Cleo LexiCom®

Release Notes

Version 5.7

December 2021

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

Contents

Cleo LexiCom 5.7 Release Notes

Cleo LexiCom software provides you with a wide variety and combination of file transfer capabilities that allow you to initiate transfers, control your transfers and environment, monitor your file transfer activities, and take actions as appropriate based on your file transfer activities.

Cleo VersaLex is the platform that powers the Cleo family of Secure Data Integration (SDI) products—The Cleo LexiCom® product is a desktop-based client solution for communication with major trading networks. The Cleo VLTrader® product is a server-level solution designed to meet the needs of mid-enterprise organizations. The Cleo Harmony® product is tailored for large enterprise needs. Enterprise capabilities include system monitoring, enhanced business-level dashboards, VLTracker, SNMP traps, dynamic blacklisting, and whitelisting.

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

What's new in version 5.7

This section outlines new features and enhancements included in this version of Cleo LexiCom.

Technology Refresh

In Version 5.7, we have refreshed underlying technologies in Cleo LexiCom. These upgrades include support for TLS 1.3 and replacing Oracle 8 JRE with OpenJDK 8.

JMS Enhancements

JMS support has been expanded in Cleo LexiCom.

- The JMS URI now allows you to use the new `filenameProp` property to construct filenames based on parameters you specify.
- The TextMessage JMS message type is now supported by the JMS URI.

Security Enhancements

Expired and retired trusted CA certificates will not be installed for new Cleo VersaLex installs. The expired certificates will remain intact for Cleo VersaLex upgrades. Some trusted CA certificates have been updated with new versions.

With this release, Cleo products have been enhanced to use Bouncy Castle libraries version 1.66.

Upgrading to version 5.7

Before you upgrade Cleo LexiCom

If you are upgrading from an earlier version to Cleo LexiCom 5.7, be aware that Cleo LexiCom no longer supports the **AS/400** operating system. See Cleo LexiCom 5.7 System Requirements.

Recommendations for Upgrading

When upgrading to Cleo LexiCom version 5.7, Cleo recommends the following:

- Back up your configuration using the **Export** functionality. In the Web UI, go to **Administration > System > Export**. In the native UI, go to **File > Export**. Performing an **Export** will save your data in a format that you can import using the Cleo LexiCom **Import** functionality should the need arise.
- Make sure your system meets the system requirements for Cleo LexiCom version 5.7, as it requires greater resources than earlier versions. All new installs must be 64-bit. Visit Cleo LexiCom 5.7 System Requirements to view the System Requirements for your product.
- Run the Cleo LexiCom 5.7 installer to perform an in-place upgrade. Your data and configuration remain intact from the previous version of the Cleo LexiCom software.

Update history

The following section contains descriptions of issues fixed in Version 5.7 and subsequent patch releases:

Fixed issues in version 5.7.0.4

Enhancements - Framework

- The Generate Report option in the admin web UI Transfers page would previously include only the information viewable from the UI grid. Now all available transfer information, such as file path, is included in the generated report. Also, a report generated from classic mode specifically now includes the file path if it is enabled in the user's group.

Enhancements - HTTP

- Added a new HTTP SaveErrorResponseContentOnPutPlusGet advanced property, which when set on causes the response content from a PUT+GET command request to be saved to the inbox even on error responses.

Enhancements - ebMS

- Added an option to ebXML to modify the case of the Content-Id header.

Enhancements - MQ

- Added support for the following MQ SSL cipher specs: ECDHE_RSA_AES_128_GCM_SHA256 and TLS_AES_256_GCM_SHA384.

Enhancements - SMTP

- Added the ability to configure individual SMTP Proxies to use Start TLS via the property 'Use Start TLS' in the proxy configuration screen. This property defaults to 'True' to match existing functionality.

Bug Fixes - HTTP

- Fixed an issue where SSL connections could fail with a NullPointerException when SSL Debug was enabled.

Bug Fixes - SSH FTP

- Fixed a potential SFTP server problem where a file stat request would not return a response. This could occur after a file upload, if a file stat request from a client occurred at the same time that the file was deleted or moved by the server.

Bug Fixes - Connector

- Fixed an issue where users would not be able to CD into a subdirectory of an Azure Blob connector when the Azure Blob container was set up as Data Lake Storage.

Security - Framework

- VersaLex now ensures that any paths in filenames on incoming requests are ignored for protocols that do not support paths, including AS2, ebMS, RNIF, and SMTP.

Fixed issues in version 5.7.0.3

Enhancements - SFTP

- Added support for the following SFTP algorithms: Public Key: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, Key Exchange: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, and MAC: hmac-sha2-512, hmac-sha2-256-96, hmac-sha2-512-96. The new Public Key algorithms are available on the client side only, while the new Key Exchange and MAC algorithms are available on both client and server side (although server side only applies to VLTrader and Harmony). The new Key Exchange algorithms are not available in FIPS mode.
- All negotiated algorithms are now logged at the beginning of each SFTP client and server session.

Enhancements - S3

- Added new S3 connector property, AccessControlList (ACL), for cross-account use. This new property applies the selected ACL permissions on objects PUT to a bucket.

Bug Fixes - AS2

- Fixed an issue where, if the AS2 Receipt-Delivery-Option header contained a username:password in the URL, it would fail to send the MDN to the trading partner.

Fixed issues in version 5.7.0.2

Enhancements - ebMS

- Added new ebMS "Allow Incoming Request With Missing Role Element" advanced property, which when enabled allows an incoming request without a role element value to be processed if it otherwise matches a configured ebMS mailbox.

Fixed issues in version 5.7.0.1

Enhancements - Framework

- Added the ability to import a P12 certificate through the REST API.

Bug Fixes - Framework

- Fixed an issue, introduced in 5.7.0.0, where importing a User certificate with a DSA key would fail.
- Fixed an issue where generating a User certificate with a DSA key would fail.
- Fixed an issue where connecting to the WebUI through a HTTP/s port with FIPS mode enabled would cause the web browser to report a cipher error and prevent the page from loading. Note: VLProxy 3.9.0.1 is required if using VLProxy.
- Fixed an issue where updating a host's certificate through REST API would set the host to 'Not Ready' when the certificate is a PGP key-generated certificate.

Bug Fixes - FTP

- Fixed an FTPs Active mode issue introduced in 5.7.0.0 where, when the 'SSL Maximum Protocol Version' was set below the new maximum of 'TLS 1.3', it would fail to find an open data port in the specified range or it would fail in SSL negotiation.

Bug Fixes - SSH FTP

- Fixed an issue where, if the trading partner's SSH server prematurely closed a client connection during the initial protocol version negotiation, the result could be excessive CPU usage up to the configured connection timeout.

Fixed issues in version 5.7

Enhancements - Framework

- Added support for Transport Layer Security (TLS) Protocol Version 1.3.

  Note: When the `SSL Maximum Protocol Version` is left blank, the software will attempt to use TLS 1.3.
- Added two new system-level other properties: **Email And Execute On Resolution** and **Email Local And Partner Activation Notifications**. Both of the new properties default to `true`, which matches previous behavior. If **Email And Execute On Resolution** is `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. **Email And Execute On Resolution** applies to all three levels of **Email/Execute On Repetitive Failures**. If **Email Local And Partner Activation Notifications** is true, when a scheduled certificate is activated, an email is sent to the system administrator.
- Addressed an issue where `FileNotFoundExceptions` were being thrown because scheduled autosend files were temporarily unstable due to a slow underlying file system. Now, when running scheduled actions, these files are bypassed, avoiding unnecessary exceptions and Email-On-Fail emails.
- Base release notes will be appended to the patch notes that are included within each patch, as stored in the `conf/notes.txt` file.
- Converted host-level Advanced property, `SSL Cipher`, to a regular expression field. Now, users can enter regular expressions (enclosed in brackets) or wildcard expressions to restrict the list of ciphers presented to the SSL server. The ability to specify only a single cipher is still possible, however, the UI has been improved to make this selection easier. Refer to the user's guide for detailed information on the usage of this property.
- Improved wording for messages related to actions that are temporarily blocked from scheduler processing, especially as it relates to failed actions due to slow file systems.
- An overrun of the data segment in the SSL/TLS handshake and a resulting failed inbound connection during SSL/TLS handshake could occur when both of the following are true: 1) any of the HTTP/s, FTP/s, SMTP/s or OFTP/s client authentication settings are enabled in the Local Listener and configured to `Accept all Certificate Manager Trusted CA certificates`; 2) the number of installed trusted CA certificates causes the byte length of the Distinguished Names of those trusted CA certificates to exceed 65535 bytes. To help diagnose this problem, a log message and email notification will now be sent when the byte count exceeds 65535 bytes. An example of that message would be: "There are 2300 trusted CA certificates with 65570 total bytes registered for HTTP/s client authentication. This exceeds the maximum threshold of 65535 bytes and may cause inbound connections to fail during the SSL/TLS handshake. You should remove unused trusted CA certificates to get that byte count below the maximum threshold." After you remove the unused CA certificates, you must restart the Local Listener for those changes to take effect. Once the byte count falls below the maximum threshold, another log message and email notification will be sent. An example of that message would be: "There are now 1200 trusted CA certificates registered for HTTP/s client authentication with 43456 total bytes and is below the maximum threshold. No further action is necessary at this time."

Bug Fixes - Framework

- Removed unsupported PSK ciphers from SSL cipher suites.
- Fixed an issue where user certificate private keys exported with Base64 encoded PKCS #8 (.PEM) format had incorrect header and footer values.
- Added support for the %transferid% macro in the destination filename field of the PUT and GET commands for FTP and SFTP. Also added support for %transferid% within the destination filename field of LCOPY commands.
- Added more detailed messaging around upgrading through our product. We are now specifying that you need to run the native UI as an admin user in Windows to upgrade through the product.

- Fixed an issue where passwords that start with "#" or "*" were not always handled correctly. Please note that passwords that begin with "#" or "*" should not be escaped by adding an extra "#" or "*". Rather, the passwords should be entered literally.
- Fixed an issue where updating to an incorrect Local Signing or Encryption certificate in a running Local Listener would prevent SSHFTP and FTP users from logging in.
- Fixed an issue where temporary actions were being written to top.xml unnecessarily causing delays in processing.
- Cleo LexiCom only: Fixed an issue where using -f option (process command line options from a file) would cause a NoClassDefFoundError exception causing the operation to fail.
- Fixed an issue where using the "All" button to select Trading Partner/CA Certificates in the Export window would improperly populate the list with duplicate entries, which would then produce an unusable export filter.
- Fixed a problem where the concatenated file size (for example, "10+20") was being reported for the %filesize% macro when placed in an 'Execute On Check Conditions Met' string for a multi-file result. Now the concatenated string is split apart for each file (for example, "10" and "20").

Bug Fixes - FTP

- Fixed an issue where the "RESULT" log was missing when a FTP GET action failed on a CD command.

Bug Fixes - AS2/AS3

- Fixed an issue in the AS2 receiver where, if an asynchronous MDN was requested and the AS2 relationship was unknown, the MDN would not be sent and there was no Result logged.

Bug Fixes - SSH FTP

- Fixed an issue where, if an optional comment is returned from the SSH FTP server during version negotiation, SSH_MSG_KEX_INIT would fail with an Invalid Packet Size exception.
- Fixed an issue where incorrect permissions were sent when retrieving a file from an SSHFTP server.

Security - Framework

- Expired and retired trusted CA certificates will not be installed for new Cleo VersaLex installs. The expired certificates will remain intact for Cleo VersaLex upgrades. Some trusted CA certificates have been updated with new versions.
- Upgraded the Bouncy Castle libraries to version 1.66. This includes necessary updates to Cleo software.