check notification.

Cleo VLNavigator LDAP user configuration reference

Email Address Attribute

Required field. Attribute name for a user's email address.

Note: If you do not specify the **Email Address** attribute and you have LDAP users who try to reset a password via email, the Cleo Harmony application will not send password-reset emails.

Phone Attribute

First Name Attribute

Last Name Attribute

Full Name Attribute

Optional fields. Other options might depend on the values you specify for these fields.

User UID Attribute

Required field.

An additional distinguishing attribute in the user list.

LDAP Account for Extracting Users

Username

Password

Credentials used to login to extract LDAP user from the LDAP directory service to populate the optional default LDAP user group or when you browse for users on the **Cleo VLNavigator User** tab. In addition to the **List** button here and in each of the local user host mailbox LDAP tabs, this account is used to periodically extract users in order to check mailbox license limits and to create user subdirectories.

Create/Maintain Default LDAP Group

Select the check box to create the optional Default LDAP user group. Clear the check box to remove the Default LDAP user group. See Default LDAP group on page 691.

Default LDAP group

On the LDAP Server tab (see Users LDAP Server), when an LDAP directory service is configured, the optional **Username** and **Password** fields are specified, **Create/Maintain Default LDAP Group** is selected, and **Apply** is clicked, a special user group called **Default LDAP** will appear under the **Users** tree. The **Default LDAP** group is a convenience group, provided as an easy way to add many users at one time. The users within this group will correspond to those shown when **List** is clicked (not including any users that already exist within other VLNavigator user groups).

Once created, the Default LDAP group can be disabled, refreshed, or removed by right-clicking the user group within the tree pane and selecting **Disable**, **Refresh**, or **Remove**. If **Remove** is selected, **Create/Maintain Default LDAP Group** cleared for you and the group is removed. Another way to remove the **Default LDAP** group is to clear **Create/Maintain Default LDAP Group** and click **Apply**.

The users within the **Default LDAP** group cannot be edited or disabled; however, they can be moved to another user group by right-clicking on the user within the tree pane and selecting **Move**.

User Group Tab

See Create a User Group on page 919 for information about creating, renaming, disabling, or removing a user group.

VLNavigator User Group Tab

The **User Group** tab is displayed when you select a user group from the **Users** tree branch.

Select **User Group enabled** to allow users belonging to this group to log into the Cleo VLNavigator and Cleo Harmony applications.

Select **LDAP User Group** to enable the **LDAP** panel on the **User Group** tab and automatically populate the group with members of the LDAP service. Users are authenticated through the external directory server.

If necessary, select **Override System Options** to specify settings for **Base DN** and **Search Filter** (see Specifying default host directories on page 700 **Configure System Options: LDAP Server**) to match the intended set of users for this mailbox. Alternatively, the **Extend Search Filter** can be used to append rules to the default system search filter.

Use **List** to list the users and their attributes matching the Base DN and Search Filter.

User Group VLNavigator Privileges

Use the **VLNavigator Privileges** tab to specify which parts of the tree pane are visible to the user group.

There are three trees for which you can assign privileges for the user group: Systems, Users, and Applications. For each, you can select from the following privileges:

- **No access**: tree cannot be viewed.
- **View-only**: tree is viewable, but changes cannot be applied.
- **Editable**: tree is viewable and changes can be applied.

When you select **View-only** or **Editable** for any of the trees, you can apply the privilege to all items or a subset of the items in the tree. If the user group has at least one view-only or editable **VLNavigator** privilege, it is allowed to log into any Cleo VLNavigator instance installed within the configured VersaLexes.

Alternatively, you can control the items available for the user group on a per-tree basis using the **Systems tree branches accessible**, **Users tree branches accessible**, and **Applications tree branches accessible fields**.

User Group: System Privileges Tab

Use the **System Privileges** tab to control the system-level items to which a user group has access.

- Choose one of the following for each **System Privilege**:
  - **No access**: item cannot be viewed.
  - **View-only**: item is viewable, but changes cannot be applied.
  - **Editable**: item is viewable and changes can be applied.
- Additionally, a subset of the **System** privileges, if set to **View-only** or **Editable**, can also have **Stop/start** enabled; this indicates that a member of the user group is allowed to stop and start (that is, run) the item. Relative to the **System options** privilege, this indicates that a member of the user group is allowed to stop the Windows service or Unix daemon. Relative to the **Hosts** privilege, this indicates that a member of the user group is allowed to stop and start the actions within hosts.
- Host folder branches can be set to a semicolon-separated list of Cleo Harmony host folder names that are accessible by the user group. This setting affects which host folders are viewable both with the Cleo Harmony application. The `*` and `?` wildcard characters can be used. This setting has no affect on the root folder of the active host tree; it only impacts the subfolders. This setting also influences wherever active hosts are listed or referenced, including the scheduler, router, TCP/IP port usage report, transfer log report, system log, messages pane, etc. In general, if a host is not viewable, configuration and status information about the host is not available throughout the user interface.
- The property, `Accessing raw payload from transfer reports requires Host permissions` can be turned off to allow users with the ability to view transfer reports (but wihtout the aiblity to view hosts) to view or eamil raw payload.
- If the user group has at least one view-only or editable system privilege, it is allowed to log into the selected set of **VersaLex Pools** and individual instances of the Cleo Harmony application.

User Group File Transfer Report Tab

The following describes the **File Transfer Report** tab. The Cleo Harmony Transfer Report table columns, accessible file types, and accessible transaction types can be configured per user group. The Accessible File Types and accessible transactions take effect only on the VersaLexes that are licensed and configured to track specific **EDI**, **XML**, or **TEXT** document contents.

- A user group that is no longer **User Group enabled** cannot be used to log into either the Cleo VLNavigator or Cleo Harmony applications.
- Each item in the **Report Column** table can be shown in the Cleo Harmony Transfer Report table by enabling the **Report Column**. The **Custom Name** allows the user to configure custom column headers in the table. The **Up** and **Down** buttons are used to arrange the order of the enabled columns in the Transfer Report Table.
- The **Accessible File Types** configures which tracked file types (EDI, XML, or Text) can be accessed by users of this user group. If a user does not have access to this file type, then they will not be able to View or Email a copy of the file but they will be able to see the transfer occurred in the Cleo Harmony Transfer Report table.
- The **Transactions user group can/can NOT access** contains a table of all ASC X12, EDIFACT, and TRADACOMS transactions. If **can** is selected, then the selected items in the table specify which transactions types the user can access. If **can NOT** is selected, then the selected items in the table specify which transaction types the user cannot access. If a non-accessible transaction type is contained within a tracked file, then the entire file will not be accessible to the user. This means the user cannot View or Email a copy of the file. The **All** and **None** buttons are used to select or clear all of the EDI transaction types.

User Group Application Settings Tab

The following describes the **Application Settings** tab. Note that this tab will not be present unless a database is chosen (see Applications on page 660) and at least one application is enabled under the **Applications** tree branch.

The left pane shows the list of applications that can be enabled or disabled for this user group. This list includes those configured for the **Applications tree** privilege under the **VLNavigator Privileges** tab for this user group. See User Group VLNavigator Privileges on page 929.

- See Operator Audit Trail on page 933 for information about the Operator Audit Trail application.

To enable or disable a feature, click the feature in the left pane and then select or clear **Application enabled for User Group**. Alternatively, you can right-click on the feature and select **Enable** or **Disable**.

Cleo VLNavigator User Tab

See Add a User on page 920 for information about how to add, rename, move, disable or remove a user.

The following describes the **User** tab.

User enabled

Select this check box to enable the user. A user must be enabled to log into Cleo VLNavigator or Cleo Harmony applications.

LDAP User

Select this check box to use LDAP to authenticate this user. The LDAP directory service configured on the Users LDAP Server panel is used to authenticate LDAP users and to obtain the full names and email addresses. If you select this check box, the **Username**, **Password**, **Confirm Password**, **Full Name**, and **Email Address** fields are disabled.

When creating or modifying an LDAP user, click the **[...]** button to display a list of LDAP users within the configured directory, base DN, and search filter.

Note: If you have not specified the optional **Username** or **Password** within the LDAP Server tab, you will be asked to authenticate the first time you click the **[...]** button. You must enter a valid LDAP username and password to obtain the list.

Username

Password

These fields are required.

The value you specify in the **Username** field must be unique across all user groups. The **Password** can make use of any keyboard characters. When logging in, the **Username** and the **Password** are case sensitive.

When creating or modifying a non-LDAP user, you must use the **Username**, **Password** and **Confirm Password** fields.

Optional Alias

If you specify a value, the alias rather than the username is displayed in the Cleo VLNavigator tree.

Full Name

Email Address

The **Full Name** and **Email Address** fields are used by optional applications you configure on the Applications dialog box. See Applications on page 660).

The **Email Address** field is required.

Applications

The **Applications** tree branch contains information about the configurable applications. The applications listed under this branch include those configured for the Applications tree privilege under the **VLNavigator Privileges** tab for the user group associated with the current user. See User Group Tab on page 929.

When you select the **Applications** tree branch, the **Settings** tab appears.

The **Database** drop-down displays the list of databases that have been configured. See Databases on page 722. For any of the applications to be operational, a database must be configured. When the **Database** selection is cleared, the Application Settings dialog box appears, informing you that the applications will be disabled.

Test Database Connection can be used to test the connection to database. After the connection is tested, success or failure conditions will be reported.

Export Database Definition can be used to export the SQL statements that VLNavigator uses to create the database tables relative to the VLNavigator operations.

The exported file will contain the following types of DDL statements: CREATE TABLE, ALTER TABLE, and CREATE INDEX. These statements can be modified (e.g., to use a specific table space), but the table and column names must be unaltered. The modified script can then be used to create a modified database; however, if VLNavigator has already created the tables, DROP statements will need to be added to the beginning of the script.

After selecting the desired database and testing the connection, click **Apply**.

Dashboards

The Cleo Dashboards web application provides views of trading relationships from the perspective of a business user, including:

- Tracking of document exchanges per trading partner
- Review of service level agreements (SLA) and key performance indicators (KPI)
- Supplementary and customized reports catered for specific business use cases (for example, EDI transactional report)

Prerequisites for the Cleo Dashboards application include:

- The **Dashboards** resource path enabled within the Cleo Harmony application.
- A separate report server installed and its location configured within the Cleo Harmony application. The same report server instance can be employed for both the Cleo Dashboards and Cleo System Monitor applications.
- Both prerequisites are configured in the Cleo Harmony Local Listener Web Browser Service: **Dashboards/ Monitor** tab. See Configuring Dashboards and System Monitor for web browser service on page 794.

Configure your dashboards

The database first needs to be configured in the **Applications > Settings** tab. See Applications on page 660. Once the database has been successfully configured, the application is enabled by selecting **Dashboards** under **Applications** in the tree pane and selecting **Application enabled** in the **Settings** tab.

Note: Once the application is enabled, you must restart the Cleo Harmony or Cleo VLTrader service/daemon before you use Cleo Dashboards.

Once enabled, general access to **Dashboards** is granted in the **User Group: Application Settings Tab**. See User Group Application Settings Tab on page 930. Once general access is granted, additional user group configuration is allowed, as described below.

Note: The user group configuration panels below refer to reports and components. The initial, default published reports provided by Cleo are all dashboards (.dsh files) that are comprised of library components (.lc files) that link to web reports (.wls files).

The **Privileges** sub-tab identifies access and update privileges at the public, custom, and private levels:

- **Public**: Standard reports/components provided by Cleo deployment
- **Custom**: Customized reports/components optionally available to other users and user groups

- **Private**: Customized reports/components only available to that user

User groups will always have read-only access to the public **Dashboards** area and read-write access to their private **Dashboards** area. Optionally, a user group can be granted read-only or read-write access to the custom **Dashboards** reports/components area. With this method, Cleo's standard reports/components are always available, and any customizations to Cleo's standard reports/components can be either kept private or shared with other users.

The **Reports** sub-tab identifies which reports are initially shown when the user first opens the **Dashboards** web application.

The report sequence defaults to the Cleo-provided standard **Public** reports.

1. Use the right-click menu options in the table to **Move Up** or **Move Down** the sequence of a report in the list or to **Remove** a report from the list (this only removes the report from this display list; the report itself still exists).
2. Click **Add** to insert a **Public** or **Custom** report to the end of the list.
3. Click **Reset Defaults** to revert the list back to the standard Cleo-provided **Public** reports.
4. Click **Delete Report File** to permanently remove a **Custom** report from the report server.

The report sequence configured at the user group level can be overridden at the user level. If **Override User Group settings** is selected for a user, the same **Reports** sub-tab as above is enabled for the user and operates in a similar fashion:

1. Use the right-click menu options in the table to **Move Up** or **Move Down** the sequence of a report in the list or to **Remove** a report from the list (this only removes the report from this display list; the report itself still exists).
2. Click **Add** to insert a **Public** or **Custom** or **Private** report to the end of the list.
3. Click **Reset Defaults** to revert the list back to the standard Cleo-provided **Public** reports.
4. Click **Delete Report File** to permanently remove a **Private** report from the report server.

Operator Audit Trail

The **Operator Audit Trail** application keeps a record of updates made by users using the Cleo Harmony and Cleo VLNavigator user interfaces. You can view, save, and print reports based on these records.

Configuring Operator Audit Trail

Before you can configure any applications, including the Operator Audit Trail, you must have a database configured for the Cleo VLNavigator software to use. See Applications on page 660.

1. In the Cleo VLNavigator tree pane, select **Operator Audit Trail** under **Applications**.

   The **Settings** tab appears.
2. On the **Settings** tab, select the **Application enabled** check box.
3. Optional - configure the application to purge old events automatically. On the Settings tab, select the **Automatically purge Operator Audit Trail events after # days** and enter the number of days.

   Events older that the number of days you specify are deleted from the database.
4. Click **Apply** to save your configuration.

Once you have enabled the **Operator Audit Trail** application, any user updates made using the Cleo Harmony and Cleo VLNavigator user interfaces are logged to the database for all users.

In addition to the **Application** settings, there are **User Group Application** settings, where you can enable or disable the application for an entire user group. If disabled for a user group, the audit trail will still be logged for these users, but they will not be able to view the audit trail.

Viewing the Operator Audit Trail

Use the Cleo VLNavigator application to view the **Operator Audit Trail**. For information about the report itself, see About the Operator Audit Trail Report on page 935.

1. In the tree pane, right-click the **Users** folder, a specific **User Group** folder or a specific **User**.

   For a **Users** folder, the audit trail includes the audit events for all users in the user groups to which the logged-in user has access. For the Administrator users, this will always include all users.

   For a specific **User Group** folder, the audit trail includes the audit events for all users in the selected user groups.

   For a specific **User**, the audit trail includes the audit events only for the selected user. You can select multiple users from a single user group and display the audit trail for those users.
2. Select **View Operator Audit Trail** from the drop-down menu.

   The **Operator Audit Trail Report Filter** dialog box appears.
3. Optional - Specify filter criteria. See Filtering the Operator Audit Trail on page 934.
4. Click **Generate** to display the report.

   The **Operator Audit Trail Report** appears.
5. Optional - Click **Filter** after you generate the report to filter the report again.
6.

Filtering the Operator Audit Trail

The **Operator Audit Trail Report Filter** dialog box is displayed when you select the **View Operator Audit Trail** option for all users, a User Group or a specific User. Use the **Operator Audit Trail Report Filter** dialog box to filter the report based on a time period and other criteria you specify.

1. Optional - Click **Open** to read a set of previously saved filter criteria into the fields in the dialog box.
2. Specify a time period for which you want to see audit trail data.

   Use the **From** and **To** fields to specify starting and ending times for the reporting period.
3. Select other criteria from the following tabs.
   a) Use the **Hosts/Mailboxes** tab to select hosts and mailboxes for which you want to see audit trail events that have been logged. The **Include Folder(s)** list controls what is displayed in the **Include Host(s)\Mailbox(es)** list. The **Include Host(s)\Mailbox(es)** list also contains a **Show Mailboxes** option. If selected, the list displays down to the mailbox level. If cleared, it only displays hosts.
   b) Use the **Service/Config/Misc** tab to select services, configurations, and other miscellaneous items for which you want to see audit trail events. The **Services** list contains system-level runnable items. The **Configurations** list contains system-level configuration items. The **Misc Items** list contains other miscellaneous items that do not fall into the other categories.
   c) Use the **Event** tab to select events for which you want to see audit trail information. The **Event Types** list contains all the different event types saved. **CA Cert Events** and **User Cert Events** are special in that they are a series of events themselves.
   d) Use the **Systems** tab to select pools and instances of VersaLex for which you want to see audit trail information. Only the pools configured in the Cleo VLNavigator application are available from this list.
4. Use the **Sort By** field to specify the initial sort for the report.

   Choose from the following:

   - **Date/Time only**
   - **Item Name**
   - **Username then Item Name**
   - **Username**

All but the first sort options listed also sort by date/time when the other criteria match.

5. Optional - Click **Save As** to save your filter criteria as an XML file. Click **Close** to close the dialog box without saving.
6. Optional - **Open** allows the user to read a previously saved Filter into the panel. **Save As** saves the current filter to an XML file. This file can either be used with **Open** or as input to the command line reporting. **Generate** generates the report and displays the report screen. **Close** closes the filter dialog box. **Help** displays the part of the user manual associated with the filter dialog.

About the Operator Audit Trail Report

The Operator Audit Trail Report displays a sorted table based on the criteria selected in the filter. You can sort the table based on any column by clicking on the column header. Clicking on the column header that already contains the sorting arrow will reverse the order from ascending to descending (or vice versa).

Report content

The report contains the following information for each event.

Date/Time

The date and time of the operator event.

Computer Name

The name of the computer where the user interface is active. In the case of a Web-based UI, the IP address is shown in this column.

Serial Number

The serial number of the Cleo Harmony software on which the modification occurred.

Username

The name of the logged-in user.

Item Type

Item Name

Information regarding the item with which this event is associated. You specify the items included in the report using filter criteria. See Filtering the Operator Audit Trail on page 934.

Commands

The command buttons at the bottom of the panel allow various actions on the data.

Filter

Displays the **Operator Audit Trail Report Filter** dialog box allowing you to change filter criteria.

Refresh

Refreshes the data based on the filter to display any new events.

Save as CSV

Opens a dialog box in which you can select a file location and file name to store a .CSV file of the data in the table.

Generate HTML Report

Displays the filter dialog box again. Update the filter if necessary and select **Generate** to display an HTML version of the file. While the HTML version of the file is displayed, you can click **Save As** to save the HTML file.

Drilling down into report data

Once you have generated a report, you can drill down into the report data. Double-click a row or right-click a row and select **View** from the menu to display information from that row in a separate dialog box. If there is any addition information stored about the event in this row, it is also displayed in the dialog box. You can also print the data in the dialog box using **Print** or use **Close** to dismiss the dialog box.

Cleo VLNavigator System Monitor

The **System Monitor** web application provides views of system status and health from the perspective of a system operator, including:

- Cleo Harmony and Cleo VLProxy resource, service, and queue usage
- Active solicited and unsolicited sessions
- Active UI sessions

Prerequisites for the Cleo System Monitor application include:

- The System Monitor resource path enabled within the Cleo Harmony application
- A separate report server installed and its location configured within the Cleo Harmony application; the same report server instance can be employed for both the **Dashboards** and **System Monitor** applications

Both prerequisites are configured in the Cleo Harmony **Local Listener Web Browser Service: Dashboards/Monitor** tab. See Configuring Dashboards and System Monitor for web browser service on page 794.

Configuring VLNavigator System Monitor

Before you can configure any applications, including the System Monitor, you must have a database configured for the Cleo VLNavigator software to use. See Applications on page 660.

Note: Once the application is enabled, you must restart the Cleo Harmony or Cleo VLTrader service/daemon before you use Cleo System Monitor.

1. In the Cleo VLNavigator tree pane, select **System Monitor** under **Applications**.

   The **Settings** tab appears.
2. On the **Settings** tab, select the **Application enabled** check box and click **Apply**.
3. Restart the Cleo Harmony or Cleo VLTrader service/daemon.
4. Grant access to the System Monitor. Click the user group to which you want to grant access and then click the **Applications Settings** tab. See User Group Application Settings Tab on page 930.
5. In the **Application Settings** tab, click **System Monitor** and then click the **Application Enabled for User Group** check box.

   The **Privileges** and **Reports** tabs are enabled for the user group.
6. Select the options you want for the user group.
   - The **Privileges** sub-tab allows you to specify access and update system monitor privileges at the public, custom, and private levels.
     - **Public**: Standard reports/components provided by Cleo deployments
     - **Custom**: Customized reports/components optionally available to other users and user groups
     - **Private**: Customized reports/components only available to that user
   - The **Reports** sub-tab identifies the reports initially shown when the user first opens the **System Monitor** web application.

The report sequence defaults to the Cleo-provided standard **Public** reports. The initial default published reports provided by Cleo are all dashboards (`.dsh` files), which are comprised of library components (`.lc` files) that link to web reports (`.wls` files).

User groups will always have read-only access to the public **System Monitor** area and read-write access to their private **System Monitor** area. Optionally, you can grant a user group read-only or read-write access to the custom **System Monitor** reports/components area. This means Cleo's standard reports and components are always available, and any customizations to Cleo's standard reports and components are either kept private or shared with other users.

a. Use the right-click menu options in the table to **Move Up** or **Move Down** the sequence of a report in the list or to **Remove** a report from the list (this only removes the report from this display list; the report itself still exists).
b. Click **Add** to insert a **Public** or **Custom** report to the end of the list.
c. Click **Reset Defaults** to revert the list back to the standard Cleo-provided **Public** reports.
d. Click **Delete Report File** to permanently remove a **Custom** report from the report server.

7. Optional - Override user group report sequence for individual users.

a) Select an individual user from a user group and then select the **Applications Settings** tab.
b) On the **Application Settings** tab, select the **Override User Group settings** check box.

1. Use the right-click menu options in the table to **Move Up** or **Move Down** the sequence of a report in the list or to **Remove** a report from the list (this only removes the report from this display list; the report itself still exists).
2. Click **Add** to insert a **Public**, **Custom**, or **Private** report to the end of the list.
3. Click **Reset Defaults** to revert the list back to the standard Cleo-provided **Public** reports.
4. Click **Delete Report File** to permanently remove a **Private** report from the report server.

The report sequence configured at the user group level can be overridden at the user level. If **Override User Group Settings** is selected for a user, the same **Reports** sub-tab as above is enabled for the user and operates in a similar fashion.

a. Use the right-click menu options in the table to **Move Up** or **Move Down** the sequence of a report in the list or to **Remove** a report from the list (this only removes the report from this display list; the report itself still exists).
b. Click **Add** to insert a **Public**, **Custom**, or **Private** report to the end of the list.
c. Click **Reset Defaults** to revert the list back to the standard Cleo-provided **Public** reports.
d. Click **Delete Report File** to permanently remove a **Private** report from the report server.

The Reports sub-tab allows you to

Configure Cleo Unify

Before you can use Cleo Unify, you must enable it and specify some basic configuration values.

1. If necessary, start the Cleo VLNavigator application.
2. Go to **Applications > Unify**.

Note: If the **Unify** option is not available, it could mean Cleo Unify is not correctly installed. Contact your system administrator.

3. In the **Settings** tab, select the **Application enabled** check box.
4. Specify values for the following fields:

- **Primary file repository** and **Maximum size** – a local directory where files you upload to Cleo Unify will be stored. Maximum size is a limit on the size of the directory, not any one file. You must specify values for these fields.
- **Overflow file repository** and **Maximum size** – a local directory where uploaded files that do not fit in the **Primary file repository** are stored. Maximum size is a limit on the size of the directory, not any one file. These fields are optional.
- **From email address for user notifications** – the email address Cleo Unify will use to send notification email to users.
- **Permanently remove trash after *n* day(s)** – the number of days after which Cleo Unify will permanently delete any files you delete from a Cleo Unify folder.

  CAUTION: When you delete a file from a Cleo Unify folder, it is not immediately removed from your system. It remains in the **Primary file repository** folder until the number of days you specify elapse. Specifying a large number of days could cause you to exceed the maximum size for your folder with no recourse except to wait for the number of days to elapse.

5. Click the **User Groups** tab.

   The **User Groups** tab provides a list of user groups who have access the Cleo Unify application. See User Group Tab on page 929 for information about user groups.
6. Select the user groups that should have access to the application and deselect those user groups that should not have access.
7. Click **Apply**.

Configure Cleo Trust

Before you can use Cleo Trust, you must enable it and specify some basic configuration values.

1. If necessary, start the Cleo VLNavigator application.
2. Go to **Applications > Unify**.

   Note: If the **Unify** option is not available, it could mean Cleo Trust is not correctly installed. Contact your system administrator.
3. In the **Settings** tab, select the **Application enabled** check box.
4. Specify values for the following fields:

   - **Primary file repository** and **Maximum size** – a local directory where files you upload to Cleo Trust will be stored. Maximum size is a limit on the size of the directory, not any one file. You must specify values for these fields.
   - **Overflow file repository** and **Maximum size** – a local directory where uploaded files that do not fit in the **Primary file repository** are stored. Maximum size is a limit on the size of the directory, not any one file. These fields are optional.
   - **From email address for user notifications** – the email address Cleo Trust will use to send notification email to users. You must specify a value for this field.
   - **Permanently remove trash after *n* day(s)** – the number of days after which Cleo Trust will permanently delete any files you delete from a Cleo Trust folder.

     CAUTION: When you delete a file from a Cleo Trust folder, it is not immediately removed from your system. It remains in the **Primary file repository** folder until the number of days you specify elapse. Specifying a large number of days could cause you to exceed the maximum size for your folder with no recourse except to wait for the number of days to elapse.
5. Click the **User Groups** tab.

The **User Groups** tab provides a list of user groups who have access the Cleo Trust application. See User Group Tab on page 929 for information about user groups.

6. Select the user groups that should have access to the application and deselect those user groups that should not have access.
7. Click **Apply**.

Appendix

A

REST API

With release 5.3, you can access Cleo Harmony or Cleo VLTrader functionality through a REST API, allowing easy integration with provisioning and operational systems regardless of implementation language or topology.

For more information, visit http://developer.cleo.com.

Appendix

B

Extended Commands

This section contains a detailed discussion of some of the extended commands that are available to Cleo Harmony application users.

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

- CHECK command on page 943
- SCRIPT command on page 951

CHECK command

Note: The `CHECK` command is only available in the Cleo Harmony and Cleo VLTrader applications.

There are times when you might need to track certain events or non-events. In some cases, these requirements might come from Service Level Agreements (SLAs) that you have with your trading partners, where a given delivery performance is part of the contract. In other cases, you might want to trigger another event. In the context of the Cleo Harmony or Cleo VLTrader system, this relates to the presence and movement of files and directories. The Cleo Harmony or Cleo VLTrader file/directory/transfer checking feature accommodates this capability through the `CHECK` command.

The `CHECK` command provides a way for you to check whether certain internal or external file movement has occurred within expected time periods and within given optional criteria. For example, you can check for the following conditions:

- if an expected inbound transfer has occurred within a specified period
- if an expected outbound transfer has not occurred within a specified period
- if a file is older than a specified age
- if a directory is not older than a specified age

If the `CHECK` conditions are met, you can use the `Execute On Check Conditions Met` property to trigger subsequent events or you can use the `Email On Check Conditions Met` to send email to key personnel. Conversely, if the `CHECK` conditions are not met, you can use the `Execute/Email On Check Conditions Not Met` properties. Note that there are no inherent pass/fail or success/error assumptions within the `CHECK` command. You have complete flexibility to specify the conditions for which you are looking; and, when the those conditions are met or not met, you can decide what action to take.

Related information

CHECK command advanced properties on page 944
CHECK command dialog on page 944
CHECK command parameters on page 945
CHECK command search scope on page 949
CHECK command reference on page 950

CHECK command advanced properties

The following properties are specific to the CHECK command. See Setting advanced host properties on page 89 for a description of these properties.

- Email On Check Conditions Met
- Email On Check Conditions Not Met
- Execute On Check Conditions Met
- Execute On Check Conditions Not Met

Note:

1. For the Execute On Check Conditions Met property, if multiple files contribute to the conditions being met, and one of the following file macros is in the system command, the command will be executed repeatedly—once for each file.
   - %file%
   - %sourcefile%/%srcfile%
   - %sourcefilebase%/%srcfilebase%
   - %sourcefileext%/%sourcefileext%
   - %destfile%
   - %destfilebase%
   - %destfileext%
   - %filesize%
2. The macros listed above are not available to Execute On Check Conditions Not Met.

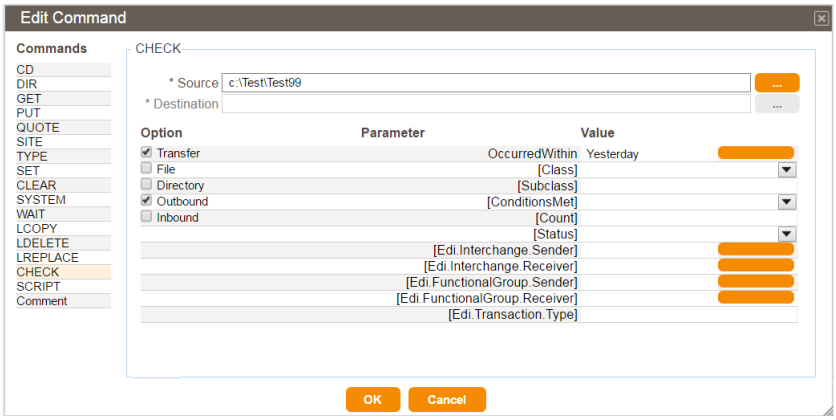
See Using Macro Variable (Execute-On context).

CHECK command dialog

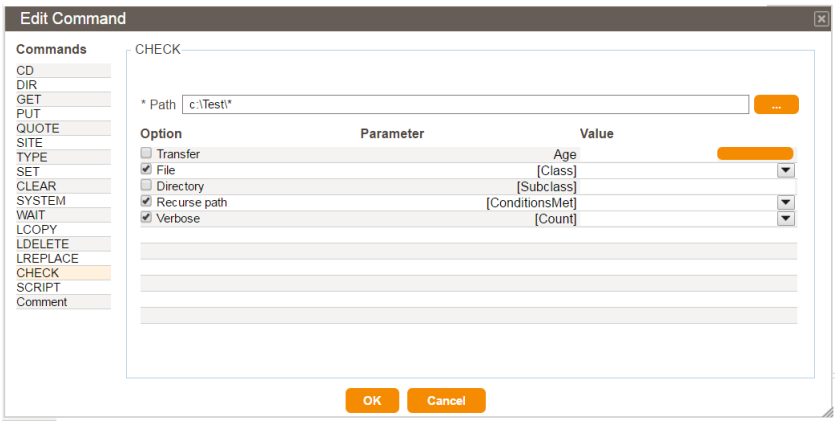
The **Edit Command** dialog box for the CHECK command is very similar to other command dialogs. However, because of its complexity, additional wizard dialogs are provided to aid in building a CHECK command. See also Compose an Action and Composing a host action on page 91

The CHECK command dialog box provides access to the many **Option** and **Parameter** settings available. They can be very powerful and can provide you with great flexibility in building your checks. For information about the **Option** settings, seeCHECK command reference on page 950. For information about **Parameter** settings, see CHECK command parameters on page 945. For all parameters, if you mouse-over the associated **Value** cell, you will receive a brief tool-tip help message regarding the parameter.

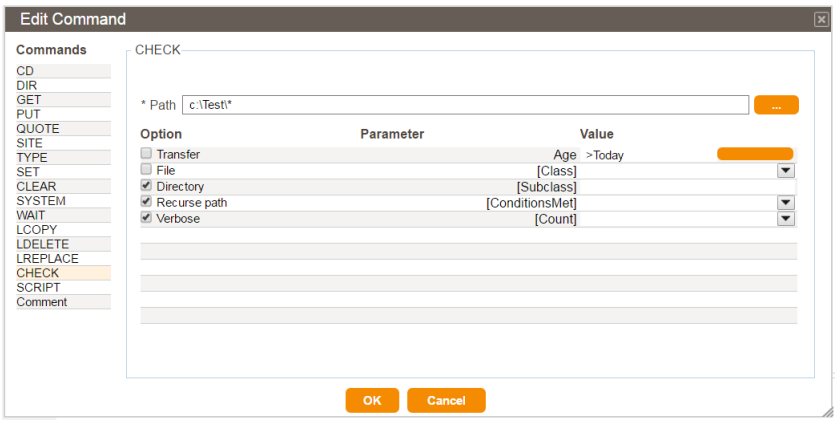
CHECK -TRA (transfer):



`CHECK -FIL` (file):



`CHECK -DIR` (directory):



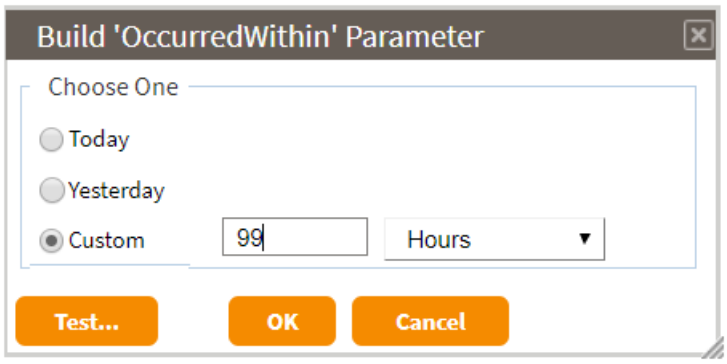
CHECK command parameters

OccurredWithin

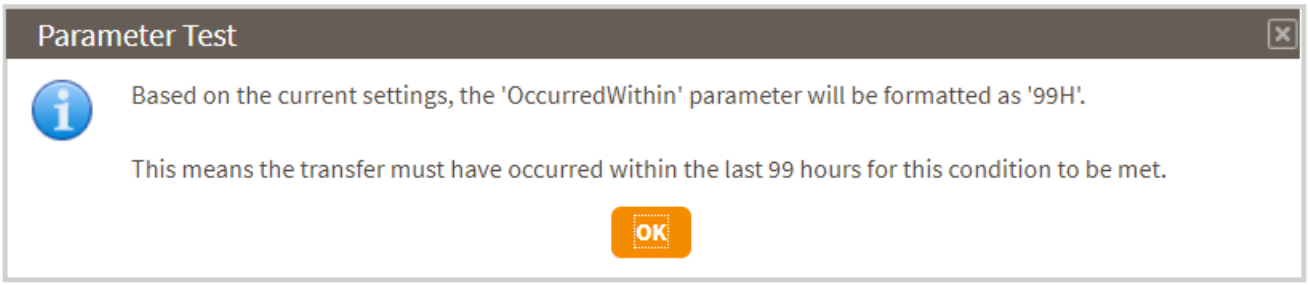
Required for the transfer (`-TRA`) option. Indicates the time period in which the transfer for which you want to check should have occurred. The value or `OccurredWithin` can either be expressed explicitly as "*nn*`[D|H|`

M|S], where *nn* is a number from 1-99 and the letter following indicates days, hours, minutes, or seconds; or it can be the keyword "Yesterday" or "Today".

To enter this parameter, either type the string in directly or click on the cell to show the [Build...] button. The [Build...] button, if selected, will display the following wizard dialog that can be used to build the 'OccurredWithin' parameter.



- Select 'Today', 'Yesterday', or 'Custom'. If 'Custom' is specified, then enter a value between 1 and 99 and a unit (e.g., '99 Hours' as shown above).
- To obtain a written translation of your settings, click on the [Test...] button. You will receive a dialog such as follows.



- Once you are satisfied with your settings, click the [OK] button.

Age

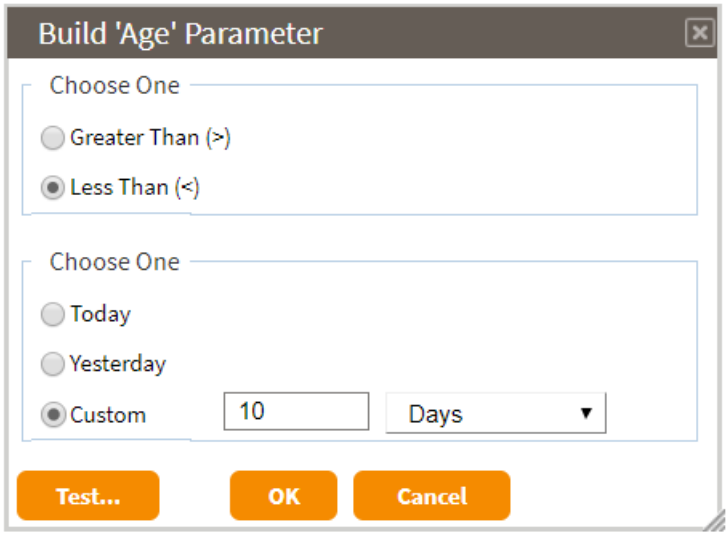
This parameter is required for the file (-FIL) and directory (-DIR) options. It specifies the age condition for which the files/directories should be checked. The value of Age may be of the form "[<|>]*nnn*[D|H|M|S]" where *nnn* is a number from 0-999 and the letter following indicates days, hours, minutes, or seconds. The "<" or ">" symbol must be present to indicate whether the check is looking for ages greater than or equal to, or less than or equal to, the specified age. For example, "Age=>24H" indicates the check should look for files/directories equal to or older than 24 hours. The value of Age can also be "[<|>]Yesterday" or "[<|>]Today".

Notes:

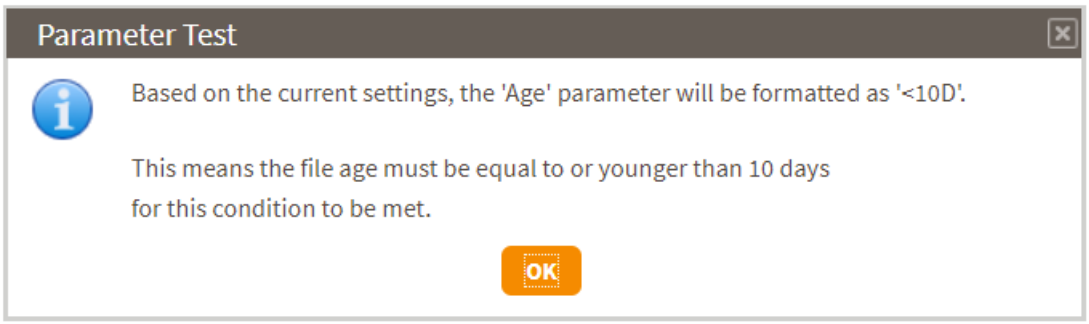
1. To simply check for existence of a file/directory, use a parameter setting of ">0[D|H|M|S]". (It does not matter which unit is selected in this case.)

2. A parameter setting of "<0[D|H|M|S]", is really nonsensical because it is essentially looking for files/directories with future ages. This setting will be flagged as an error.

To enter this parameter, either type the string in directly or click on the cell to show the [Build...] button. The [Build...] button, if selected, will display the following wizard dialog that can be used to build the 'Age' parameter.



- Select 'Greater Than (>)' or 'Less Than (<)'.
- Select 'Today', 'Yesterday', or 'Custom'. If 'Custom' is specified, then enter a value between 0 and 999 and a unit (e.g., '10 Days' as shown above).
- To obtain a written translation of your settings, click on the [Test...] button. You will receive a dialog such as follows.



- Once you are satisfied with your settings, click the [OK] button.

Class

Subclass

These parameters, if specified, are for categorizing the result of the CHECK command (what is referred to as a "checkpoint") within the Dashboards application SLA/KPI report.

- **Class –** there are two settings for this parameter:
  - **SLA** (Service Level Agreement) – verification of internal or external customer commitments
  - **KPI** (Key Performance Indicator) – measurement for self-policing/self-improvement
- **Subclass** – this parameter is freeform and can be set to any value that has meaning within the business use case.

ConditionsMet

This parameter, if specified, signals that records should be added to the transfer log when the CHECK command is executed (see Transfer Entries for CHECK Commands). Further, this parameter indicates how to classify the result when the conditions are met. There are two settings for this parameter:

- **Error** - if the conditions of the CHECK are met, then the result should be classified as "Error". If the conditions of the CHECK are not met, then the result should be classified as "Success".
- **Success** - if the conditions of the CHECK are met, then the result should be classified as "Success". If the conditions of the CHECK are not met, then the result should be classified as "Error".

Note that the Advanced property, 'Terminate On Fail', is only honored if this parameter is set and the result of running the CHECK is classified as "Error". See Set Advanced Host Properties for a description of 'Terminate On Fail'.

To enter this parameter, either type the string in directly or click on the cell to show a drop-down list containing available options from which you can select. If [ConditionsMet] is not specified, then the result will always be classified as "None", irrespective of whether the conditions were met or not. Also, the CHECK operation will not be added to the transfer log.

Status

This parameter is only applicable to the transfer (-TRA) option. When checking for a transfer, it's possible to qualify the status of the transfer. There are three settings for this parameter:

- **Delivered** - this term applies to transfer statuses of 'Success', 'Warning', and 'Receipt Pending'. Although rarely seen, the 'Delete Error' and 'Delete Resolved' statuses are also included in this category.
- **Completed** - this term applies to transfer statuses of 'Success', and 'Warning'. Although rarely seen, the 'Delete Error' and 'Delete Resolved' statuses are also included in this category.
- **Any** this term applies to any transfer status, including 'Error', 'Exception', and 'Interrupted'.

To enter this parameter, either type the string in directly or click on the cell to show a drop-down list containing available options from which you can select. If [Status] is not specified, the default status is **Delivered**.

Count

This parameter is applicable to all options (-TRA, -FIL, and -DIR). For -TRA, it indicates the minimum number of transfers records found that meet the CHECK conditions. Its value should be a number from 1-99999. For the -FIL and -DIR options, [Count] can either be the keyword, "All", or a number from 1-99999. If a number is specified, it indicates the minimum number of files/directories that should meet the CHECK conditions. If "All" is specified, it indicates that all files/directories *that are found* according to the path specification must meet the age criteria. This implies that if no files/directories are found according to the path, the conditions will also be met.

To enter this parameter, either type the string in directly or click on the cell to show a drop-down list containing available options from which you can select (the drop-down list is only available for -FIL/-DIR operations). If [Count] is not specified, the default value is one (1).

Edi....

The [Edi....] parameters are only applicable to the transfer (-TRA) option and only when database transfer logging is enabled. They indicate additional (EDI) conditions that must be met for a particular transfer record. For the 'Edi.Interchange.Sender' and 'Edi.FunctionalGroup.Sender' parameters, the syntax is "EDI Sender:Qualifier", where Qualifier is optional. For the 'Edi.Interchange.Receiver' and 'Edi.FunctionalGroup.Receiver' parameters, the syntax is "EDI Receiver:Qualifier", where Qualifier is optional. For the 'EDI.Transaction.Type' parameter, multiple transaction types may be entered, separated by a semicolon (';') or comma (',').

If any of the [EDI...] parameters contain embedded spaces, the Edit Command dialog will automatically replace these with '\s'. Note that if you are keying the command in directly from the freeform editor on the Commands tab, you will be responsible for inserting '\s' for every embedded space. In general, when typing commands without the use of the Edit Command dialog editor, special escape sequences must be used to identify certain characters:

\s = space character

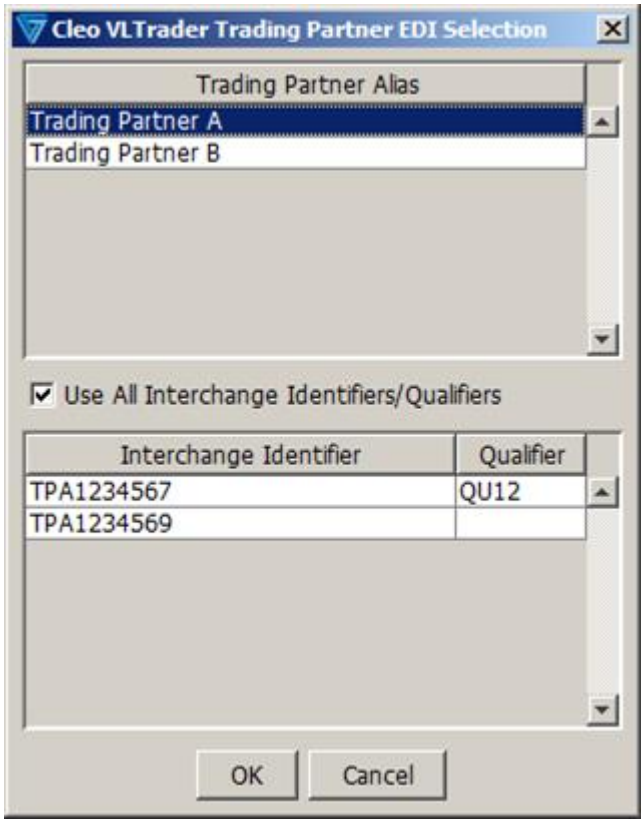
\t = tab character

\n = newline character

\r = carriage return character

\\ = slash character

To enter these parameters, either type the string in directly or, for the 'Edi…Sender' / 'Edi…Receiver' parameters, click on the cell to show the [Build...] button. The [Build...] button, if selected, will display the following wizard dialog that can be used to build the 'Edi…Sender' / 'Edi…Receiver' parameters.



If a Trading Partner Alias is selected along with '**Use All Interchange Identifiers/Qualifiers**', then a trading partner alias variable will be used. This will match any of the Interchange Identifiers/Qualifiers configured for the Trading Partner. If '**Use All Interchange Identifiers/Qualifiers**' is not selected, then the user can select a specific Interchange Identifier/Qualifier pair to be used. Once the selections have been made and the [OK] button is selected, then the selection will be placed in the appropriate field depending on which [Build…] button was selected.

CHECK command search scope

The `CHECK -TRA` command is available within any host, including the local user and local commands hosts. When run, its scope of search is determined by the host\mailbox from which it is run. For example, a `CHECK -TRA` command run from a mailbox-based action within '`Looptest FTP\myMailbox`' will search for transfers occurring within host, 'Looptest FTP', and mailbox, 'myMailbox'. Likewise, a `CHECK -TRA` command run from a host-based action within '`Looptest FTP`' will search for transfers occurring within *any* mailbox of host, '`Looptest FTP`'.

The CHECK -FIL or CHECK -DIR commands are also available in any host, including local user and local commands hosts. However, CHECK -FIL/-DIR commands are not tied to any specific host or mailbox. They may check for any file or directory within the file system.

CHECK command reference

Check to see if a transfer has occurred within a given specification, or check the age of file or directory.

```
CHECK -TRA|-FIL|-DIR  -IN|-OUT  -VER -REC "source" | "destination" | "path"
                    OccurredWithin= | Age=
                    [Class]=SLA|KPI
                    [Subclass]=
                    [ConditionsMet]=
                    [Status]=
                    [Count]=
                    [Edi.Interchange.Sender]=
                    [Edi.Interchange.Receiver]=
                    [Edi.FunctionalGroup.Sender]=
                    [Edi.FunctionalGroup.Receiver]=
                    [Edi.Transaction.Type]=
```

-TRA

Check that a transfer has occurred.

Requires the OccurredWithin parameter. See CHECK command parameters on page 945.

-FIL

Check a file age or existence.

Requires the Age parameter. See CHECK command parameters on page 945.

-DIR

Check a directory age or existence.

Requires the Age parameter. See CHECK command parameters on page 945.

-IN

Check an inbound transfer. This option is only applicable to CHECK -TRA operations.

-OUT

Check an outbound transfer. This option is only applicable to CHECK -TRA operations.

-VER

This option is only applicable to CHECK -FIL and CHECK -DIR operations. In addition to logging FILE elements for files/directories that meet CHECK -FIL/-DIR requirements, also log informational FILE elements for those files that match the path but do not meet the other requirements, for example, age.

-REC

Recursively search all subdirectories. This option is only applicable to CHECK -FIL/-DIR operations. Note that it is the last path token (file or directory) that is searched for in recursive operations.

"source"

Local source path for an outbound (-OUT) transfer check.

- The path can be to a filename or to a directory.
- * and ?, or a regular expression, are supported in filename, as well as each level of the path. See Using wildcards and regular expressions on page 69 for additional information. Wildcards are only available on the CHECK command.

- The final token of the path should be explicitly specified, either as a specific name or a wildcard/regular expression.
- If you specify a relative path, it uses the default outbox for remote hosts and the user home directory for local user mailbox-based actions. For local user host-based actions, the default root directory is used.
- Macro variables are supported. See Using Macro Variables (Source File context) for a list of the applicable macros.

"*destination*"

Local destination path for an inbound (`-IN`) transfer check.

- The path can be to a filename or to a directory.
- `*` and `?`, or a regular expression, are supported in filename, as well as each level of the path. See Using wildcards and regular expressions on page 69 for additional information. Wildcards are only available on the `CHECK` command.
- The final token of the path should be explicitly specified, either as a specific name or a wildcard/regular expression.
- If you specify a relative path, it uses the default inbox for remote hosts and the user home directory for local user mailbox-based actions. For local user host-based actions, the default root directory is used.
- Macro variables are supported. See Using Macro Variables (Destination File context) for a list of the applicable macros.

If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

"*path*"

Local path for a file/directory check.

- The path can be to a filename or to a directory.
- `*` and `?`, or a regular expression, are supported in filename, as well as each level of the path. See Using wildcards and regular expressions on page 69 for additional information. Wildcards are only available on the `CHECK` command.
- The final token of the path should be explicitly specified, either as a specific name or a wildcard/regular expression. When a file (`-FIL`) path ends with `/` or `\`, a `*` is automatically added to the path.
- If you specify a relative path, it uses the default inbox for remote hosts and the user home directory for local user mailbox-based actions. For local user host-based actions, the default root directory is used.
- Macro variables are supported. See Using Macro Variables (Source File context) for a list of the applicable macros.

If the path contains a space, dash (-), comma (,), or equal sign (=), it must be enclosed with double quotes ("...").

SCRIPT command

Note: The `SCRIPT` command is only available in the Cleo Harmony and Cleo VLTrader software.

The `SCRIPT` command is available to all protocols for executing JavaScripts within an action. The `SCRIPT` command is similar to the existing `SYSTEM` command and shares the same macro values. The `SCRIPT` command (along with other select action commands, e.g. `LCOPY`) is available for use with existing ExecuteOn functionality if preceded by a `$` (for example, `$SCRIPT`).

JavaScript files (normally `.js` extension) will be compiled into Java classes as needed. A file's last modified time will be used for indicating the file has changed and needs to be recompiled. The Cleo Harmony application uses Rhino (http://www.mozilla.org/rhino), which is an open source, pure Java, JavaScript engine to interpret

and compile JavaScript source files into Java classes for execution. See https://developer.mozilla.org/en/Rhino_JavaScript_Compiler.

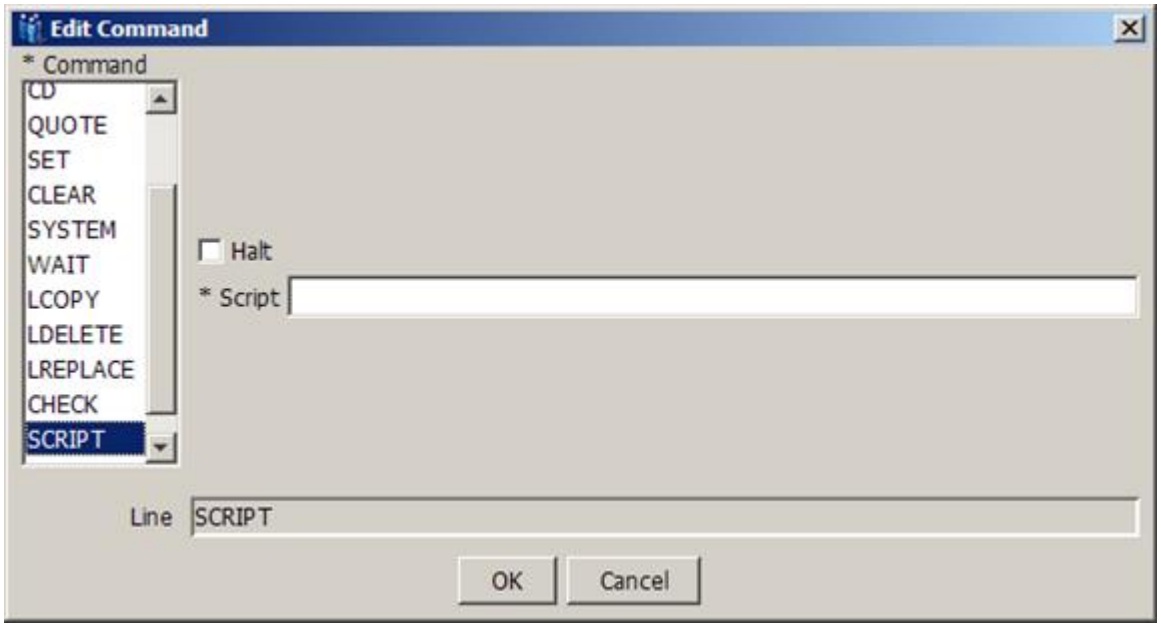
Refer to the API javadocs for examples and a description of the methods and functions available from within JavaScript (refer specifically to the ISessionScript class javadoc). The methods include the ability to run other action commands within JavaScript and writing to debug or the system log. These methods, when combined with JavaScript, make it possible to have complex sequences or decisions that would not be possible using action commands alone.

Related information

SCRIPT command reference on page 952
SCRIPT command dialog on page 952

SCRIPT command dialog

The Edit Command dialog for the SCRIPT command is similar to the SYSTEM command dialogs. See SCRIPT command reference on page 952 for a description of the `HALT` parameter and command syntax.



SCRIPT command reference

The SCRIPT command has the following syntax:

```
SCRIPT [-HALT] [SuccessCodes=…] "scriptFilename" ["argument"... ]
```

`-HALT`

Stop the script execution when a service/daemon is requested. When not specified, the service/daemon may not shutdown until the script has finished executing.

`[SuccessCodes=…]`

For the SCRIPT commands, VersaLex allows you to define integer value exit codes to consider successful. To define these codes, the optional parameter, `[SuccessCodes=...]`, must precede the command string. The values specified are the exit codes (and code ranges) your application considers to be successful. Within the list,

use commas to separate codes and code ranges (low to high). By default, either zero or undefined (no return code) are considered successful.

"*scriptFilename*"

Local source path to the JavaScript file to execute.

"[*argument]*"

Optional argument(s) to pass to the script. Macro variables are supported. See Using Macro Variables (SYSTEM and SCRIPT Command context) for a list of the applicable macros.

Appendix

C

URI File System Interface

The Cleo Harmony and Cleo VLTrader applications employ a URI File System Interface, used to store and retrieve payload files. This section details the three predefined URI schemes: **JMS**, **MSMQ**, and **VLPipe**. You can also develop custom URI schemes and add them to the Cleo Harmony or Cleo VLTrader application.

URI File System interface overview

Note: This section applies to the Cleo Harmony and Cleo VLTrader applications only.

The Cleo Harmony application currently has three predefined URI schemes:

- **JMS**: Used to read and write messages to Java Message Service queues. Cleo Harmony implements the client side of JMS. See JMS URI scheme on page 955.
- **MSMQ**: Used to read and write messages to Microsoft Message Queuing queues. Cleo Harmony implements the client side of MSMQ. See MSMQ URI scheme on page 960.
- **VLPipe**: Used to pipe payload coming into one mailbox out through another Cleo Harmony mailbox. See VLPipe URI scheme on page 962.

In addition, you can develop custom URI schemes in Java and add them to the Cleo Harmony application. See custom URI schemes

These URI schemes can be used in the host-level Inbox and Outbox fields or as the source/destination in actions. If the URI scheme mimics a file system, then that scheme can be used for local user folders.

Sample URIs:

- `jms:jndi:InboxQueue?jndiConnectionFactoryName=ConnFact&filenameProp=filename`
- `msmq:DIRECT=OS:.\private$\Inbox?createQueue=true`
- `vlpipe:FTPPipeDevTest\myMailbox`
- `mydb:\MyDBInbox`
- `hdfs:\hdfsnamenode:50070\Inbox`

Note: The scheme name in the URI is case insensitive.

JMS URI scheme

The VersaLex JMS URI is for using Java Message Service (JMS) queues instead of local file system files for payload sent to and/or received from trading partners.

The basic format of the JMS URI is:

```
jms:jndi:jmsQueueName?param1=value1&param2=value2&param3=...
```

Example:

```
jms:jndi:OutboxQueue?
msgFilename=test.edi&jndiConnectionFactoryName=ConnectionFactory&
jmsSelector=(SomeProperty='abcd')&filenameProp=filename
```

The JMS URI system interface has these important qualifications:

1. VersaLex JMS URI only supports Java Naming and Directory Interface (JNDI) connections to JMS providers.
2. JMS supports many different message types: BytesMessage, TextMessage, StreamMessage, MapMessage, ObjectMessage, and Message. VersaLex JMS URI only supports the BytesMessage and TextMessage message types. All other message types in the queue will be ignored and remain in the queue.
3. JMS supports Topics as well as Queues. VersaLex JMS URI only supports Queues.
4. If necessary, a custom JMS URI can be created which could support any of the items not supported above.

JMS URI Parameters

Optional parameters specified in the URI include the following:

jndiConnectionFactoryName=

This parameter is the connection factory name within JMS. Since there can be multiple connection factories within a single JMS, this parameter is typically required.

jndiInitialContextFactory=

This parameter is the initial context factory name. With some JMS implementations, such as GlassFish, this parameter does not need to be specified as it will be automatically determined during the call to `javax.naming.InitialContext()`.

jndiURL=

This parameter is the JNDI URL. With some implementations, such as GlassFish, this parameter does not need to be specified as it will be automatically determined during the call to `javax.naming.InitialContext()`.

ctxProps=

This parameter is used to specify additional properties that will be used during the call to `javax.naming.InitialContext(environment)`. InitialContext is used when making a connection to the JMS provider.

connectionID=

This parameter is used to specify a connection ID to reference properties from the properties file specified in the system property `cleo.uri.jms.connectionFile`.

msgType=

This parameter is used to specify whether the JMS message should be considered to be a JMS TextMessage or a JMS BytesMessage. Text messages use the UTF-8 character set. The legal values are `text` for a TextMessage and `bytes` for a BytesMessage. The default value is `bytes`.

filenameProp=

JMS does not have a set place to store a filename for a message. This parameter specifies the name of a String Property to hold the filename for a message. If this property is not present, then no filename will be saved into sent messages. If this property is not present when reading from the queue, the filename will be based on the JMS message ID.

msgFilename=

This parameter is used to specify the filename for a `PUT`, `GET`, `PUT+GET`, or `LCOPY` command. It is used in conjunction with the filenameProp parameter. When used as the source for a command, the filename can be a wildcard or regular expression.

maxMessages=

This parameter is used to specify the maximum number of messages that will be read from the queue. Please note that if a JMS selector is used, the number of messages matching that selector will be returned. If a JMS selector is not used and a filename wildcard is used, it will read the first *maxNumOfMessages* messages and then apply the filename filter. This could result in fewer messages than expected.

jmsProps=

This parameter is used to specify JMS message string properties that will be added to the message. This parameter is only used in the Inbox or as the file destination.

jmsSelector=

This parameter is used to specify a JMS selector expression to select only certain items from the queue. The syntax of the expression is based on a subset of the `SQL92` conditional expression syntax. For example, the string *(prop1='val1') and (prop2 LIKE 'val%%')* selects only those messages containing a string property, *prop1*, with a value of *val1* and another string property, *prop2*, with a value starting with *val*. This parameter is used in the Outbox or as the file source. The typical % used in the JMS Selector expression must be specified as two percents (%%) since VersaLex uses % for macros.

msgID=

This parameter is used to specify a specific JMS message ID. This parameter cannot be a wildcard or regular expression. It is not typically specified in an action. It can be used to retrieve a specific message out of the JMS queue.

Parameters that could be added automatically by VersaLex include the following:

msgFilename=

This parameter is the filename for the message. If no filenameProp is specified, this will be the JMS message ID converted to a filename. Otherwise it contains the value from the String property specified by filenameProp.

msgID=

This is the JMS message ID. It is added to the URI so that a `-DEL` operation on a `PUT` can delete the specific message read.

length=

This is the length of the message.

time=

This is the timestamp of the JMS message. The format of the message time is YYYYMMDD-HHMMSS.

correlationId=

This is the correlation ID of the JMS message.

System properties can be defined for some of the JMS URI parameters. The parameters defined at the system property level would apply to all JMS URIs unless overridden in the URI itself or by a Connection ID property. The following system properties can be defined:

cleo.uri.jms.jndiConnectionFactoryName

Can be used in place of the jndiConnectionFactoryName URI parameter.

cleo.uri.jms.jndiInitialContextFactory

Can be used in place of the jndiInitialContextFactory URI parameter.

cleo.uri.jms.jndiURL

Can be used in place of the jndiURL URI parameter.

cleo.uri.jms.filenameProp

Can be used in place of the filenameProp URI parameter.

cleo.uri.jms.maxMessages

Can be used in place of the maxMessages URI parameter.

cleo.uri.jms.context.*ContextKey*

Can be used in place of or in addition to the ctxProps URI parameter and/or the Connection ID context properties. For example, if you wanted to set java.naming.security.authentication to **simple** as a default for all JMS connections, you would add the following line to the `system.properties` file:
`cleo.uri.jms.context.java.naming.security.authentication=simple`

cleo.uri.jms.connectionFile

Used to define a properties file containing JMS connection properties. The properties in this file are used in conjunction with the connectionID URI parameter above.

Certain properties can be defined per Connection ID. The properties defined at the Connection ID level would apply to any JMS URIs using the specific Connection ID which are not overridden in the URI itself. The following Connection ID properties may be defined for each *connectionID*.

cleo.uri.jms.connections.connectionID.username

Username used when creating connections to the JMS queue.

cleo.uri.jms.connections.connectionID.pw

Password used when creating connections to the JMS queue.

cleo.uri.jms.connections.connectionID.jndiConnectionFactoryName

Can be used in place of the jndiConnectionFactoryName URI parameter.

cleo.uri.jms.connections.connectionID.jndiInitialContextFactory

Can be used in place of the jndiInitialContextFactory URI parameter.

cleo.uri.jms.connections.connectionID.jndiURL

Can be used in place of the jndiURL URI parameter.

cleo.uri.jms.connections.connectionID.filenameProp

Can be used in place of the filenameProp URI parameter.

cleo.uri.jms.connections.connectionID.maxMessages

Can be used in place of the maxMessages URI parameter.

cleo.uri.jms.connections.connectionID.context.ContextKey

Can be used in place of, or in addition to, the ctxProps URI parameter and the System context properties. For example, to set java.naming.security.authentication to **simple** for Connection ID ConnID1, you would add the following line to the properties file:
`cleo.uri.jms.connections.ConnID1.context.java.naming.security.authentication=simple`

Some parameters and properties can be specified at three different levels: in the URI string, in the Connection ID properties, and in the System properties. The parameters specified in the URI always override the values in the Connection ID properties and the System properties. The Connection ID properties override those in the System properties. If a value is in the System property that is not needed for a specific Connection ID property, the property can be added to the Connection ID properties file without a value.

There are many JMS servers available. Each of these servers provide their own custom .jar files that are used to send and receive JMS messages. These .jar files should be added to the VersaLex base class path using the cleo.additional.classpath system property. If more than one .jar file is necessary, the list of .jar files should be separated with a semicolon (;) on Windows systems and a colon (:) on Unix systems. Forward slashes (/) can be used for both Windows and Unix. If a backslash is used (\), then two backslashes (\\) must be used between each directory.

For example, for GlassFish V3 the system property defined in the conf/system.properties file would look similar to `cleo.additional.classpath=C:/glassfish3/glassfish/lib/gf-client.jar`.

If the GlassFish server is not installed on the same workstation as VersaLex, then either:

- GlassFish would need to be loaded on the same workstation as VersaLex but not executed
- The necessary GlassFish files would need to be copied from the GlassFish installation to the VersaLex workstation
- The GlassFish files would need to be accessed through a network share.

JMS URI Sample Usages

If the host-level Inbox/Outbox are specified as JMS queues:

Inbox:

```
jms:jndi:InboxQueue?
jndiConnectionFactoryName=ConnectionFactory&filenameProp=filename
```

Outbox:

```
jms:jndi:OutboxQueue?
jndiConnectionFactoryName=ConnectionFactory&filenameProp=filename
```

Sample commands:

`PUT -DEL *`

Sends all messages in queue and deletes after successful send.

`PUT -DEL test.edi`

Sends the first message with the filename `test.edi` and deletes after successful send.

`PUT -DEL [test.edi]`

Sends all messages with the filename property matching the regular expression [test.edi]. If there are multiple test.edi messages in the queue, each of them will be sent and deleted after a successful send.

`GET *`

Retrieves all remote files and stores them in the InboxQueue.

`LCOPY -DEL * C:\SomeDir\`

Copies all messages from the InboxQueue to `C:\SomeDir\` and deletes them from the queue.

In the case of unsolicited incoming files, the files will automatically be added as messages to the end of InboxQueue.

If the host-level Inbox/Outbox are specified as folders on the local file system:

- Inbox: `Inbox/`
- Outbox: `Outbox/`

Then you can still use the JMS queue within the action commands.

Sample commands:

`PUT -DEL "jms:jndi:OutboxQueue?msgFilename=*&`
`jndiConnectionFactoryName=ConnectionFactory&filenameProp=filename"`

Sends all messages in the queue and deletes after successful send

`PUT -DEL "jms:jndi:OutboxQueue?msgFilename=test.edi&`
`jndiConnectionFactoryName=ConnectionFactory&filenameProp=filename"`

Sends the first message with the filename property of `test.edi` and deletes after successful send

**PUT -DEL "jms:jndi:OutboxQueue?msgFilename=[test.edi]&
jndiConnectionFactoryName=ConnectionFactory&filenameProp=filename"**

Sends all files which match the regular expression [test.edi]. If there are multiple test.edi messages in the queue, each of them will be sent and deleted after a successful send.

**GET * "jms:jndi:InboxQueue?jndiConnectionFactoryName=ConnectionFactory&
filenameProp=filename"**

Retrieves all remote files and stores them in the InboxQueue.

**LCOPY -DEL "jms:jndi:InboxQueue?jndiConnectionFactoryName=ConnectionFactory&
filenameProp=filename" C:\SomeDir**

Copies all messages from the InboxQueue to `C:\SomeDir\` and deletes them from the queue.

MSMQ URI scheme

The VersaLex MSMQ URI is for using Microsoft Message Queuing (MSMQ) queues instead of local file system files for payload sent to and received from trading partners.

The basic format of the MSMQ URI is:

```
msmq:DIRECT=OS:msmqQueue?param1=value1&param2=value2& param3=…
```

Example:

```
msmq:DIRECT=OS:.\private$\Inbox?createQueue=true
```

VersaLex only supports the DIRECT=OS queues.

MSMQ URI Parameters

Optional parameters specified in the URI include the following:

createQueue=

Specifies whether or not the queue should be created if it does not exist.

msgLabel=

Specifies the MSMQ message label. The message label is used as the filename.

msgID=

Specifies a MSMQ message ID. This parameter cannot be a wildcard or regular expression. This parameter is not typically specified in an action. It can also be used to retrieve a specific message out of the MSMQ queue.

timeoutSec=

Specifies the number of seconds to wait when reading a specific message from the queue. If not specified, the default is 5 seconds. This parameter is not typically specified.

Parameters that can be automatically added by VersaLex include the following:

msgLabel=

Specifies the MSMQ message label. The message label is used as the filename.

msgID=

Added to the URI so that a `-DEL` operation on a `PUT` can delete the specific message read.

length=

Length of the message.

arrival=

Arrival time of the message.

correlationID=

Correlation ID of the message.

MSMQ URI Sample Usages

If the host-level Inbox/Outbox are specified as MSMQ queues:

- Inbox: `msmq:DIRECT=OS:.\private$\Inbox?createQueue=true`
- Outbox: `msmq:DIRECT=OS:.\private$\Outbox?createQueue=true`

Sample commands:

`PUT -DEL *`

Sends all messages in the queue and deletes them after successful send.

`PUT -DEL test.edi`

Sends the first message with the label `test.edi` and deletes it after successful send.

`PUT -DEL [test.edi]`

Sends all messages with message label matching the regular expression [test.edi]. If there are multiple `test.edi` message labels in the queue, each will be sent and deleted after successful send.

`GET *`

Retrieves all remote files and stores them in `DIRECT=OS:.\private$\Inbox`.

`LCOPY -DEL * C:\SomeDir\`

Copies all messages from the `DIRECT=OS:.\private$\Inbox` to `C:\SomeDir\` and deletes them from the queue.

In the case of unsolicited incoming files, the files will automatically be added as messages to the end of `DIRECT=OS:.\private$\Inbox`.

If the host-level Inbox/Outbox are specified as folders on the local file system as follows, then you can still use the MSMQ queue within the action commands:

- Inbox: `Inbox/`
- Outbox: `Outbox/`

Sample commands:

`PUT -DEL "msmq:DIRECT=OS:.\private$\Outbox?msgLabel=*"`

Sends all messages in the queue and deletes them after successful send.

`PUT -DEL "msmq:DIRECT=OS:.\private$\Outbox?msgLabel=test.edi"`

Sends the first message with the label `test.edi` and deletes it after successful send.

`PUT -DEL "msmq:DIRECT=OS:.\private$\Outbox?msgLabel=[test.edi]"`

Sends all messages with labels matching the regular expression [test.edi]. If there are multiple `test.edi` message labels in the queue, each of them will be sent and deleted after successful send.

`GET * "msmq:DIRECT=OS:.\private$\Inbox"`

Retrieves all remote files and stores them in `DIRECT=OS:.\private$\Inbox`.

`LCOPY -DEL "msmq:DIRECT=OS:.\private$\Inbox" C:\SomeDir\`

Copies all messages from `DIRECT=OS:.\private$\Inbox` to `C:\SomeDir\` and deletes them from the queue.

VLPipe URI scheme

The VersaLex VLPipe URI is for piping input payload from one host's Inbox out through another mailbox. The host and mailbox are specified in the URI. The <send> action will be used to send incoming payload out through the host \mailbox. VLPipe can only be used for inboxes – it is nonsensical for outboxes.

The basic format of the MailboxPipe URI is:

```
vlpipe:host\mailbox
```

Example:

```
vlpipe:FTPPipeDevTest\myMailbox
```

VLPipe URI Sample Usages

If the host-level Inbox is specified as a mailbox pipe:

```
vlpipe:FTPPipeDevTest\myMailbox
```

Then all incoming payload (whether solicited or unsolicited) will be redirected through <send>myMailbox@FTPPipeDevTest

Custom URI scheme

Custom scheme(s) can be created to access payload not normally accessible to VersaLex. A URI scheme must start with a letter and be followed by one or more alpha-numeric characters.

The custom URI scheme implementation must provide three basic classes:

1. **File class** – A class that provides that similar functionality as the java.io.File class. The custom *Scheme* File class must extend com.cleo.lexicom.beans.LexURIFile.
2. **InputStream class** – A class that provides similar functionality as the java.io.InputStream class. The custom *Scheme* InputStream class must extend java.io.InputStream.
3. **OutputStream class** – A class that provides similar functionality as the java.io.OutputStream class. The custom *Scheme* OutputStream class must extend java.io.OutputStream.

These three custom-written classes are configured in system properties. System properties are used to configure the class names for single URI scheme:

cleo.uri. ***scheme*** .file (required)

cleo.uri. ***scheme*** .inputstream (required)

cleo.uri. ***scheme*** .outputstream (required)

In addition, an optional classpath variable is provided to specify the path to the implementation jar and any support jar files necessary:

cleo.uri. ***scheme*** .classpath (optional)

If any additional jars need to be in the base VersaLex class loader, then the **cleo.additional.classpath** system property must be used.

The Cleo versions of JMS, MSMQ, and VLPipe can be replaced with custom versions by specifying these system properties for JMS, MSMQ, or VLPipe and naming the custom classes.

Further documentation for custom URI schemes is provided in the API documentation (see LexURIFile in the JavaDocs).

Appendix

D

Troubleshooting

Following is a list of potential problems while using Cleo Harmony. The list covers general problems. For technical support, call 1-866-444-2536 or email support@cleo.com.

Note: Technical support is on a paid subscription basis. See Cleo Technical Support on page 11.

The Cleo Harmony application will not install – installer stops

Possible cause: Windows desktop does not have enough display colors.

Possible solution: Increase the number of display colors.

The Cleo Harmony application will not install – Message "No GZIP found"

Possible cause: Unix platforms require either GZIP or ZIP be installed as a prerequisite.

Possible solution: Install GZIP or ZIP.

The Cleo Harmony application will not install; Message "Can't connect to X11 window server ..."

Possible cause: Unix platforms require an X window to run the GUI installer.

Possible solution: Either run the installer in an X window or run the installer with console mode turned on (-i console).

The Cleo Harmony application will not install – Message box: "Magic number does not match" or "The program is too big to fit into memory"

Possible cause: Windows virus scanning software is running.

Possible solution: Stop virus scanning software and retry.

Possible cause: Downloaded size of install does not match advertised size

Possible solution: Retry or obtain VersaLex via another media

The Cleo Harmony application will not execute

Possible cause: Java Virtual Machine is missing.

Possible solution: Reinstall VersaLex and include the JVM in the download

Possible cause: `license_key.txt` is invalid.

Possible solution: See Registering your serial number on page 658

Possible cause: `\logs\ \ VersaLex.xml` file is corrupted.

Possible solution: If you cannot open log file in a browser, archive or delete the file.

Possible cause: `\conf\Options.xml` file is corrupted.

Possible solution: If you cannot open log file in a browser, archive or delete the file.

Possible cause: `\lib\LexiCom.jar`, `\lib\lexbean.jar`, or `lax.jar` file is missing or corrupted

Possible solution: Reinstall VersaLex

Possible cause: An exception is occurring at startup

Possible solution: Look in the `logs\` directory for a file named `exception.txt`. If it exists, it will contain the date and time of the exception and a trace.

Cannot see the Cleo Harmony application window

Possible cause: Using PCAnywhere.

Possible solution: In PCAnywhere, go to **Tools** > **Options** > **Host** operation and set the video selection option to **Compatibility**.

Message box: "VersaLex requires Java VM version x.x, found Java VM version x.x"

Possible cause: Java Virtual Machine too old or too new

Possible solution: Reinstall VersaLex and include the JVM in the download

Message box: "Invalid license string" or similar error

Possible cause: `license_key.txt` file is corrupted

Possible solution: See Registering your serial number on page 658

Message box: This license requires Host ID "xxxxxx". Your Host ID is "yyyyyy".

Possible cause: Permanent licenses are for a specific install of the Cleo VersaLex application. A permanent license cannot be used for two different installs,

Possible solution: Purchase another copy of VersaLex.

Possible cause: The `license_key.txt` has been incorrectly created for the wrong host ID.

Possible solution: Contact Cleo support

Message box: This application has been copied to another location. Please re-license it with your existing license key.

Possible cause: Backup utility is modifying time/date stamp oflicense files.

Possible solution: Exclude the `\.license` subfolder from the backup. Delete the `\.license` subfolder. If the product is still under a temporary license, see Registering your serial number on page 658. If the product has been permanently licensed, contact Cleo support.

Message: Exception: "java.lang.ClassNotFoundException: com.cleo.LexiCom.beans...

Possible cause: VersaLex bean `lib\_.jar` file is missing

Possible solution: Reinstall the Cleo Harmony application.

Possible cause: `\hosts\_.xml` or `\hosts\preconfigured\_.xml` file refers to an unknown bean class

Possible solution: Reinstall Cleo Harmony

Host icon not displaying in tree

Possible cause: VersaLex bean `lib\_.jar` file is missing or corrupted

Possible solution: Reinstall Cleo Harmony

Message: Exception: "org.xml.sax.SAXParseException: ...

Possible cause: `\hosts\_.xml` or `\hosts\preconfigured\_.xml` file is corrupted

Possible solution: If you cannot open host file in a browser, then manually correct or delete the file. Reinstall the Cleo Harmony application to reinstall pre-configured hosts.

Message: Warning: 'xxx' property specified in 'xxx' element in host file 'hosts_.xml' does not exist; value not set in 'Xxx' host

Possible cause: `\hosts\_.xml` or `\hosts\preconfigured\_.xml` file contains unknown property name

Possible solution: Host is still usable. Reinstall the Cleo Harmony application to reinstall pre-configured hosts.

Dial-up internet connection failing (Windows users only)

Possible cause: `LexiComDialer.exe` not installed in the VersaLex home directory

Possible solution: Reinstall the Cleo Harmony application and include Cleo LexiCom Dialer in the install.

Possible cause: Invalid dial-up setup

Possible solution: See Setting up a dial-up connection (Windows users only) on page 56

Possible cause: Connection timeout value too small

Possible solution: See Specifying default host directories on page 700

Possible cause: Hardware or other problem

Possible solution: Solution is outside Cleo Harmony

Initial connection to host times out

Possible cause: Local packet filtering firewall is blocking traffic

Possible solution: See Reviewing TCP/IP port usage on page 887

Possible cause: Local forward proxy is required

Possible solution: See Configuring for a proxy on page 881

Possible cause: Connection timeout value too small

Possible solution: Increase the host timeout value

Possible cause: Server is down or experiencing difficulties

Possible solution: Retry. If problem persists, contact server administrator

Initial connection to host fails

Possible cause: Server address is a fully-qualified name, and it cannot be resolved

Possible solution: If ping cannot resolve the fully-qualified name, change the host server address to an IP address

Possible cause: Network address unreachable

Possible solution: Unless need to setup dial-up connection, solution is outside Cleo Harmony

Possible cause: Wrong network parameter

Possible solution: Check host general, protocol, and firewall settings.

Possible cause: Wrong login parameter

Possible solution: Check mailbox and action settings

Possible cause: Server certificate not trusted or client certificate missing or invalid

Possible solution: Check trusted Certificate Authorities (see Certificate management on page 661) and check host and mailbox security settings

Cleo Harmony application is slow starting up

Possible cause: `\logs\ VersaLex.xml` file is too large

Possible solution: Archive or delete the log file.

Command prompt window showing up behind GUI window

Possible cause: Using wrong executable

Possible solution: Use `VersaLex.exe` rather than `VersaLexc.exe`.

Command line options not printing any messages

Possible cause: Using wrong executable

Possible solution: Use `VersaLex.exe` rather than `VersaLexc.exe`

Message Exception:"java.io.IOException: Unable to create xxx 'xxx' directory (The directory path syntax may be incorrect)."

Possible cause: Directory is on a mapped drive and the Cleo VersaLex application is running as a Windows service

Possible solution: By default, windows services run under a SYSTEM user and do not see mapped drives. Either do not run Cleo Harmony as a service **or** use the full network path name for the directory (for example, instead of `G:\in` use `\\server\\sharename\in`) and change the service's logon account.

Appendix

E

XML file formats

The XML files in the Cleo Harmony, Cleo VLTrader, and Cleo LexiCom server directories have built-in preconfigured host and log file formats which become activated when the user configures them. This section explains the formatting of the host and log files.

Host files

Each available host type within the Cleo Harmony software comes pre-configured within an XML file in the `\hosts\preconfigured` directory. If a pre-configured host is activated, its XML file is copied to the `\hosts` directory and is then updated as the user further configures the host through the Cleo Harmony panels.

A host XML file is generally formatted as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <Host class="encoded LexiCom class" alias="name of service, VAN, or ?" transport="method/protocol"
  type="specific type" application="category">
   <Property1>value</Property1>
   <Property2>value</Property2>
   <Property...>value</Property...>
  - <Mailbox class="encoded LexiCom class" alias="your company, location, username, or ?">
      <Property1>value</Property1>
      <Property2>value</Property2>
      <Property...>value</Property...>
    - <Action class="encoded LexiCom class" alias="send, receive, or ?">
        <Property1>value</Property1>
        <Property2>value</Property2>
        <Property...>value</Property...>
        <Commands>line 1 line 2 ...</Commands>
      </Action>
    - <Action...>
        <Property1>value</Property1>
        <Property2>value</Property2>
        <Property...>value</Property...>
      </Action...>
    </Mailbox>
  - <Mailbox...>
      <Property1>value</Property1>
      <Property2>value</Property2>
      <Property...>value</Property...>
    </Mailbox...>
  - <TradingPartner class="encoded LexiCom class" alias="trading partner's name">
      <Property1>value</Property1>
      <Property2>value</Property2>
      <Property...>value</Property...>
    </TradingPartner>
  - <TradingPartner...>
      <Property1>value</Property1>
      <Property2>value</Property2>
      <Property...>value</Property...>
    </TradingPartner...>
</Host>
```

- One and only one `<Host>` element exists in the file.
- `<Host>` may contain zero or more `<Mailbox>` elements and zero or more `<TradingPartner>` elementss.
- `<Mailbox>` may contain zero or more `<Action>` elements.
- The `class="path"` identifies the VersaLex module that corresponds to this host type and tree level. It is a java class path relative to the base VersaLex bean package.
- The `alias="value"` cannot contain the backslash character (\).
- `<Property1>`, `<Property2>`, `<Property...>` do not actually exist. Some common property names and possible values do exist, but most are dependent on the specific host type.

The common `<Host>` level properties and their definitions and values are as follows:

<Address>

The server address, either a fully-qualified name (recommended) or an IP address.

<Port>

The server port, either a specific port number or `-1` to indicate the default port for the protocol.

<Connecttype>

The connection type. Possible values are:

- 0: system default

- 1: direct internet access
- 2: LexRas dial-up connection
- 3: GXS IBC dial-up connection

<Phonebookentry>

Existing Windows RAS phonebook entry

<Ibcusername>

GXS IBC account username

<Ibcpassword>

GXS IBC account password

<Inbox>

Any local or shared directory

<Outbox>

Any local or shared directory

<Sentbox>

Any local or shared directory

<Notes>

Any pertinent information

The `<Mailbox>` and `<TradingPartner>` level each only have one common property:

<Notes>

Any pertinent information

The `<Action>` level properties and their definitions are:

<Commands>

Formatted command lines and syntax specific to hosts

<Messages>

Messages logged the last time the action was run

<Notes>

Any pertinent information

All pre-configured hosts are not created equally. The more generic host types contain little or no properties, while the more specific host types may contain almost all the required properties. The more information contained in the pre-configured host file, the less information the user must provide when the host is activated.

For example, the following generic HTTP/s host file provides no property values.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<Host class="*CwwQNwwPCws3URoNChwaDFERHhodDwsLF1FBBRsPGhoPUwwaEQ4PBk5D"
  alias="Generic HTTP/s" transport="HTTPs" preconfigured="2002/07/29 08:48"
  serial="CLEOWS01:LX9012" />
```

If you want to start with the generic HTTP/s host to connect to our example ABC VAN host, use the Cleo Harmony configuration panels to provide values for the following properties.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <Host class="*CwwQNwwPCws3URoNChwaDFERHhodDwsLF1FBTx0KFUhLUxwGFBpGRkM*" alias="ABC VAN"
  by="aevett" enabled="True" local="False" modified="2002/10/11 15:32" preconfigured="2002/05/22 07:57"
  ready="True" transport="HTTPs" serial="CLEOWS01:LX9012">
  <Address>cleows01.dficomm.dficom.com</Address>
  <Connecttype>0</Connecttype>
  <Filedelimiter>\t</Filedelimiter>
  <Fileidentifiedby>2</Fileidentifiedby>
  <Fileidentifiedfieldnum>1</Fileidentifiedfieldnum>
  <Fileidentifiedposition>1</Fileidentifiedposition>
  <Headerlines>1</Headerlines>
  <Linedelimiter>\n</Linedelimiter>
  <Port>-1</Port>
  <Secure>True</Secure>
 - <Mailbox class="*BxAdExYeMgwPCws3URoNChwaDFERHhodDwsLF1E*" alias="myMailbox" by="aevett"
    enabled="True" modified="2002/07/22 16:33" ready="True">
   - <Action class="*ERAWCxw+DA8LCzdRGg0KHBoMUREeGh0PCwsXUQ**" alias="send+receive"
      by="aevett" enabled="True" modified="2002/07/22 16:33" ready="True">
      <Commands>CONNECT PUT -DEL .\ GET -DIR -DEL -UNI .\</Commands>
    </Action>
   - <Action class="*ERAWCxw+DA8LCzdRGg0KHBoMUREeGh0PCwsXUQ**" alias="send" by="aevett"
      enabled="True" modified="2002/08/12 08:10" ready="True">
      <Commands>CONNECT PUT -DEL .\</Commands>
    </Action>
   - <Action class="*ERAWCxw+DA8LCzdRGg0KHBoMUREeGh0PCwsXUQ**" alias="receive" by="aevett"
      enabled="True" modified="2002/08/23 13:39" ready="True">
      <Commands>CONNECT GET -DIR -DEL -UNI .\</Commands>
    </Action>
  </Mailbox>
  <Syntax>CONNECT POST /servlet/edi/login?key=1&user=&*pswd=</Syntax>
  <Syntax>PUT POST /servlet/edi/send receiver=%tp,type=|EDIFACT|X12|XML|,filename=%file</Syntax>
  <Syntax>GET POST /servlet/edi/receive?filename=%dir</Syntax>
  <Syntax>DIR POST /servlet/edi/list?[type=|EDIFACT|X12|XML|]</Syntax>
  <Syntax>DELETE POST /servlet/edi/delete?filename=%dir</Syntax>
</Host>
```

The best way to learn a property name and possible values for a specific host type is to use the Cleo Harmony UI to configure the host and then interrogate the XML file.

System log file

Located in `\logs\VersaLex.xml`, the system log file is also an XML file. While your VersaLex software is running, the log is continually appended with any messages generated by running actions or by the application shell. However, even though it is continuously updated, the log is always a valid and well-formed XML file.

The log XML file is formatted as follows:

```
<?xml version="1.0" standalone="yes" ?>
- <Log descName="Cleo Communications application log file">
  - <Session appName="LexiCom" version="2.0">
      <System name="CLEOWS01" address="10.10.1.65" locale="USA" timeZone="CST" OS="Windows 2000" version="5.0" java="1.3
    - <Run date="2002/05/17 12:03:10" TN="1" CN="1" EN="1">
      - <Event>
          <Thread type="CommandLine" action="<send+receive>myMailbox@ABC VAN" />
          <Mark date="2002/05/17 12:03:10" TN="1" EN="1" />
        </Event>
      - <Event>
          <Command text="CONNECT user=82351,*pswd=*DBoRGxoNTg**" type="HTTP" line="1" />
          <Mark date="2002/05/17 12:03:12" TN="1" CN="1" EN="2" />
        </Event>
      - <Event>
          <Detail level="0">Connecting to https://cleows01.dficomm.dficom.com...</Detail>
          <Mark date="2002/05/17 12:03:12" TN="1" CN="1" EN="3" />
        </Event>
      - <Event>
          <Request text="POST /servlet/edi/login key=1,user=82351,pswd=*DBoRGxoNTg**" type="HTTP" />
          <Mark date="2002/05/17 12:03:12" TN="1" CN="1" EN="4" />
        </Event>
      - <Event>
          <Response host="200 OK" />
          <Mark date="2002/05/17 12:03:16" TN="1" CN="1" EN="5" />
        </Event>
      - <Event>
          <Result text="Success" command="CONNECT user=82351,*pswd=*DBoRGxoNTg**" line="1" />
          <Mark date="2002/05/17 12:03:16" TN="1" CN="1" EN="6" />
        </Event>
      - <Event>
          <Command text="PUT -DEL .\ receiver=73529,type=X12" type="HTTP" line="2" />
          <Mark date="2002/05/17 12:03:16" TN="1" CN="2" EN="7" />
        </Event>
      - <Event>
          <File source="outbox\test.txt" direction="Local->Host" number="1 of 1" />
          <Mark date="2002/05/17 12:03:16" TN="1" CN="2" EN="8" />
        </Event>
      - <Event>
          <Request text="POST /servlet/edi/send" type="HTTP" />
          <Mark date="2002/05/17 12:03:16" TN="1" CN="2" EN="9" />
        </Event>
      - <Event>
          <Transfer kBytes="1.497" seconds="0.67" />
          <Mark date="2002/05/17 12:03:17" TN="1" CN="2" EN="10" />
        </Event>
      - <Event>
          <Response host="200 OK" />
          <Mark date="2002/05/17 12:03:17" TN="1" CN="2" EN="11" />
        </Event>
      - <Event>
          <Result text="Success" command="PUT -DEL .\ receiver=73529,type=X12" line="2" source="outbox\test.txt" direction="
            deleted.</Result>
          <Mark date="2002/05/17 12:03:17" TN="1" CN="2" EN="12" />
        </Event>
      + <Event>
      + <Event>
      + <Event>
      + <Event>
      + <Event>
      + <Event>
      - <Event>
          <End />
          <Mark date="2002/05/17 12:03:29" TN="1" EN="19" />
        </Event>
      </Run>
    </Session>
  + <Session appName="LexiCom" version="2.0">
  </Log>
```

- One and only one <Log> exists in the file.
- <Log> may contain one or more <Session>elements.
- <Session> has the product name and version.
- <Session> contains one <System>, one <License>, and one <Run>.

- <System> has information about the computer.
- <License> has information about the installed license.
- <Run> has the <Session> starting date/time stamp, <Thread> number, <Command> number, and <Event> number.
- <Run> may contain one or more <Event> elements.
- <Event> contains either <Thread>, <Detail>, <Command>, <File>, <Transfer>, <Request>, <Response>, <Result>, or <End> always followed by <Mark>.
- <Thread> marks the start of an action run, has run type and action path.
- <Detail> provides extra detailed information anywhere in the flow.
- <Hint> provides insight into possible cause of error or exception.
- <Command> marks the start of a command within an action, has command text and line number.
- <File> marks the start of a file transfer within a command, has file paths and counts. If the file being transferred is part of a zip archive, then the entry name is included. Further, if the file being transferred is part of an unzip operation, then the entry number is placed in brackets (e.g., number=1[5] of 3 indicates this file is the fifth entry of the first zip file a total of three zip files that are being unzipped).
- <Transfer> marks the completion of a file transfer, has transfer rate.
- <Request> contains the protocol-specific request made to the host.
- <Response> contains the protocol-specific response from the host.
- <Result> marks the end of a command or file transfer, has resultant status. The <Result> element also repeats <Command>, <File>, and <Transfer> information so that this element alone can be used to determine command and file transfer results. The CRC-32 value, if available, is also included in the <Result> element.
- <End> marks the end of an action.
- <Mark> has the date/time stamp and corresponding <Thread> number, <Command> number, and <Event> number.

Because more than one action can be active at any given time, the <Thread> number and <Command> number references provide a means for grouping related <Event>s together.

The command line options allow an extra log file (same format) to be generated to a user-specified path (see Running from the command line on page 38). This log file is in addition to the overall system log file and contains only the messages generated by that session of the Cleo Harmony server.

The Cleo Harmony software provides a log file viewer for the active log file or any archived log file. Outside of Cleo Harmony, a log file can be viewed through any browser (like above) at any time, potentially with an XSL style sheet applied.

Appendix

F

Cryptographic Services

This secction provides information about the cryptographic services that can be used with your VersaLex system. The VersaLex products support six common cryptosystems: SSL/TLS, SSHv2, S/MIME, XML, OpenPGP, and FIPS 140-3.

- SSL/TLS is supported through FTP, HTTP, OFTPv2, and SMTP.
- SSHv2 is supported through SSH FTP.
- S/MIME is supported through AS2/HTTP, AS3/FTP, OFTPv2, and RNIF/HTTP.
- XML is supported through AS4/HTTP, ebXML/HTTP, and mailbox-level packaging.
- OpenPGP is supported through mailbox-level packaging.
- FIPS 140-3 is layered on top of all the other cryptosystems.

The following describes the supported cryptographic services, as well as encryption, content integrity, and signatures.

Cryptographic services overview

SSL/TLS

Secure Sockets Layer (SSL) and the newer Transport Layer Security (TLS) provide a secure connection over any TCP/IP protocol using a combination of cryptographic processes. The initial handshake between client and server negotiates a version and cipher. RFC 8446 specifies the latest TLS version.

SSHv2

Secure Shell 2 is a secure communications protocol that encompasses several layers of architecture, including transport, authentication, and connection. Public key, cipher, key exchange, and hash algorithms are negotiated between client and server at the beginning of each connection.

S/MIME

Internet MIME (Multipurpose Internet Mail Extensions) messages consist of two parts: headers (describing the content) and a body (consisting of the actual data content or payload). MIME was not designed to provide for the application of security services, therefore S/MIME (Secure/Multipurpose Internet Mail Extensions) was created as a format and protocol for applying authentication, message integrity, non-repudiation (through the use of public key cryptography) and confidentiality (using encryption) to the Internet MIME message.

S/MIME is supported by transport mechanisms in one of either two versions: S/MIME v2 or S/MIME v3. The most notable difference between the two is that S/MIME v3 supports a wider variety and more secure set of encryption algorithms. The Cleo products support S/MIME v3; however, it is important to know which algorithms are supported by your trading partners before deciding upon the specific algorithms for both signing and encryption.

XML

XML Encryption and XML Signature are published recommendations of the World Wide Web Consortium (W3C). These recommendations define the syntax and processing rules for encrypting and signing data. Generally, the encrypted symmetric key is contained within the *EncryptedKey* element and the encrypted data is contained within the *EncryptedData* element. See http://www.w3.org/TR/xmlenc-core for detailed information regarding XML encryption. For digital signing, the *Signature* element is the primary element for encapsulating the digital signature. See http://www.w3.org/TR/xmldsig-core for detailed information regarding XML signatures.

OpenPGP

OpenPGP is a non-proprietary protocol for encrypting using public key cryptography. The OpenPGP protocol defines standard formats for encrypted messages, signatures, and certificates for exchanging public keys. See RFC 2440 for detailed information on the OpenPGP Message Format.

FIPS 140-3

The Federal Information Processing Standard (FIPS) 140-3 is a U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products. NIST oversees validation of modules for FIPS compliance. The FIPS edition of VersaLex provides a FIPS 140-3 compliant solution.

Note: FIPS 140-2 is being deprecated for the newer FIPS 140-3 standard. During this transition, FIPS 140-2 certifications are not being renewed.

Signing and encryption: general overview

In order to sign and/or encrypt a message, at least one public/private key pair is needed. The public key is provided to users who want secure communication. The sender's private key is used to digitally sign a message. When this message is received, the sender's public key is used to verify the digital signature in order to prove that the message originated with the sender.

For encryption, the sender uses the recipient's public key to encrypt the message. When the message is received, the recipient uses the recipient's own private key to decrypt the message. As long as the private key is protected and is accessible only by the originator, the recipient of a digitally signed message is able to confirm the originator of the message and both parties will be assured that the message has not been compromised.

Content integrity through digital signatures (signing)

Encryption guarantees the confidentiality of a data transaction. Content integrity guarantees that the receiving trading partner gets the data in its originally sent form, ensuring that no modifications have been made to the data when it is in transit between trading partners.

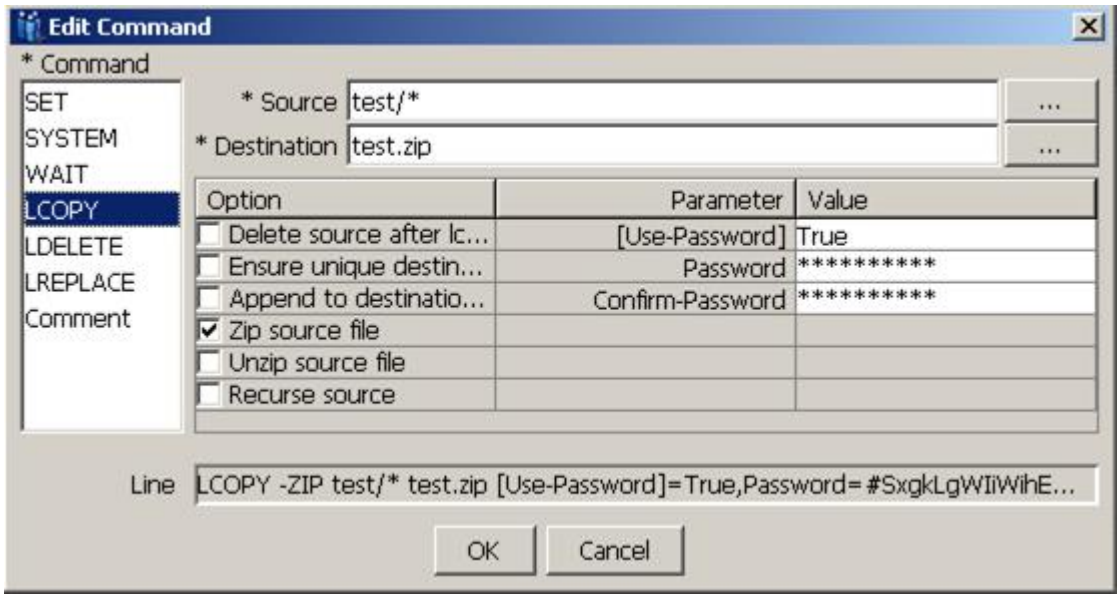
Content integrity is achieved if the sender provides a digital signature, which includes an integrity control value. This value can be computed by using an appropriate cryptographic algorithm to fingerprint the data content. These cryptographic algorithms are called one-way hash functions or message integrity checks. Unlike encryption algorithms, however, one-way hash functions cannot be reversed or decrypted. One-way hash functions are constructed such that the probability is infinitely small that some arbitrary piece of plain-text can be hashed to a particular value, or that any two pieces of plain-text can be hashed to the same value. One-way hash values are usually 112 bits or more. The longer the hash value, the more secure it is.

One-way hash functions do not require a key. Common hash algorithms are SHA-1 (Secure Hash Algorithm 1), which generates a hash value of 160 bits, MD5 (Message Digest 5) which generates a hash value of 112 bits, and SHA-2 (aka SHA-256), which generates a hash value of 256 bits. To determine content integrity, the sending trading

partner adds a digital signature to the data content, which includes a one-way hash value of the message. This value is unique and fingerprints the transaction. The sending trading partner sends the hash value along with the data. The receiving trading partner, using the same one-way hash function, calculates the hash value for the received data message content. If the received hash value matches the calculated hash value, then the receiving trading partner is assured that the data content has not been tampered with or altered in any way.

Encryption of zip files

Within the VersaLex `LCOPY` command, it is possible to encrypt and decrypt zip archive files according to the AES encryption standard (128-bit, 192-bit, and 256-bit). Refer to http://www.winzip.com/aes_info.htm for further information on the AES-encrypted ZIP files. To encrypt or decrypt, certain parameters must be specified on the `LCOPY` command. See the editor dialog for the `LCOPY` command.



The Use-Password parameter is optional. When this parameter is set to `True`, a password must be specified. The length of the password determines the strength of the AES encryption key. Passwords with a length less than 8 characters are invalid as they are too weak. Passwords with a length between 9 and 32 characters have a 128-bit key, which is the weakest. Passwors with a length from 33 to 48 characters have a 192-bit key, and passwords with a length from 49 to 64 characters have a 256-bit key, which is the strongest.

The security of your data depends not only on the strength of the encryption method but also on the strength of your password, including factors such as length and composition. There are also measures that you can take to ensure your password is not disclosed to unauthorized third parties. If you type in the `LCOPY` command directly from the freeform editor of the **Action** tab, any password data will be shown in clear-text. For highest security when typing your password use the editor dialog box (which will not echo the clear-text password); or enter the `LCOPY` command, double-click on the new command to display the editor dialog box, and then click **OK**. After you click **OK**, the password is encrypted and cannot be observed by unauthorized parties.

When using the freeform editor, if a password has an embedded space, you must use a `\s` to represent the space within the command. If you leave an embedded space in the password the command will not be parsed correctly. However, if you use the editor dialog box, embedded spaces are properly handled automatically. In general, when typing commands without using the editor dialog box, you must use special escape sequences to identify certain characters:

- `\s`: space
- `\t`: tab
- `\n`: newline
- `\r`: carriage return
- `\\`: slash

To disable zip file encryption, set the Use-Password parameter to `False` or leave the field empty.

Appendix

G

AS2 Checklist

1. Are you using a translator? □ Yes □ No

If "Yes", which one? _____

2. Do you have a firewall? □ Yes □ No

If "Yes", which one? _____

3. Are you using a proxy server? □ Yes □ No

If "Yes", what is the URL? _____

4. What is the URL of your remote trading partner (including the port)? _____

Note: the URL is in the form: **http(s)://host-ipaddress-or-name:port/optional-path?optional-parameters**

If ':port' is omitted, assume port 80 for HTTP and port 443 for HTTPs (SSL).

5. What is your AS2-Name? _____

(This is the unique AS2 identifier for this trading relationship.)

6. What is your remote trading partner's AS2-Name? _____

7. Will you be using the same certificate for both signing and encryption? □ Yes □ No

8. Have you created or obtained certificates for signing and encryption? □ Yes □ No

If "Yes", have you exchanged the certificate(s) with your remote trading partner? □ Yes □ No

9. Will any of your remote trading partners be using SSL? □ Yes □ No

If "Yes", do you have an SSL server-style certificate? □ Yes □ No

If "Yes", have you exchanged this certificate with your remote trading partner? □ Yes □ No

10. What is the email address of the contact person at your location who will be responsible for AS2 message administration?

11. What is the IP address or host name where your AS2 VersaLex product is installed?

12. What ports would you like to use for receiving messages from your remote trading partners?

Cleo suggests using port 5080 for HTTP and port 5443 for HTTPs but any unused ports between 0 - 65535 may be used.

HTTP: _____ HTTPs: _____ *

(*only needed if the answer to Question #9 was "Yes")

13. Will the content of the messages you will be sending to your remote trading partners be:

□ signed?

□ encrypted?

If selected, can your remote trading partner accept 3DES (Triple DES) encryption?

□ Yes □ No

□ compressed?

14. What type of content will you primarily be sending?

□ EDI - X12

□ EDIFACT

□ XML

□ Binary

□ Plain Text

15. Will you be requesting MDNs (receipts) from your remote trading partner? □ Yes □ No

If "No", skip the remaining questions.

16. Will the MDNs be signed? □ Yes □ No

17. How will the MDNs be returned? □ Synchronously □ Asynchronously

If "Asynchronously", what preferred transport method will you use to receive them?

□ HTTP

□ HTTPs

□ SMTP Email address of the recipient _____

18. Would you like to forward non-SMTP MDNs to an email recipient? □ Yes □ No

If "Yes", what is the email address of the recipient? _____

What is the name of your mail server (optional)? _____

AS/400 Network Access Setup

Use this guide to configure VersaLex on a Windows PC and map to the AS/400 through a networked drive.

AS/400 Network Access overview

AS/400 Network Access is an add-on feature available to those that have purchased it. If you did not purchase AS/400 Network Access, but need this functionality, contact your Cleo sales representative.

The AS/400 is also known as the “iSeries”, “System I” or "IBM i", but will continue to be referred to generically throughout this document as the “AS/400” however “iSeries”, “System i” or "IBM i" may be used interchangeably.

AS/400 Network Access enables VersaLex to read and write directly from the AS/400 native (QSYS.LIB) file system, allowing for seamless conversion of the data between EBCDIC and ASCII formats. Using AS/400 Network Access, AS/400 native files can be read or written by VersaLex, running under either the Windows or Unix platform. For additional information on installing VersaLex on either of these platforms, refer to the VersaLex User's Guide, which be found on the Cleo web site at http://www.cleo.com/Lexicomdoc, http://www.cleo.com/VLTraderdoc, or http://www.cleo.com/Harmonydoc

Network Access process map

The following are the tasks that you must perform in order to successfully access files on a AS/400 server accessible through your network.

- ☐ Configure VersaLex for AS/400 Network Access
- ☐ Select the Native AS/400 Inbound/Outbound Directory Paths
- ☐ Create Inbound and Outbound Files
- ☐ Create Links in VersaLex for the Inbound and Outbound Files
- ☐ Define a Default File Member (AS2 only)
- ☐ Configure AS/400 Mapped Drives for Text Conversion (Windows only)

Configuring AS/400 Network Access

Follow the instructions below to configure the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application to access files on the AS/400.

On the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom menu bar, select **Configure** > **AS/400**.

The following display panel will appear:

In the top portion of the panel:

Select the **Enable AS/400 network access** check box

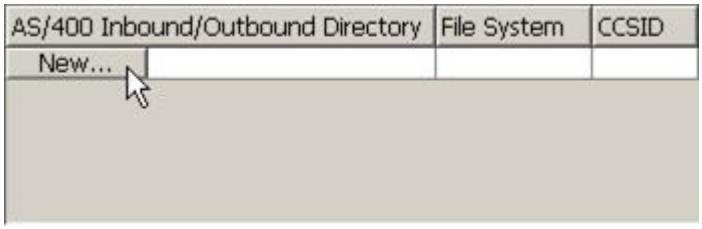
In the **Address** field, enter the IP address of the remote AS/400

In the **User ID** and **Password** fields, enter a valid user ID / password on the remote AS/400. Use [**Validate Login**] to verify the entries. This user must have at least "All Object Access" system privilege if accessing native files that are not owned by this user.

Selecting the AS/400 Inbound/Outbound Directory paths

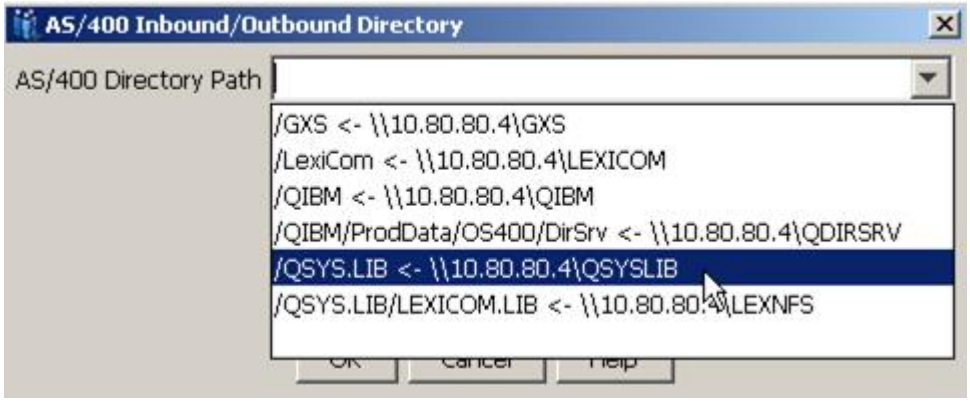
Follow these steps to add an AS/400 directory path to the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom configuration. Repeat this process for each additional directory path:

1. In the lower portion of the AS/400 Configuration panel, click the **New** button as shown:



2. A display similar to the following will appear. Click on the down arrow to get a list of all AS/400 mapped file shares in your network:

3. If you have mapped AS/400 file shares, a display similar to the following will be shown:



4. Select the desired mapped file share, if one exists. Otherwise, enter the desired path in the **AS/400 Directory Path** field (for example, /QSYS.LIB for Native File System access or /LexiCom for Integrated File System access).
5. Select the appropriate file system option, i.e., either **Native File System** or **Integrated File System**.
6. If the **Integrated File System** option is selected, enter the appropriate **Coded Character Set ID** value, if provided by your trading partner. If this field is left blank, the CCSID value based on the default locale will be used.
7. If the **Native File System** option is selected, select the **Pad Inbound to Record Length** option if inbound files will contain variable length records.

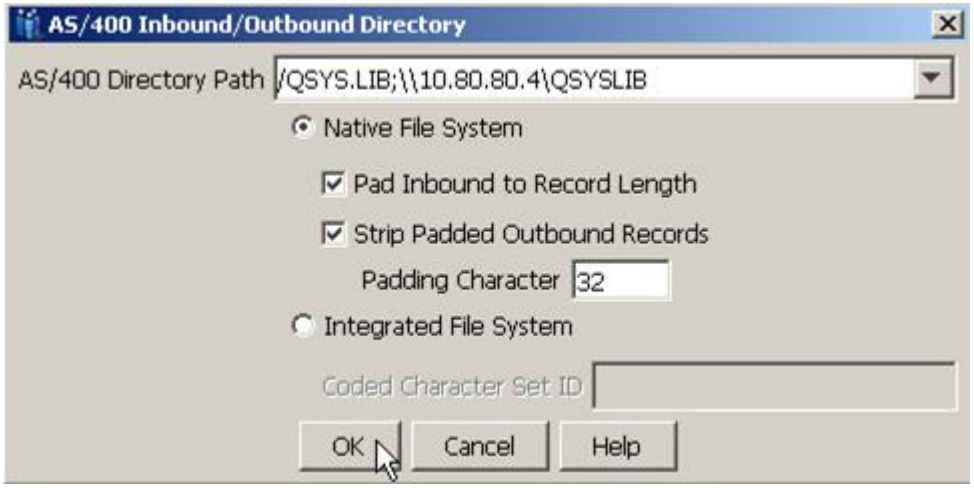
   When this option is selected, all records are transformed to a fixed-length format as they are stored in the AS/400 NFS file member. End of line terminators (that is, CR, LF or CRLF) are stripped from the record and the remainder of the record is padded with blanks. The record length is determined from the AS/400 target file. If

the inbound file contains a record larger than the AS/400 target file, an error will be logged and the file will not be stored. When this option is not selected, the inbound file will be assumed to already be fixed-length and will be streamed, i.e., no padding will be done to the records as they are written to the AS400 NFS file member and end of line terminators will not be stripped from the file.

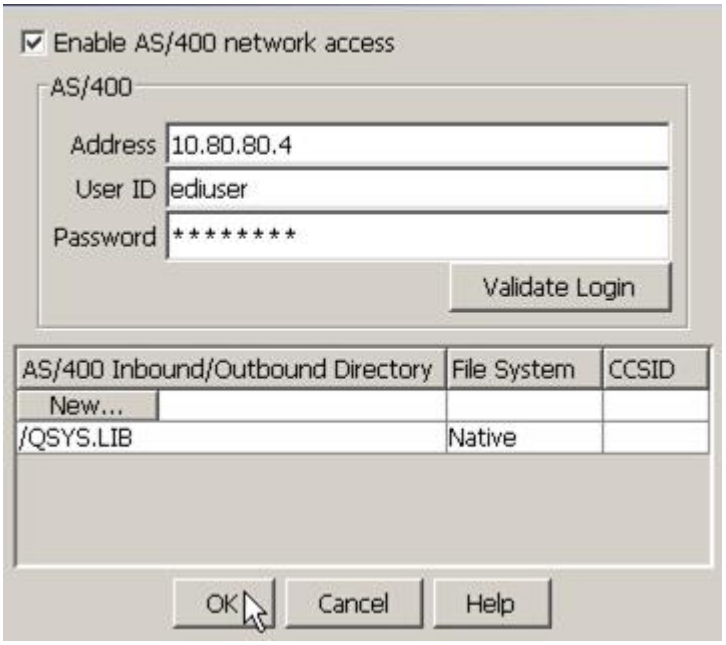
8. Select the **Strip Padded Outbound Records** option if outbound records are a fixed record length and are padded with the specified Padding Character. The record length is determined from the AS/400 NFS target file. When this option is selected, padding characters after the terminator (CR, LF or CRLF) will be removed.

   The **Padding Character** is the decimal value of the character used in AS/400 target file for padding outbound records. By default, this value is set to 32 (the ASCII representation of a space). Any ASCII value between 0 – 127 can be used.

9. The updated display should look similar to the one that follows. Click **OK**.



10. The updated AS/400 Configuration panel will now be displayed similar to the one below. Click **OK**.



Creating Inbound and Outbound native files

Note: This section is only applicable to users who will be writing to the Native File System. If you are writing to the Integrated File System, you can skip this section.

Before you can successfully read and write AS/400 native files, they must be created using the following AS/400 CL commands. In this example, we have created a LEXICOM library where the INBOUND, OUTBOUND and SENTMSG files will reside:

```
CRTPF FILE(LEXICOM/INBOUND) RCDLEN(132) MAXMBRS(*NOMAX) SIZE(*NOMAX)
```

```
CRTPF FILE(LEXICOM/OUTBOUND) RCDLEN(132) MAXMBRS(*NOMAX) SIZE(*NOMAX)
```

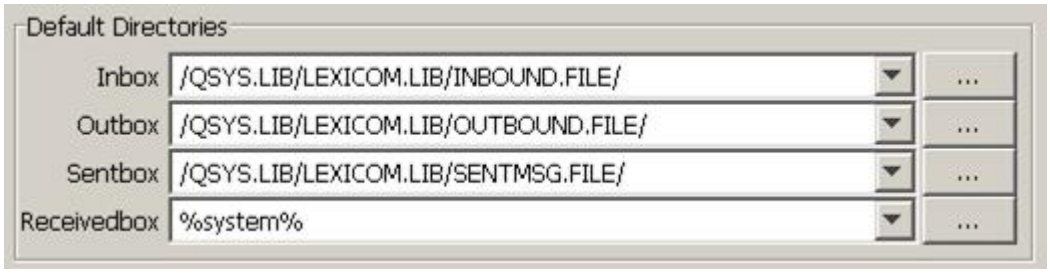
```
CRTPF FILE(LEXICOM/SENTMSG) RCDLEN(132) MAXMBRS(*NOMAX) SIZE(*NOMAX)
```

Note: Inbox, Outbox, and Sentbox (optional) are the only local directories that can be "mapped" to the AS/400 native file system. *Do not attempt to map the MDN or certs directory to the AS/400 native file system!*

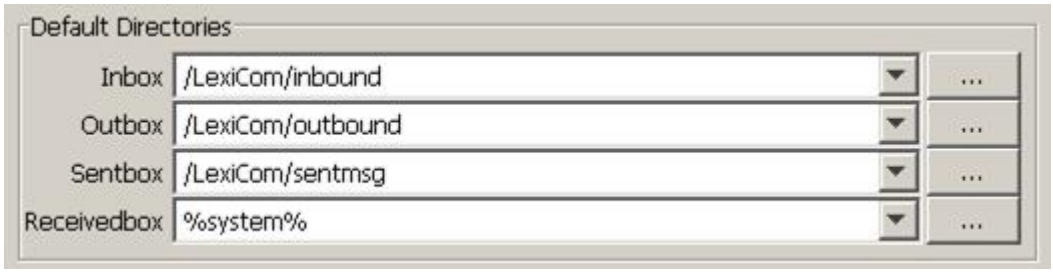
Creating links for the Inbound and Outbound files

The next step is to link the INBOUND and OUTBOUND (and optionally the SENTBOX) files that were created in the previous section with the "Inbox", "Outbox" and "Sentbox" in VersaLex. To do this, on the General panel at the Host level, enter the "Inbox", "Outbox" and optionally "Sentbox" entries, as shown below:

NFS Access Example



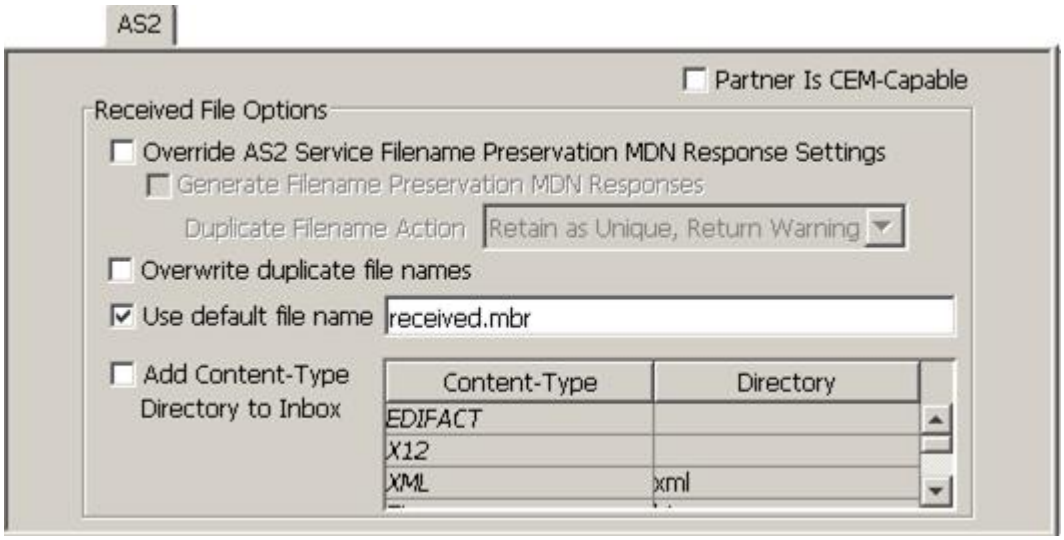
IFS Access Example



Defining a default file member (AS2 only)

If you are using AS2, in most cases you will need to define a default file name where the received entries will be stored. An AS/400 file *must* be specified in the form: /QSYS.LIB/LIBRARY.LIB/OBJECT.FILE/FILE.MBR.

To accommodate this format requirement, on the **Host** > **AS2** panel, add a file with a `.mbr` extension, as illustrated below:



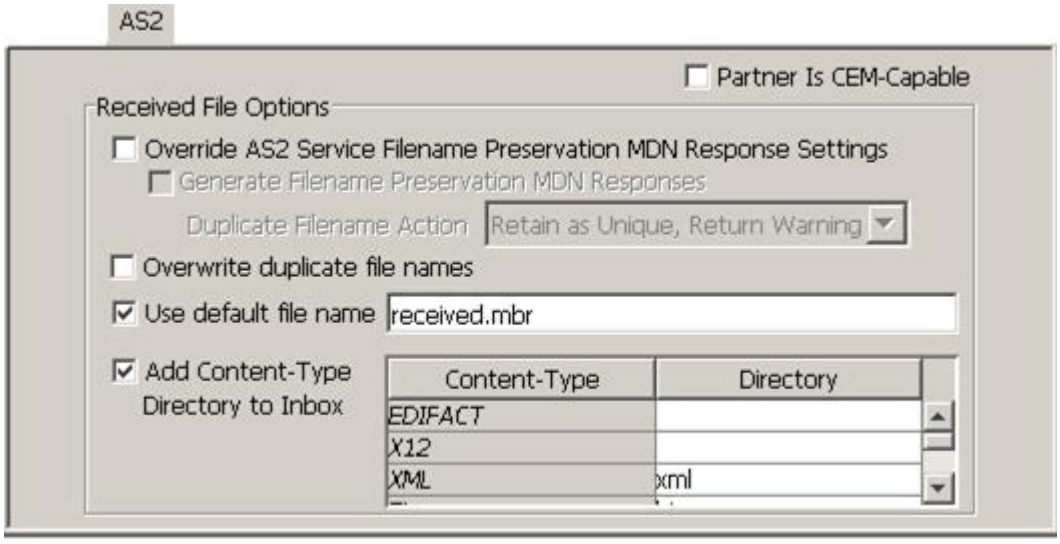
Defining an Authorization List

If objects defined in the /LexiCom IFS or NFS directory need to be accessed but are not owned by the user that originally created them, **Authorization Lists** can be used to allow users read and write access rights to specified IFS folders or NFS libraries and files. (If a user is not included in the Authorization List, then the *PUBLIC authority assigned to the particular IFS or NFS directory will apply *and will override the read/write authority originally assigned to the network access file share*.) If read and/or write access is not properly assigned to users that will be reading and writing in the NFS directories, LexiCom will log errors that access to the request was denied. See AS/400 Setup and installation on page 703 for information about creating and using Authorizations Lists for installing and configuring your AS/400 system.

Configuring content-type inboxing for the Native File System (AS2 only)

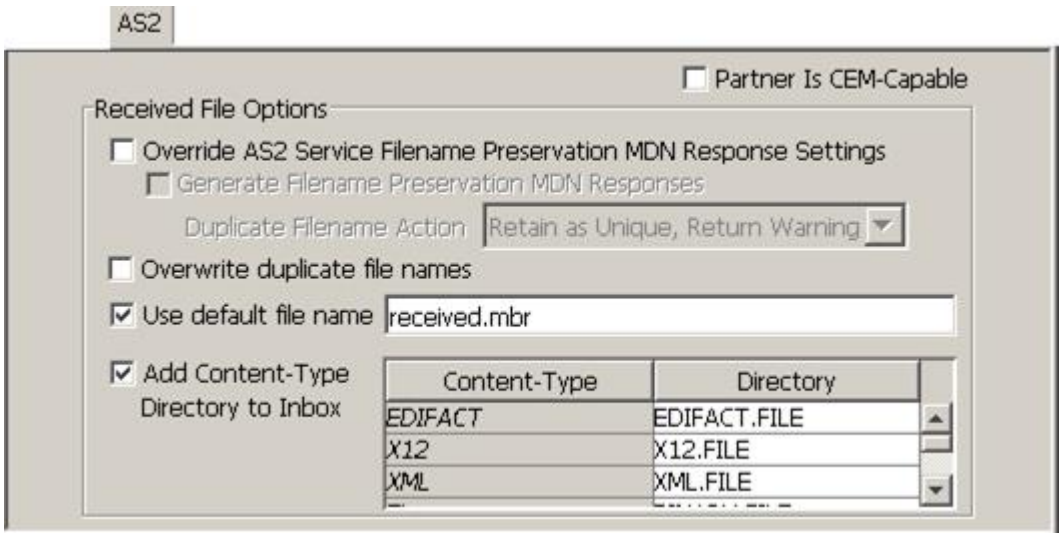
The **Add Content-Type Directory to Inbox** checkbox allows for sorting of incoming messages based on the content-type of the message to a subdirectory (under the *Inbox* specified on the General tab for the Host). You specify each of the content-types that you want directed to specified subdirectories by entering a name in the **Directory** field. Directory entries may be made for content-types of: EDIFACT, X12, XML, Binary, Plain Text, and Other (a default catch-all for messages with all other content-types you may receive.) The same subdirectory may be used for multiple content-types. You may also leave 'Directory' entries blank which will cause any received messages for that specific 'Content-Type' to be stored in the Inbox specified on the General tab.

Note: If you use this feature, incoming messages will be placed in the specified folder *based on the content type specified in the HTTP header of the message*. VersaLex does not check the actual content of the message to determine its content type.

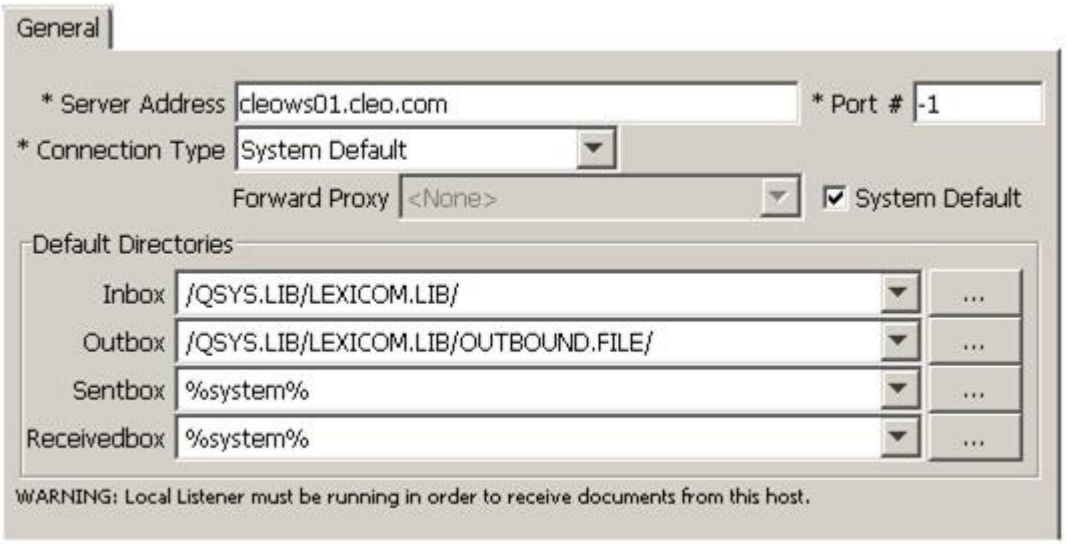


Note: If you are integrated with a translator, you should not add entries for the X12 or EDIFACT directories. These directories must remain blank in order for translator integration to work properly.

By default, the Content-Type directories are preconfigured for windows or IFS based folders. To use this feature on the AS/400 Native File System, modifications must be made to all directories that will be used so that the settings have the correct AS/400 syntax, i.e., each setting must be in the form DIRECTORY.FILE, for example:



On the 'General' tab, specify just the library for the "Inbox" value where the "Content-Type" files will be created. In this example, we have used /QSYS.LIB/LEXICOM.LIB/:



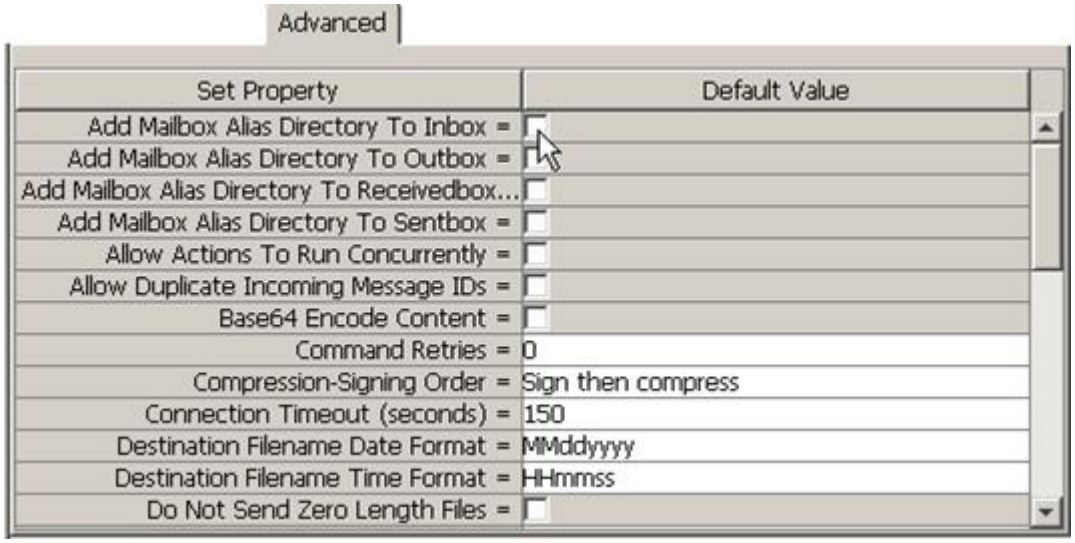
Now verify that all the "directories" that you have specified, i.e., files in the form DIRECTORY.FILE, have a matching physical file defined. In the example above, the files EDIFACT.FILE, X12.FILE and XML.FILE under the /QSYS.LIB/LEXICOM.LIB library are being used. If these files don't already exist, create a physical file for each of the files you have specified as follows:

```
CRTPF FILE(LEXICOM/EDIFACT) RCDLEN(132) MAXMBRS(*NOMAX) SIZE(*NOMAX)
```

```
CRTPF FILE(LEXICOM/X12) RCDLEN(132) MAXMBRS(*NOMAX) SIZE(*NOMAX)
```

```
CRTPF FILE(LEXICOM/XML) RCDLEN(132) MAXMBRS(*NOMAX) SIZE(*NOMAX)
```

As a final step, verify that the **Add Mailbox Alias Directory To Inbox** setting on the Advanced panel is not selected:

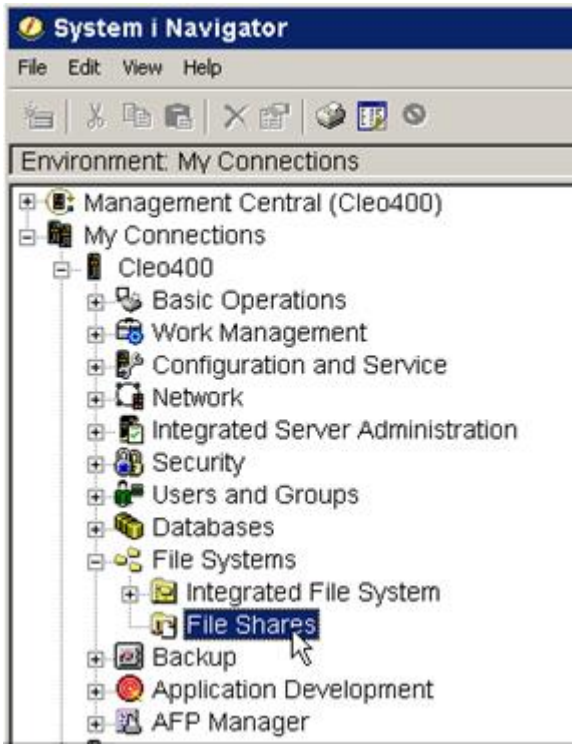


Configuring AS/400 mapped drives for text conversion (Windows only)

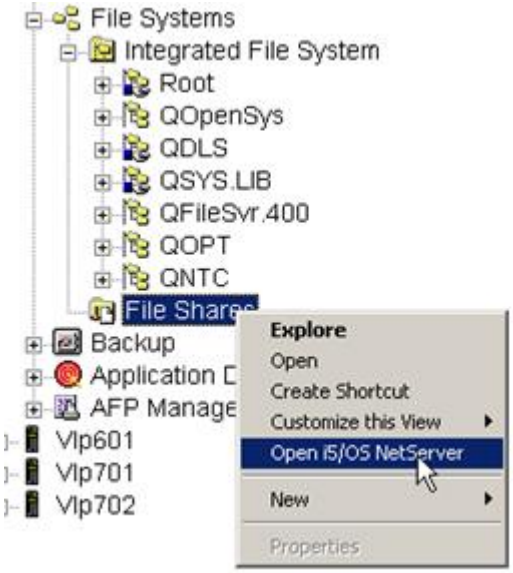
Through *IBM i Client Access for Windows*, you can map an AS/400 file share with a Windows network drive and view its contents through Windows Explorer. By default, the contents of AS/400 files are stored in EBCDIC, which cannot be viewed through Windows.

To allow automatic conversion of your files to ASCII format, follow this simple procedure:

1. Open *System i Navigator* and select the **File Shares** item:

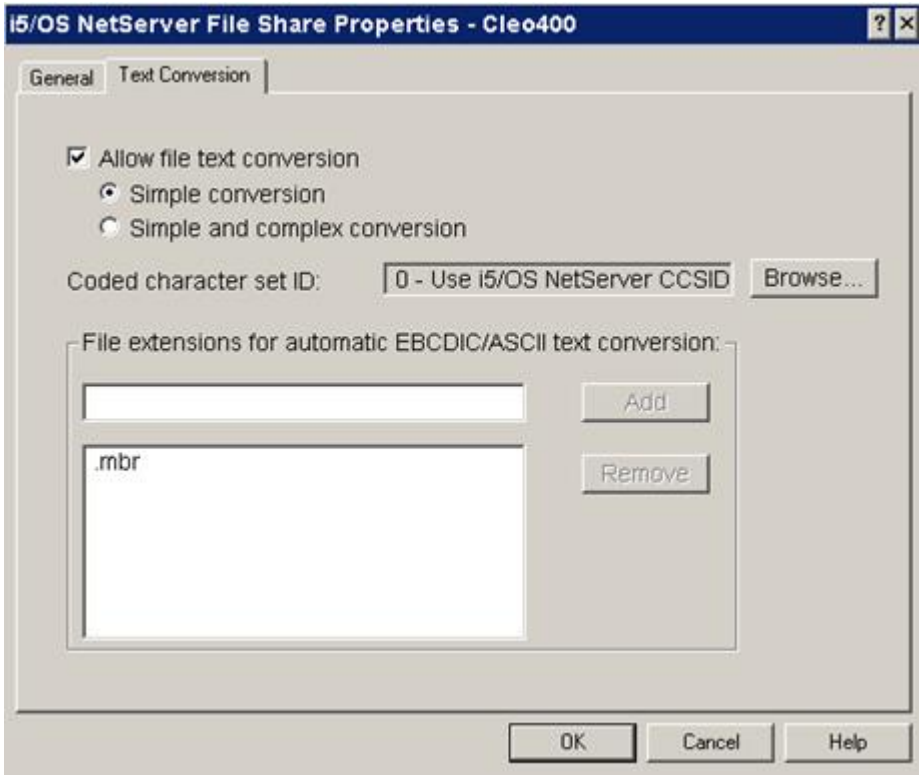


2. Right-click the **File Shares** item and select the **Open i5/OS NetServer** option:



3. Right-click the file share that you have mapped into Windows and select **Properties** option:

4. Select the **Allow file text conversion** checkbox and add the file extensions of all files that you will be viewing through Windows. In the example below, all `.mbr` files will automatically be converted:


i5/OS NetServer File Share Properties - Cleo400
General
Text Conversion
Allow file text conversion
Simple conversion
Simple and complex conversion
Coded character set ID:
0 - Use i5/OS NetServer CCSID
Browse...
File extensions for automatic EBCDIC/ASCII text conversion:
Add
.mbr
Remove
OK
Cancel
Help

Appendix

H

Database Definitions

The JDBC ODBC driver is the only JDBC driver that comes built into Cleo Harmony, Cleo VLTrader, and Cleo LexiCom. If you want to use any other driver, you must acquire it from the vendor and place the jars in the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom `lib/ext` directory.

Note: The driver jars must be placed in the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom `lib/ext` directory and **not** the `jre/lib/ext` directory.

Note: Whenever you place a new driver jar in the `lib/ext` directory, you must restart the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom software.

Driver and connection strings

This topic contains sample driver and connection strings for connecting to a database from the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application.

ODBC

ODBC data sources are generally configured with an ODBC data source administration tool, for example, in the System DSN tab of **Start** > **Control Panel** > **Administrative Tools** > **Data Sources (ODBC)**. See the appropriate database/operating system documentation for further details.

Note: Appropriate ODBC configuration is required for each computer that will access the transfer database using Cleo Harmony, Cleo VLTrader, or Cleo LexiCom.

Driver String

```
sun.jdbc.odbc.JdbcOdbcDriver
```

Connect String

```
jdbc:odbc:odbcname
```

MS Access database

Driver String

```
sun.jdbc.odbc.JdbcOdbcDriver
```

Example Connect String

```
jdbc:odbc:Driver={Microsoft Access Driver (*.mdb)};DBQ=//fi lesvr/
sharename/db/vltdb.mdb
```

MySQL Connector/J

Driver String

```
com.mysql.jdbc.Driver
```

Connect String

```
jdbc:mysql://[host][,failoverhost...][:port]/
[database][?propertyName1][=propertyValue1][&propertyName2]
[=propertyValue2]...
```

Example Connect String

```
jdbc:mysql://myhost:3306/vltdb
```

Note: For older versions of the MySQL driver the connection string was:

```
jdbc:mysql://myhost:3306/vltdb/
```

Microsoft SQL Server

Driver String

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

Connect String

```
jdbc:sqlserver://[host]:[port];databaseName=[database];
selectMethod=[selectmethod];
sendStringParametersAsUnicode=[sendStringParametersAsUnicode]
```

Example Connect String

```
jdbc:sqlserver://myhost:1433;databasename=vltdb
```

Example Connect String (with Windows Authentication):

```
jdbc:sqlserver://myhost:1433;databasename=vltdb;integratedSecurity=true
```

Note: For Windows Authentication, choose the appropriate x64 or x86 .dll file from the MSSQL JDBC connection archive (for example, `/sqljdbc_13.4/enu/auth/x64/mssql-jdbc_auth-13.4.0.x64.dll`) for your database and platform and place it in the `.../VersaLex` directory. Restart VersaLex to apply the change.

Oracle

Driver String

```
oracle.jdbc.driver.OracleDriver
```

Connect String

```
jdbc:oracle:<drivertype>:@<database>
```

Example Connect String

```
jdbc:oracle:thin:@myhost:1521:vltdb
```

IBM DB2

Driver String

```
com.ibm.db2.jcc.DB2Driver
```

Connect String

```
jdbc:db2://[host]:[port]/database
```

Example Connect String

```
jdbc:db2://myhost:50000/vltdb
```

PostgreSQL

Driver String

```
org.postgresql.Driver
```

Connect String

```
jdbc:postgresql://[host]:[port]/database
```

Example Connect String

```
jdbc:postgresql://myhost:5432/vltdb
```

Transfer database fields

When the transfer feature is enabled for a relational database, the Cleo Harmony, , or application automatically creates a set of database tables. The user specified for the database connection must have privileges to create tables and triggers.

Transfer log

This topic contains a description of the fields used for the transfer log database feature. The same fields appear in the database columns and the XML file, depending on how you store the data.

VLTransfers database table or logs/xferYYYYMMDD.xml XML file

Column/Field Name	Data Type	Length	Description
TransferID	VARCHAR	30	**Database only** Transfer ID (generated by Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application and used as a "key" to the records)
ExternalID	VARCHAR	50	Optional external ID provided by end user application
MessageID	VARCHAR	100	Message ID (generated either by Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application or the remote host)
Folder	VARCHAR	50	**Database only** Host folder alias
Host	VARCHAR	50	Host Alias
Mailbox	VARCHAR	50	Mailbox Alias
MailboxID	VARCHAR	255	**Database only** Optional identifier set via mailbox `externalID` property.

Column/Field Name	Data Type	Length	Description
Username	VARCHAR	50	**Database only** Name of user performing the transfer. If it matches the Mailbox, then this is null.
Action	VARCHAR	50	Action Alias
Transport	VARCHAR	12	Transport
StartDT	VARCHAR	20	Start Date and Time the file transfer started Format: `yyyy/mm/dd hh:mm:ss`
EndDT	VARCHAR	20	End Date and Time the file transfer completed Format: `yyyy/mm/dd hh:mm:ss`
Direction	VARCHAR	10	Direction Possible values include send or receive, or inbound or outbound for `CHECK` commands
IsReceipt	VARCHAR	1	Receipt file Possible values: `T`=True; `F`=False

Column/Field Name	Data Type	Length	Description

Status	VARCHAR	15	Status
			
			Possible values:
			
			`In Progress`
			`Receipt Pending`
			`Interim Success`*****
			`Interim Warning`*****
			`Delete Error`
			`Delete Resolved`
			`Success`
			`Warning`
			`Discarded`
			`Error`
			`Exception`
			`Interrupted`
			
			*** Database payload only**: A status of `Interim Success` when using database payload indicates that the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom FTP or SSH FTP server received a file, but it was not stored by the FTP user into the user's configured inbox subdirectory. Another transfer will be logged with a status of `Success` if and when the file is moved into the inbox directory by the FTP user via FTP rename commands. In fact, when the file is renamed by the FTP user, the payload is actually inserted into the `VLIncoming` database table at that time. See Database payload on page 1009 for more information on the database payload feature.

OrigName	VARCHAR	100	Original filename If the file is a zip archive, this field contains `zip filename[entry name]`
OrigPath	VARCHAR	200	Original path
OrigFileDT	VARCHAR	20	Original file date/time stamp Format: `yyyy/mm/dd hh:mm:ss`
FileSize	BIGINT		File size
TransferTime	FLOAT	20	Transfer time in seconds
TransferBytes	BIGINT		Transfer bytes
CRC	VARCHAR	12	**Database only** CRC-32 value associated with the transfer, or NULL if CRC is not available

Column/Field Name	Data Type	Length	Description
ResultText	VARCHAR	500	Result text
FileHeader	VARCHAR	100	File Header (future use)
VLSerial	VARCHAR	6	**Database only** Cleo Harmony, Cleo VLTrader, or Cleo LexiCom license serial number (in case multiple product instances sharing database)
CopyPath	VARCHAR	500	**Database only** Contains the path to the `sentbox/receivedbox` copy or NULL if a copy is not available.
RunType	VARCHAR	30	**Database only** Contains the run type (for example, `Interactive`, `Scheduled`, `Unsolicited`, and so on) or NULL if the run type is not available.
PreviousTransferID	VARCHAR	30	**Database only** If RunType = `Resend`, contains the transfer ID of the transfer on which this transfer was based. Otherwise, it is NULL.
Command	VARCHAR	500	**Database only** The original command string. Only present for `CHECK` commands.
InteractiveUsername	VARCHAR	50	**Database only** Name of user running the action interactively.
StartNDT	DATETIME		**Database only** DateTime version of StartDT
EndNDT	DATETIME		**Database only** DateTime version of EndDT
TradingPartnerAlias	VARCHAR	255	**Database only** Alias of trading partner associated to the host/mailbox or to the ID if tracking is enabled.
FileType	VARCHAR	255	**Database only** File extension of transferred file

Column/Field Name	Data Type	Length	Description
TrackedType	VARCHAR	25	**Database only** If the file is tracked, this is the tracked type. Possible values are `EDI`, `TEXT`, or `XML`.
IPAddress	VARCHAR	45	**Database only** IP Address of remote computer used for local user IP filtering.
StartDTInt	BIGINT		Milliseconds epoch version of `StartDT`
EndDTInt	BIGINT		Milliseconds epoch version of `EndDT`

External transfers

For both database and XML transfer logging, transfers outside the direct control of the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom application can also be logged by dropping XML files into the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom `logs\autoxfer\` directory. One XML file represents a send start or complete, a receive start or complete, or transfer in-process. Files must conform to Cleo's `webserver\WEB-INF\schemas\autoxfer.xsd` schema.

In addition to the XML schema where the `<Transferid>` and `<Status>` elements are always required, the following are also required:

- For `method=sendStart` or `receiveStart`:
  - `<Startdt>`, `<Transport>`, `<Host>`, and `<Mailbox>` are required
- For `method=transferInProcess`:
  - `<Transferbytes>` and `<Transfertime>` are required
- For `method=sendComplete` or `receiveComplete`:
  - `<Enddt>`, `<Resulttext>`, `<Transferbytes>`, and `<Transfertime>` are required
  - `<Startdt>` is also required if XML logging is in use (in order to find the XML file, which are per day)

The XML files are processed sequentially in sorted order, usually within a second. For a given transfer, the sorted order of the files must match the chronological order of a transfer - the transfer-start XML file first, any transfer-in-process XML files (if any are used) next, and the transfer-complete XML file last.

EDI tracking fields

Optionally, when logging to a database, EDI files can be detected and supplementary header information logged along with the transfer. You can configure which data is logged. See Transfers on page 895 and File tracking on page 896. Text fields are sized for the maximum values; invariably UN/EDIFACT and TRADACOMS allow for longer values than EDI-X12.

VLEDIInterchange database table

Column Name	Data Type	Length	Description		
			EDI-X12	**UN/EDIFACT**	**TRADACOMS**
TransferID	VARCHAR	30	*TransferID* in VLTransfers table		
VLSerial	VARCHAR	6	*VLSerial* in VLTransfers table		

Column Name	Data Type	Length	Description		
			EDI-X12	UN/EDIFACT	TRADACOMS
isX12	BIT		On	Off	Off
isEDIFACT	BIT		Off	On	Off
isTRADACOMS	BIT		Off	Off	On
Interchange	INTEGER		ISA count in file	UNB count in file	STX count in file
Sender	VARCHAR	35	ISA06	UNB02:1	STX02:1
SenderQualifier	VARCHAR	4	ISA05	UNB02:2	n/a
Receiver	VARCHAR	35	ISA08	UNB03:1	STX03:1
ReceiverQualifier	VARCHAR	4	ISA07	UNB03:2	n/a
InterchangeDT	DATETIME		ISA09 + ISA10	UNB04:1 + UNB04:2	STX04:1 + STX04:2
ControlNum	VARCHAR	14	ISA13	UNB05	STX05
TradingPartnerAlias	VARCHAR	255	Alias of trading partner associated with the Interchange ID.		

VLEDIFunctionalGroup database table

Column Name	Data Type	Length	Description		
			EDI-X12	UN/EDIFACT	TRADACOMS
TransferID	VARCHAR	30	*TransferID* in VLTransfers table		
VLSerial	VARCHAR	6	*VLSerial* in VLTransfers table		
Interchange	INTEGER		*Interchange* in VLEDIInterchange table		
FunctionalGroup	INTEGER		GS count in file	UNG count in file	BAT count in file
FunctionCode	VARCHAR	6	GS01	UNG01	n/a
AppSender	VARCHAR	35	GS02	UNG02:1	n/a
SenderQualifier	VARCHAR	4	n/a	UNG02:2	n/a
AppReceiver	VARCHAR	35	GS03	UNG03:1	n/a
ReceiverQualifier	VARCHAR	4	n/a	UNG03:2	n/a
GroupDT	DATETIME		GS04 + GS05	UNG04:1 + UNG04:2	n/a
ControlNum	VARCHAR	14	GS06	UNG05	BAT01

VLEDITransactionSet database table

Column Name	Data Type	Length	Description		
			EDI-X12	UN/EDIFACT	TRADACOMS
TransferID	VARCHAR	30	*TransferID* in VLTransfers table		
VLSerial	VARCHAR	6	*VLSerial* in VLTransfers table		
Interchange	INTEGER		*Interchange* in VLEDIInterchange table		
FunctionalGroup	INTEGER		*FunctionalGroup* in VLEDIFunctionalGroup table		
TransactionSet	INTEGER		ST count in file	UNH count in file	MHD count in file

Column Name	Data Type	Length	Description		
			EDI-X12	**UN/EDIFACT**	**TRADACOMS**
MessageType	VARCHAR	6	n/a	n/a	MHD02
TransactionType	VARCHAR	6	ST01	UNH02	TYP01
ControlNum	VARCHAR	14	ST02	UNH01	MHD01
DataSegment Count	INTEGER		SE01*	UNT01*	MTR01*
			* decremented by 2 because count includes the header and trailer segments		
Ref1	VARCHAR	500	Custom transaction data segment element reference number		
Ref2	VARCHAR	500	Custom transaction additional data segment element reference number(s), separated by commas		
AckStatus	VARCHAR	3	Transaction functional acknowledgment status: • If the transaction itself is an acknowledgment (EDI-X12 997 or UN/EDIFACT CONTRL), set to '-' to indicate not applicable. • Otherwise initially set to '*' while acknowledgment is pending. Once functional acknowledgment sent or received for this transaction, pending status code is updated.		
			A = accepted E = accepted, with errors M = rejected MAC failed P = partially accepted R = rejected X = rejected, after decryption	1 = acknowledged, all levels 2 = acknowledged, with errors 3 = one or more rejected 4 = rejected 5 = UNB/UNZ accepted 6 = UNB/UNZ rejected 7 = acknowledged, this level 8 = interchange received	- = not applicable
AckIControlNum	VARCHAR	14	Initially NULL. Once functional acknowledgment sent or received for this transaction, set to interchange control number of functional acknowledgment.		
TransactionDesc	VARCHAR	255	Textual description of this transaction. For example, "Purchase Order" will be stored for a transaction type of 850.		

VLEDIInterchange database table

Column Name	Data Type	Length	Description		
			EDI-X12	**UN/EDIFACT**	**TRADACOMS**
TransferID	VARCHAR	30	*TransferID* in VLTransfers table		
VLSerial	VARCHAR	6	*VLSerial* in VLTransfers table		
isX12	BIT		On	Off	Off
isEDIFACT	BIT		Off	On	Off
isTRADACOMS	BIT		Off	Off	On

Column Name	Data Type	Length	Description		
			EDI-X12	UN/EDIFACT	TRADACOMS
Interchange	INTEGER		ISA count in file	UNB count in file	STX count in file
Sender	VARCHAR	35	ISA06	UNB02:1	STX02:1
SenderQualifier	VARCHAR	4	ISA05	UNB02:2	n/a
Receiver	VARCHAR	35	ISA08	UNB03:1	STX03:1
ReceiverQualifier	VARCHAR	4	ISA07	UNB03:2	n/a
InterchangeDT	DATETIME		ISA09 + ISA10	UNB04:1 + UNB04:2	STX04:1 + STX04:2
ControlNum	VARCHAR	14	ISA13	UNB05	STX05
TradingPartnerAlias	VARCHAR	255	Alias of trading partner associated to the Interchange ID.		

VLEDIFunctionalGroup database table

Column Name	Data Type	Length	Description		
			EDI-X12	UN/EDIFACT	TRADACOMS
TransferID	VARCHAR	30	*TransferID* in VLTransfers table		
VLSerial	VARCHAR	6	*VLSerial* in VLTransfers table		
Interchange	INTEGER		*Interchange* in VLEDIInterchange table		
FunctionalGroup	INTEGER		GS count in file	UNG count in file	BAT count in file
FunctionCode	VARCHAR	6	GS01	UNG01	n/a
AppSender	VARCHAR	35	GS02	UNG02:1	n/a
SenderQualifier	VARCHAR	4	n/a	UNG02:2	n/a
AppReceiver	VARCHAR	35	GS03	UNG03:1	n/a
ReceiverQualifier	VARCHAR	4	n/a	UNG03:2	n/a
GroupDT	DATETIME		GS04 + GS05	UNG04:1 + UNG04:2	n/a
ControlNum	VARCHAR	14	GS06	UNG05	BAT01

XML tracking fields

Optionally, when logging to a database, XML files can be detected and supplementary information can be logged along with the transfer. You can configure which data is logged. See Transfers on page 895 and File tracking on page 896. XPath format is used to describe the path to the XML elements to be extracted. The table described below is used to store the extracted XML elements.

VLXMLExtractedData database table

Column Name	Data Type	Length	Description
TransferID	VARCHAR	30	*TransferID* in `VLTransfers` table
VLSerial	VARCHAR	6	*VLSerial* in `VLTransfers` table

Column Name	Data Type	Length	Description
SetID	INTEGER		Index used for multiple sets of extracted data for the same *TransferID*
SenderID	VARCHAR	255	Extracted sender identifier
ReceiverID	VARCHAR	255	Extracted receiver identifier
DocumentID	VARCHAR	255	Extracted document identifier
DocumentType	VARCHAR	255	Extracted document type
DocumentDateTime	VARCHAR	255	Extracted document date/time string
Ref1	VARCHAR	500	Custom reference information
Ref2	VARCHAR	500	Additional custom reference information
TradingPartnerAlias	VARCHAR	255	Alias of trading partner associated to the ID.

Text tracking fields

Optionally, when logging to a database, Text files can be detected and supplementary information can be logged along with the transfer. You can configure which data is logged. See Transfers on page 895 and File tracking on page 896. Data can be extracted based on column number or field numbers. The following table is used to store the extracted text strings.

VLXMLExtractedData database table

Column Name	Data Type	Length	Description
TransferID	VARCHAR	30	*TransferID* in `VLTransfers` table
VLSerial	VARCHAR	6	*VLSerial* in `VLTransfers` table
SetID	INTEGER		Index used for multiple sets of extracted data for the same *TransferID*
SenderID	VARCHAR	255	Extracted sender identifier
ReceiverID	VARCHAR	255	Extracted receiver identifier
DocumentID	VARCHAR	255	Extracted document identifier
DocumentType	VARCHAR	255	Extracted document type
DocumentDateTime	VARCHAR	255	Extracted document date/time string
Ref1	VARCHAR	500	Custom reference information
Ref2	VARCHAR	500	Additional custom reference information
TradingPartnerAlias	VARCHAR	255	Alias of trading partner associated to the ID.

Supplemental tracking fields

When logging tracking data to a database, summary data is also stored in the `VLTracked` table. This table contains data for all tracking types: EDI, XML, and Text.

VLTracked database table

Column/Field Name	Data Type	Length	Source
TransferID	VARCHAR	30	*VLEDIInterchange.TransferID* *VLXMLExtractedData.TransferID* *VLTextExtractedData.TransferID*
VLSerial	VARCHAR	6	*VLEDIInterchange.VLSerial* *VLXMLExtractedData.VLSerial* *VLTextExtractedData.VLSerial*
Interchange	INTEGER		*VLEDIInterchange.Interchange* 0 (for XML and Text)
FunctionalGroup	INTEGER		*VLEDIFunctionalGroup.FunctionalGroup* 0 (for XML and Text)
SetID	INTEGER		*VLEDITransactionSet.TransactionSet* *VLXMLExtractedData.SetID* *VLTextExtractedData.SetID*
TradingPartnerAlias	VARCHAR	255	*VLEDIInterchange.TradingPartnerAlias* *VLXMLExtractedData.TradingPartnerAlias* *VLTextExtractedData.TradingPartnerAlias*
Type	VARCHAR	255	*VLEDITransactionSet.TransactionType* (X12/ Edifact) *VLEDITransactionSet.MessageType* (Tradacoms) *VLXMLExtractedData.DocumentType* *VLTextExtractedData.DocumentType*
Description	VARCHAR	255	*VLEDITransactionSet.TransactionDesc* Description from XML Description from Text
DocumentID	VARCHAR	255	*VLEDIInterchange.ControlNum* *VLXMLExtractedData.DocumentID* *VLTextExtractedData.DocumentID*
Ref1	VARCHAR	500	*VLEDITransactionSet.Ref1* *VLXMLExtractedData.Ref1* *VLTextExtractedData.Ref1*

Column/Field Name	Data Type	Length	Source
Ref2	VARCHAR	500	*VLEDITransactionSet.Ref2* *VLXMLExtractedData.Ref2* *VLTextExtractedData.Ref2*
SenderID	VARCHAR	255	*VLEDIInterchange.Sender* [+ ":" + *VLEDIInterchange.SenderQualifier*] *VLXMLExtractedData.SenderID* *VLTextExtractedData.SenderID*
ReceiverID	VARCHAR	255	*VLEDIInterchange.Receiver* [+ ":" + *VLEDIInterchange.ReceiverQualifier*] *VLXMLExtractedData.ReceiverID* *VLTextExtractedData.ReceiverID*
DocumentDateTime	VARCHAR	255	*VLEDIInterchange.InterchangeDT* (formatted as `yyyy/MM/dd HH:mm:ss`) *VLXMLExtractedData.DocumentDateTime* *VLTextExtractedData.DocumentDateTime*
SetControlNum	VARCHAR	14	*VLEDITransactionSet.ControlNum* `NULL` (for XML and Text)
DataSegmentCount	INTEGER		`VLEDITransactionSet.DataSegmentCount` `NULL` (for XML and Text)
AckStatus	VARCHAR	3	*VLEDITransactionSet.AckStatus* `NULL` (for XML and Text)
AckIControlNum	VARCHAR	14	*VLEDITransactionSet.AckIControlNum* `NULL` (for XML and Text)
isX12	BIT		*VLEDIInterchange.isX12* `NULL` (for XML and Text)
isEDIFACT	BIT		*VLEDIInterchange.isEDIFACT* `NULL` (for XML and Text)
isTRADACOMS	BIT		*VLEDIInterchange. isTRADACOMS* `NULL` (for XML and Text)

SLA/KPI fields

This table contains low-level information regarding each `CHECK` command run (that is, each checkpoint).

Note: Only `CHECK` commands that contain the ConditionsMet parameter are recorded in the VLTrader enterprise database.

VLSLAKPI database table

Column Name	Data Type	Length	Description
TransferID	VARCHAR	30	*TransferID* in `VLTransfers` table
VLSerial	VARCHAR	6	*VLSerial* in `VLTransfers` table
CheckType	VARCHAR	30	Contains one of these values: • `File Age` • `Directory Age` • `Transfer` • `Transfer EDI Ack` • `Transfer Response`
Class	VARCHAR	20	Contains one of these values: • `SLA` • `KPI` • BLANK
Subclass	VARCHAR	30	Contains one of these values: • user-specified string • BLANK
TimeCondition	VARCHAR	100	Contains a common-language summary of the primary time condition.
Direction	VARCHAR	20	Contains one of these values: • `Inbound` • `Outbound` • `n/a`
Recurse	VARCHAR	10	Contains one of these values: • `True` • `False` • `n/a`
Status	VARCHAR	20	Contains one of these values: • `Delivered` • `Completed` • `Any` • `n/a`

Column Name	Data Type	Length	Description
Count	VARCHAR	20	Contains one of these values: • `1-99999` • `All` • `n/a`
Sender	VARCHAR	500	Contains one of these values: • user-specified string • BLANK • ‘n/a’
Receiver	VARCHAR	500	Contains one of these values: • user-specified string • BLANK • `n/a`
FunctionalGroupSender	VARCHAR	500	Contains one of these values: • user-specified string • BLANK • `n/a`
FunctionalGroupReceiver	VARCHAR	500	Contains one of these values: • user-specified string • BLANK • `n/a`
TransactionType	VARCHAR	6	Contains one of these values: • user-specified string • BLANK • `n/a`
DocumentType	VARCHAR	255	Contains one of these values: • user-specified string (planned) • BLANK • `n/a`(planned)
ResponseMatchCondition	VARCHAR	100	Contains one of these values: • user-specified string (planned) • `n/a`(planned)
ConditionsMetClassification	VARCHAR	20	Contains one of these values: • Success • Error
ConditionsMet	BIT		`true` if overall conditions of `CHECK` were met; `false` otherwise

Static tables

The static tables contain data that does not change. This data is used in conjunction with other table to present data to the user.

VLStatus database table

This table contains different statuses found in the `Status` column of the `VLTransfers` table and whether the status is considered a success or failure.

Column/Field Name	Data Type	Length	Source
Status	VARCHAR	15	Status string This status matches a status in *VLTransfers.Status*
IsSuccess	BIT		`True` if this status is considered a Success
IsFailure	BIT		`True` if this status is considered a Failure

VLTransport database table

This table contains different transport strings found in the `Transport` column of the `VLTransfers` table on whether the transport is considered a Transfer or a CheckPoint.

Column/Field Name	Data Type	Length	Source
Transport	VARCHAR	12	Transport string This string matches a transport status in *VLTransfers.Transport*.
DisplayName	VARCHAR	25	The string displayed to the user for this Transport.
IsTransfer	BIT		`True` if this transport is considered a Transfer.
IsCheckPoint	BIT		`True` if this transport is considered a CheckPoint.

Database payload

The database can also be optionally used as a repository for both incoming and outgoing payload.

Note: Only a direct JDBC driver can be used for database payload; an ODBC connection cannot be used because it does not support streaming. Also, the database in use must support Binary Large OBject (BLOB) data types.

VLOptions database table

- There is one and only one row in this table.
- All of this can be configured either by using the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom UI or by modifying the database directly.

Column Name	Data Type	Length	Description
Maximum BlobSize	INTEGER		The maximum BLOB size supported by the database (incoming and outgoing payload will be stored in a BLOB data type) The JDBC interface limits this size to 2^{31}-1 (2,147,483,647) bytes. Default: `65535 bytes`
Outgoing PollingInterval	INTEGER		The frequency at which VersaLex will check for new outgoing payload (`VLSend` and `VLOutgoing` tables) Default: `5 seconds`
Outgoing Timeout	INTEGER		For abnormally terminated or unresponsive sends, the timeout at which the send will be retried by either a parallel or restarted VersaLex Default: `30` minutes
ClearSuccessful Sends	BIT		Indicates whether successfully sent payload (`VLSend` and `VLOutgoing` tables) should be automatically cleared by VersaLex Default: `1` (`True`)
Maximum Attempts	INTEGER		Indicates maximum number of failed outgoing payload send attempts before retries are halted. Default: `0` (Indicates no limit)
Maximum Concurrent Sends	INTEGER		Maximum number of concurrent outgoing database payload actions that can be active at any given time overall. If the limit is reached and more outgoing payload is found, it is put on hold until one of the current outgoing database payload actions completes. Default: `50`
Max Concur Sends Per Mailbox	INTEGER		Maximum number of concurrent outgoing database payload actions that can be active at any given time **for any given mailbox**. If the limit is reached and more outgoing payload is found for a mailbox, it is put on hold until one of the current outgoing database payload actions for that mailbox completes. Default: 5

Column Name	Data Type	Length	Description
Bundle Same Mailbox Sends	BIT		At each polling interval, indicates to bundle payload for the same mailbox together and send one-by-one using just one mailbox session. Default: `0` (`False`)
Maximum Bundle Size	INTEGER		If bundling same mailbox sends, maximum bundle size allowed for one mailbox session. Default: `5`
Connection Poolsize	INTEGER		Indicates the number of database connections immediately obtained and continually reused. These connections are used strictly for database payload. Default: `20`
Include User Inbox Subdirs	BIT		Indicates whether files stored by a user in a subdirectory of their configured inbox should be inserted into the database. Default: `0` (`False`)
Database Payload Suspended	BIT		Indicates whether the database payload feature has been temporarily put on hold by a user Default: 0 (`False`)
AlwaysAll Mailboxes Receive	BIT		`True` if all incoming mailboxes should be used for database payload. Default: `0` (`False`)
Maximum Connections	INTEGER		The absolute maximum number of allowed database connections (including poolsize) for database payload Default: `0`
ReservedForIncoming	INTEGER		Percentage of the maximum number of database connections to reserve for incoming requests. Default: `33` (percent)
IncludeUserOutboxSubdirs	BIT		Indicates whether files stored by a connected HTTP, FTP, or SSH FTP client in a subdirectory of their configured inbox should be inserted into the database. Default: `0` (`False`)

Column Name	Data Type	Length	Description
IncomingStreamDirect	BIT		Indicates whether incoming payload should be streamed directly into the database or through a temporary file. Default: `1` (`True`)

VLMailboxes database table

- The number of rows and the `Host` and `Mailbox` columns are maintained automatically by VersaLex.
- The `ReceiveIncoming` column can be configured either via the Cleo Harmony, Cleo VLTrader, or Cleo LexiCom UI at **Configure** > **Options** > **Transfers** > **Configure** or modified directly in the database.

Column Name	Data Type	Length	Description
Host	VARCHAR	50	Active Cleo Harmony, Cleo VLTrader, or Cleo LexiCom host
Mailbox	VARCHAR	50	Active Cleo Harmony, Cleo VLTrader, or Cleo LexiCom mailbox
Receive Incoming	BIT		For this trading partner (host\mailbox), indicates whether Cleo Harmony, Cleo VLTrader, or Cleo LexiCom should insert incoming payload into the database (`VLIncoming` table) rather than write to the file system Default: `0` (`False`)

VLSend database table

Used in conjunction with `VLOutgoing` table to send outgoing payload from the database. See Sending database payload on page 1015 for more information.

Column Name	Data Type	Length	Description
SendID	INTEGER		Unique send ID (sequence identifier)
Host	VARCHAR	50	Host in `VLMailboxes` table to be used for sending
Mailbox	VARCHAR	50	Mailbox in `VLMailboxes` table to be used for sending
InsertedDT	DATETIME		Date/time outgoing payload initially inserted into database
SendingDT	DATETIME		Initially `NULL`. Date/time Cleo Harmony, Cleo VLTrader, or Cleo LexiCom started sending. Set back to NULL when send attempt either succeeds or fails.
PendingDT	DATETIME		If not `NULL`, this is the Date/time to wait for before sending
VLSerial	VARCHAR	6	Initially `NULL`. *VLSerial* of Cleo Harmony, Cleo VLTrader, or Cleo LexiCom sending. Set back to NULL if send attempt fails.
LastAttemptDT	DATETIME		Initially `NULL`. Date/time Cleo Harmony, Cleo VLTrader, or Cleo LexiCom finished last send attempt.

Column Name	Data Type	Length	Description
LastFailed Attempt ResultText	VARCHAR	150	Result text from last send attempt that failed.
Retries	INTEGER		Defaults to `0`. Current number of retries.
TotalAttempts	INTEGER		Defaults to `0`. Total number of send attempts.
SentDT	DATETIME		Initially `NULL`. Date/time Cleo Harmony, Cleo VLTrader, or Cleo LexiCom successfully finished sending.
FinalAttemptDT	DATETIME		Initially `NULL`. Date/time Cleo Harmony, Cleo VLTrader, or Cleo LexiCom halted retries (based on *VLOptions.MaximumAttempts*).

VLOutgoing database table

Used in conjunction with `VLSend` table to send outgoing payload from the database. See Sending database payload on page 1015 for more information.

Column Name	Data Type	Length	Description
SendID	INTEGER		*SendID* in `VLSend` table
Fileindex	INTEGER		Unique index for each payload to be grouped together in a single message (with same *SendID*)
ExternalID	VARCHAR	50	Optional; if present, logged along with *TransferID* in VersaLex system log file and in `VLTransfers` table
Payload	BLOB		Outgoing content
Filename	VARCHAR	100	Optional; if present, forwarded to trading partner
ContentType	VARCHAR	100	Optional; can be set to `application/edi-x12`, `application/xml`, and so on. Can include charset= parameter. If not present, content type detected by software
Filesize	INTEGER		Optional. Content size or `-1` if not known. Default: `-1`
TransferID	VARCHAR	30	Initially NULL. *TransferID* in `VLTransfers` table
VLSerial	VARCHAR	6	Initially NULL. *VLSerial* in `VLTransfers` table
MessageID	VARCHAR	100	Initially NULL. Protocol-specific message ID

VLOutgoingProperties database table

Optionally used in conjunction with `VLSend` and `VLOutgoing` tables to send outgoing payload from the database. See Sending database payload on page 1015 for more information.

Column Name	Data Type	Length	Description
SendID	INTEGER		*SendID* in `VLSend` table
Fileindex	INTEGER		Unique index of payload or `-1` if property applies to outgoing payload as a whole. Default: `-1`
Name	VARCHAR	50	Payload property (for example, *Content-Disposition*) - or - `PUT` command parameter or header name, for example, *Subject*. See specific protocol documentation for possible `PUT` command parameters/headers
Value	VARCHAR	300	Payload property value, or example, `inline`. - or - `PUT` command parameter or header value

VLIncoming database table

Used to receive incoming payload. See Receiving database payload on page 1016 for more information.

Column Name	Data Type	Length	Description
TransferID	VARCHAR	30	*TransferID* in `VLTransfers` table
VLSerial	VARCHAR	6	*VLSerial* in `VLTransfers` table
MessageID	VARCHAR	100	Protocol-specific message ID
Fileindex	INTEGER		Sequential index of each payload grouped together in a single message (with same *MessageID*)
Payload	BLOB		Incoming content
Filename	VARCHAR	255	If present in message
ContentType	VARCHAR	50	If present in message
Filesize	INTEGER		Content size
Host	VARCHAR	50	*Host* in `VLMailboxes` table that received payload
Mailbox	VARCHAR	50	*Mailbox* in `VLMailboxes` table that received payload
InsertedDT	DATETIME		Date and time at which Cleo Harmony, Cleo VLTrader, or Cleo LexiCom finished receiving content.
RetrievedDT	DATETIME		Initially NULL. Can be set by end user application to indicate payload has been processed.

VLIncomingProperties database table

Optionally used in conjunction with `VLIncoming` table to receive incoming payload. See Receiving database payload on page 1016 for more information.

Column Name	Data Type	Length	Description
TransferID	VARCHAR	30	*TransferID* in `VLTransfers` table
VLSerial	VARCHAR	6	*VLSerial* in `VLTransfers` table
Name	VARCHAR	50	Additional payload parameter/header name, for example, *Subject*.
Value	VARCHAR	300	Additional payload parameter/header value

Sending database payload

End user/application	VersaLex
• End user reviews settings in the `VLOptions` table. • End user application inserts into `VLSend` table *SendID*, *Host*, *Mailbox*, and *InsertedDT* columns and `VLOutgoing` table *SendID*, *Fileindex*, and *Payload* columns. `VLOutgoing` table *ExternalID, Filename*, *ContentType*, and *Filesize* columns are optional. Also, optionally, insert into `VLOutgoingProperties` additional `PUT` command parameters/headers, for example, *Subject*. **Note:** All corresponding inserts into `VLSend`, `VLOutgoing`, and `VLOutgoingProperties` tables must be committed to the database together. **Note:** Setting the property, `Clear.Set.Properties` to `True` in the `VLOutgoingProperties` table for a file will ensure that the properties used for that file are cleared after the file is sent and cannot be propagated to files sent later. This must be set for each file to ensure the properties are always cleared.	• VersaLex polls `VLSend` table for new outgoing payload. • While sending, VersaLex updates `VLSend` table *SendingDT*, *LastAttemptDT*, *Retries*, and *TotalAttempts* columns and VLOutgoing table *TransferID*, *VLSerial*, and *MessageID* columns. • The number of send retries and retry restart are controlled by the general VersaLex properties “Autosend Retry Attempts" and "Autosend Restart". These can be set via the VersaLex UI at **Configure** > **Options** > **Other**.

End user/application	VersaLex
• If desirable, end user application can poll `VLSend` table for payload that is either not being attempted (*`InsertedDT`* `>= 5` minutes ago and *`TotalAttempts`* `= 0`) or has repeatedly failed to be sent (*`TotalAttempts`* `> 4`) or has stopped trying (*`FinalAttemptDT`* `!= NULL`).	
	• After successfully sent, VersaLex either deletes `VLSend` and `VLOutgoing` rows if `VLOptions` table *ClearSuccessfulSends* column is true or sets the `VLSend` table *SentDT* column.

Receiving database payload

End user/application	VersaLex
• End user reviews settings in the `VLOptions` and `VLMailboxes` tables.	
	• With each new incoming payload request, VersaLex checks `VLMailboxes` table *ReceiveIncoming* column to see if trading partner's *Host\Mailbox* is set to receive database payload.
	• If database payload, VersaLex inserts into `VLIncoming` table *TransferID*, *VLSerial*, *MessageID*, *Fileindex*, *Payload*, *Filename*, *ContentType*, *Filesize*, *Host*, *Mailbox*, and *InsertedDT* columns.
• End user application polls `VLIncoming` table for new incoming payload **Note:** Payload should not be retrieved from the `VLIncoming` table until the corresponding `VLTransfers` table row no longer has a *Status* column value of `In Progress`. Valid payload will be indicated by a *Status* column value of `Success` or `Warning`. A *Status* of `Error`, `Exception` or `Interrupted` indicates that payload was not successfully received. The `VLIncomingProperties` table contains additional payload parameters/ headers not already contained within the `VLIncoming` table, for example, *Subject*.	

End user/application	VersaLex
• End user application either deletes row from `VLIncoming` table after retrieving payload or sets the *RetrievedDT* column.	

Cleo VLNavigator Application/User access database fields

The following is a description of the fields used for the Cleo VLNavigator applications and the storing of User login/access information.

DashboardsOptions database table

The DashboardsOptions table is used to store options relating to Dashboards.

Column/Field Name	Data Type	Length	Source
DashboardsOptionsID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
ScorecardEnabled	TINYINT		Flag indicating if the scorecard is enabled (0 = disabled; 1 = enabled)

VLApplicationNum table

The VLApplicationNum table is used to store Cleo VLNavigator application names and enabled/disabled flags for the application as a whole.

Column Name	Data Type	Length	Description
VLApplicationNum	INTEGER		Number assigned by Cleo VLNavigator for each application
Application	VARCHAR	255	Application name
IsEnabled	TINYINT		Flag indicating if the application is enabled (0 = disabled; 1 = enabled)

VLContact table

The VLContact table is used to store various types of contact information for a user.

Column Name	Data Type	Length	Description
VLContactID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
VLEntityID	INTEGER		*VLEntityID* in `VLEntity` table
VLContactNum	INTEGER		*VLContactNum* in `VLContactNum` table
Value	VARCHAR	255	Depending on the value in *VLContactNum*, this is either an email address, phone number, or IP address.

Column Name	Data Type	Length	Description
IsPrimary	TINYINT		Set to `1` for the primary contact for a user and 0 otherwise.

VLContactNum table

The VLContactNum table is used to store enumerated list of contact information types (Example: “Work Email”).

Column Name	Data Type	Length	Description
VLContactNum	INTEGER		Number assigned by Cleo VLNavigator for each contact type.
Description	VARCHAR	255	Description of contact information type

VLEntity table

The **VLEntity** table is used to store information on both the configured Users and User Groups.

Column Name	Data Type	Length	Description
VLEntityID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
Name	VARCHAR	255	For a group, the Group Name is stored here. For non-LDAP users, this contains the user’s Full Name.
VLEntityGroupID	INTEGER		*VLEntityGroupID* in `VLEntityGroup` table
IsEnabled	TINYINT		Group/User enabled (1) or disabled (0) flag
IsDefaultEntity	TINYINT		Set to `1` for User Groups and `0` otherwise
IsSystemAdmin	TINYINT		Set to `1` for the System Administrator user and `0` otherwise.

VLEntityApplication table

The **VLEntityApplication** table is used to store information on whether each Cleo Harmony application is enabled or disabled for a specific User or User Group.

Column Name	Data Type	Length	Description
VLEntityApplicationID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
VLEntityID	INTEGER		*VLEntityID* in `VLEntity` table
VLApplicationNum	INTEGER		*VLApplicationNum* in `VLApplicationNum` table
IsEnabled	TINYINT		Set to `1` if the application is enabled and 0 if disabled for the user/group

VLEntityApplicationFile table

The **VLEntityApplicationFile** table is used to store file paths associated to a specific application.

Column/Field Name	Data Type	Length	Source
VLEntityApplicationFileID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
VLEntityID	INTEGER		*VLEntityID* in `VLEntity` table
VLApplicationNum	INTEGER		*VLApplicationNum* in `VLApplicationNum` table
Sequence	INTEGER		Sequence order of files
Path	VARCHAR	255	Path to file for this application

VLEntityApplicationPrivilege table

The **VLEntityApplicationPrivilege** table is used to store specific privileges that the VLEntity has for an application.

Column/Field Name	Data Type	Length	Source
VLEntityApplicationPrivilegeID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
VLEntityID	INTEGER		*VLEntityID* in `VLEntity` table
VLApplicationNum	INTEGER		*VLApplicationNum* in `VLApplicationNum` table
Privilege	VARCHAR	255	Privileged item name

VLEntityGroup table

The **VLEntityGroup** table is used to store the type of group (VLNavigator Group, VLNavigator Admin Group, …) for each User Group configured.

Column Name	Data Type	Length	Description
VLEntityGroupID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
VLGroupNum	INTEGER		*VLGroupNum* in `VLGroupNum` table

VLEntityNum table

The **VLEntityNum** table is used to store the enumerated list of Entity types (Example: “VLNavigator Person”).

Column Name	Data Type	Length	Description
VLEntityNum	INTEGER		Number assigned by Cleo VLNavigator for each Entity type
Description	VARCHAR	255	Description of Entity type

VLGroupNum table

The **VLGroupNum** table is used to store the enumerated list of Group types (Examples: “VLNavigator Admin Group”, “VLNavigator Group”)

Column Name	Data Type	Length	Description
VLGroupNum	INTEGER		Number assigned by Cleo VLNavigator for each Group type

Column Name	Data Type	Length	Description
Description	VARCHAR	255	Description of Group type

VLOpAuditTrail table

The **VLOpAuditTrail** table is used to store a trail of events of things the users have done through the Cleo Harmony and Cleo VLNavigator user interfaces.

Column Name	Data Type	Length	Description
VLOpAuditTrailID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
ModDateTime	DATETIME		Date and time of the audit trail event
ComputerName	VARCHAR	255	Computer name or IP address from where the modification was made
VLSerial	VARCHAR	255	Serial number of Cleo Harmony, Cleo VLTrader, or Cleo LexiCom from where the modification was made
Username	VARCHAR	255	Logged in user
UserFullName	VARCHAR	255	Full username of logged in user
ItemType	VARCHAR	255	Type item modified
ItemName	VARCHAR	255	Name of item modified
OldItemName	VARCHAR	255	Original name of item modified (in the case of a renamed item)
EventType	VARCHAR	255	Type of event that has occurred
PathName	VARCHAR	255	Relative path of file modified

VLOpAuditTrailOptions table

The **VLOpAuditTrailOptions** table is used to store information on if and when to purge old Operator Audit Trail events

Column Name	Data Type	Length	Description
VLOpAuditTrailOptionsID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
PurgeEventsEnabled	TINYINT		Set to `1` if purge of old events is desired. Set to `0` otherwise.
PurgeAfterDays	INTEGER		Operator Audit Trail events will be purged after they are older than this number of days

VLUser table

The **VLUser** table is used to store information on the users that can log into the Cleo Harmony and Cleo VLNavigator applications. **Note**: The users in the Administrator group are also store in the encrypted Users.xml file so that administrators can log in even when the database is not functioning.

Column Name	Data Type	Length	Description
VLUserID	INTEGER		Generated by Cleo VLNavigator and used as a *key* to the records.
VLEntityID	INTEGER		*VLEntityID* in `VLEntity` table.
FirstName	VARCHAR	255	User's first name.
LastName	VARCHAR	255	User's last name.
BuildFullName	TINYINT		`True` if the full name should be built from *FirstName* and *LastName*.
UserName	VARCHAR	255	Log in user name.
Alias	VARCHAR	255	Optional user alias.
LDAPUser	TINYINT		Set to `1` for an LDAP user. Set to `0` otherwise.
UserPassword	VARCHAR	255	Password for non-LDAP users.
UserUID	VARCHAR	255	Unique identifier for non-LDAP users.

VLUserEntityGroup table

The **VLUserEntityGroup** table is used to store information related to VLNavigator user groups.

Column Name	Data Type	Length	Description
VLUserEntityGroupID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
VLEntityGroupID	INTEGER		*VLEntityGroupID* in `VLEntityGroup` table
LdapUserGroup	TINYINT		`True` if this is an LDAP group
OverrideDomain	TINYINT		`True` if overriding the base domain
Domain	VARCHAR	255	Overriding base domain
OverrideFilter	TINYINT		`True` if overriding LDAP search filter
Filter	VARCHAR	255	Overriding search filter
ExtendFilter	VARCHAR	255	Extension of search filter

VLUserEntityGroupAccess table

The **VLUserEntityGroupAccess** table is used to store User Group access to the various instances of the Cleo Harmony application configured.

Column Name	Data Type	Length	Description
VLUserEntityGroupAccessID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
VLEntityGroupID	INTEGER		*VLEntityGroupID* in `VLEntityGroup` table
VLPools	VARCHAR	255	List of VersaLex pools to which the user group has access

Column Name	Data Type	Length	Description
VLSerials	VARCHAR	255	List of Cleo Harmony, Cleo VLTrader, or Cleo LexiCom serial numbers to which the user group has access

VLUserEntityGroupPrivilege table

The **VLUserEntityGroupPrivilege** table is used to store access levels to various items within the Cleo Harmonyapplication.

Column Name	Data Type	Length	Description
VLUserEntityGroupPrivilegeID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
VLEntityGroupID	INTEGER		*VLEntityGroupID* in `VLEntityGroup` table
VLPrivilegeItem	VARCHAR	255	List of specific items within Cleo Harmony, Cleo VLTrader, or Cleo LexiCom to which the user group has access
VLPrivilegeAccess	VARCHAR	255	Access restriction level for *VLPrivilegeItem*(s)

VLUserEntityGroupTRAccess table

The **VLUserEntityGroupTRAccess** table is used to store which file types the user group has access to within Transfer Report. If the user group does not have access to a file type, then users within that group will not be able to view or email the contents of the transferred file.

Column Name	Data Type	Length	Description
VLUserEntityGroupTRAccessID	INTEGER		Generated by the Cleo VLNavigator application and used as a "key" to the records
VLEntityGroupID	INTEGER		*VLEntityGroupID* in `VLEntityGroup` table
AccessibleFileTypes	VARCHAR	255	List of specific file types (EDI, XML, Text), separated by commas, within the Transfer Report to which the user group has access.
TransactionsAccessible	Bit		`ON` if the transaction types in the `VLUserEntityGroupTREDITypes` table are accessible to the user group. `OFF` if the transaction types in the `VLUserEntityGroupTREDITypes` table are not accessible to the user group.

VLUserEntityGroupTRColumns table

The **VLUserEntityGroupTRColumns** table is used to store which Transfer Report columns are displayed and which order they are displayed. It also stores any custom column names configured.

Column Name	Data Type	Length	Description
VLUserEntityGroupTRColumnsID	INTEGER		Generated by the Cleo VLNavigator application and used as a "key" to the records

Column Name	Data Type	Length	Description
VLEntityGroupID	INTEGER		*VLEntityGroupID* in `VLEntityGroup` table
ColumnName	VARCHAR	255	Either `VLTransfers` table column name or one of the items tracked through file tracking
CustomColumnName	VARCHAR	255	User-customized column name
Enabled	Bit		`ON` if this column is displayed in the Transfer Report table; Otherwise, `OFF`
ColumnNumber	INTEGER		Order of the columns in the Transfer Report table (0-based)

VLUserEntityGroupTREDITypes table

The **VLUserEntityGroupTREDITypes** table is used to store which EDI types the user group can/cannot access. Whether the user group can or cannot access the items in this table depends on the TransactionsAccessible flag in the VLUserEntityGroupTRAccess table.

Column Name	Data Type	Length	Description
VLUserEntityGroupTREDITypesID	INTEGER		Generated by the Cleo VLNavigator applcation and used as a "key" to the records
VLEntityGroupID	INTEGER		*VLEntityGroupID* in `VLEntityGroup` table
EDIType	VARCHAR	255	Either `ASC X12`, `EDIFACT`, or `TRADACOMS`
TransactionType	VARCHAR	255	Specific transaction type Example: `850` (for ASC X12)

VLUserEntityGroupTreeAccess table

The **VLUserEntityGroupTreeAccess** table is used to store user group access to the Cleo Harmony and Cleo VLNavigator applications

Column Name	Data Type	Length	Description
VLUserEntityGroupTreeAccessID	INTEGER		Generated by Cleo VLNavigator and used as a "key" to the records
VLEntityGroupID	INTEGER		*VLEntityGroupID* in `VLEntityGroup` table
VLPoolTreeSubset	VARCHAR	255	List of VersaLex pools to which the user group has access
UserGroupTreeSubset	VARCHAR	255	List of Cleo Harmony, Cleo VLTrader, or Cleo LexiCom user groups to which the user group has access
HostFolderTreeSubset	VARCHAR	255	List of host folder tree to which the user group has access

Column Name	Data Type	Length	Description
ApplicationTreeSubset	VARCHAR	255	List of Cleo VLNavigator applications to which the user group has access
RawPayloadNeedsHostPermissions	TINYINT		Set to `1` if accessing raw payload from Transfer Reports requires the Host system privilege