Cleo LexiCom®

Release Notes

Version 5.8.1

June 2025

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.

© 2003-2025 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

Cleo LexiCom 5.8.1 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 5.8.1

Enhancements - Framework

- Updated AS/400 CL scripts to add support for V7R5 and remove support for V7R2. Updated jt400.jar to JT Open 20.0.8 (java 8).
- Added new REST API endpoints for system configuration: settings/{options|listener|proxies}. Please see developer.cleo.com for information on these new endpoints.
- In the product launcher bootstrap configuration, LexiCom now includes an "AS/400 Install Share Directory" setting. This new setting eliminates the need to use a Windows 7 machine to administer an AS/400 native install, and instead allows a second local install to be pointed at the AS/400 install. This second local install does not need to be licensed separately. Please refer to the product help for this setting for details.
- Fixed an issue using TLS 1.3 where the legacy_version header was set incorrectly in the "Client Hello" message. It is now set to TLS 1.2 in accordance with the RFC.

Enhancements - OFTP

- Added support for SHA256 and SHA512 in the OFTP signing algorithm dropdown.

Enhancements - RNIF

- Added support for SHA256 and SHA512 in the RNIF signing algorithm dropdown.

Enhancements - SSH FTP

- SFTP client now discovers which signature algorithms are supported by the server and uses the rsa-sha2-256 key authentication algorithm instead of sha-rsa when supported.

Bug Fixes - Framework

- When VersaLex is running on an unsupported operating system, fixed an issue where software update check would incorrectly indicate the product was on the current release and patch levels.
- Fixed an issue using TLS 1.3 where the legacy_version header was set incorrectly in the "Client Hello" message. It is now set to TLS 1.2 in accordance with the RFC.

Upgrading to version 5.8.1

When upgrading to Cleo LexiCom version 5.8.1, 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 5.8.1, as it requires greater resources than earlier versions. All new installs must be 64-bit. Visit Cleo LexiCom 5.8.1 System Requirements to view the System Requirements for your product.
- Run the Cleo LexiCom 5.8.1 installer to perform an in-place upgrade. Your data and configuration remain intact from the previous version of the Cleo LexiCom software.

Update history

This section contains descriptions of enhancements and issues fixed in releases of Version 5.8.1. The following Release Index table provides information about availability and release type for each release.

Table 1: Release Index

Version	Availability	Release Type	Release Date
5.8.1.0	General	Major	10-April-2025
5.8.1.1	Limited	Restricted	14-May-2025

Enhancements and Fixed issues in version 5.8.1

Availability	Release Type	Release Date
General	Major	10-April-2025

Security - Framework

- Fixed an issue where clients were able to negotiate elliptical curve ciphers outside of the VersaLex Local Listener settings. Also removed deprecated named elliptical curves from the Local Listener according to RFC 8422. Lastly, VersaLex now honors the existing Local Listener advanced property "SSL Ignore Client Cipher Preference Order" for elliptical curve ciphers as well. Note: VLProxy 3.10.1.0 is required if using VLProxy.
- This update contains other security-related improvements. For customer protection, Cleo does not disclose all security update details. For further information, please contact customer support. For critical security updates or if there is a known exploit, Cleo will publish a security bulletin and notify customers.

Enhancements - Framework

- Macro replacement is now supported in a wildcarded GET or LCOPY command source. Note that macro replacement is still not supported in a source containing a regular expression.
- Fixed an issue where importing a PKCS#12 file would fail if the certificate was generated with a brainpool elliptic curve.
- If there is an error reading an XML config file and it's not a syntax exception, the stack trace of the causing exception is now logged to assist in diagnosis.
- PGP certify, sign, and encrypt key usage flags are now being set (refer to https://www.rfc-editor.org/rfc/rfc4880#section-5.2.3.21). These flags may be required by other software packages when exchanging PGP keys.
- Upgraded Apache Log4j library to version 2.22.0
- Added a new HTTP 'Save Error Response Content On Put Plus Get' 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 - HTTP

- Added the ability to use macros in the source of HTTP and HTTP/s actions.

Enhancements - RNIF

- Added option 'Add Filename to Attachment Content Type' for RNIF to add the filename of the attachment to the Content-Type MIME header.
- Removed RNIF 1.1 Content-Type header check for "version=1.0" so it is compatible with systems that do not send the version.
- Added support for CIDX (Chemical Industry Data eXchange). CIDX can be enabled in an RNIF host by selecting 'RNIF Version' v1.1 and selecting the 'CIDX' checkbox. A new 'Incoming content format', MIME, has been added which will store the incoming MIME data instead of just the service content. A new Advanced property, Save Received Ack As Payload, has also been added. Enabling this property will copy the Received Ack into the Inbox and Receivedbox. Note: VLProxy 3.10.0.7 is required if using VLProxy.

Enhancements - SSH FTP

- Added support for hmac-sha2-256-etm@openssh.com and hmac-sha2-512-etm@openssh.com algorithms for both client and server SFTP connections. Note: VLProxy 3.10.0.10 is required if using VLProxy.

- Added a new SSH FTP "Large File Transfer" property. It uses a large window size and sends 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.
- On both the SFTP client and server sides, added support for the rsa-sha2-256 and rsa-sha2-512 public key algorithms. Note: VLProxy 3.10.0.3 is required if using VLProxy.
- On the SFTP client side, added support for the ssh-ed25519 public key algorithm. This algorithm is not supported in FIPS mode.
- Added support for ECDSA and Ed25519 algorithms during SFTP key authentication for both client and server connections. ECDSA and Ed25519 keys can be imported or generated, but note that these can only be used with SFTP. Ed25519 is not supported in FIPS mode. Note: VLProxy 3.10.0.2 is required if using VLProxy.

Bug Fixes - Framework

- Fixed an issue where a NullPointerException could be thrown if there was an issue listing folders while doing file cleanup at startup. This was introduced in 5.8.0.24.
- Added extra synchronization when reading and updating the schedule to prevent possible loss of scheduled items.
- Removed the option to disable strong protection when exporting user certificate and private key due to weak protection no longer being supported.
- Removed an error message from being logged for stale WebUI sessions. This was introduced in 5.8.0.20.
- Fixed an issue with the Web UI where users could still schedule actions to run continuously without polling for files.
- Fixed an issue where the Certificate Signing Request generated for an ECDSA certificate had an invalid signature.
- Fixed a problem where a PKCS#12 certificate/private key using the ECDSA or Ed25519 algorithm could not be imported. Note: Ed25519 is not supported in FIPS mode. Also fixed a problem in FIPS mode where a missing cryptography library was causing all PKCS#12 imports to fail.
- Fixed an issue where a certificate signing request (CSR) could not be generated on a user certificate with an ECDSA or ED25519 private key.
- When running VersaLex commandline, eliminated a "WARN StatusConsoleListener" deprecation warning that would be printed multiple times to the console at the beginning of execution. This warning started appearing with version 5.8.0.14.
- Unify Only: Fixed an issue where some Unify features (such as ellipses and right clicks) would not work on new Chromium browsers (such as Chrome and Edge) due to browser updates. Related incident #8274345.
- When not polling for files, can no longer set a new schedule for an action to run continuously. The schedule recurrence must now be at least 5 seconds. Related incident #8282893.
- Fixed an issue where a CA store certificate that was previously browsed and selected for configuration (e.g. OpenPGP encryption/signature verification certificate) was not being properly re-selected for the same configuration when re-browsing.
- Fixed an issue where 'Local packaging encryption is not allowed for appended transfers' would be reported if '-ape' was contained in the filename while using packaging.
- Fixed an issue where OpenPGP unpackaging could fail depending on the packaged file size.

Bug Fixes - FTP

- When the Security Mode in an FTPs host is changed to none, the Advanced "Explicit SSL Post Command" property value is now cleared if it is still set to the default of "PBSZ 0;PROT P". Refer to the Explicit SSL Post Command documentation for more information.

Bug Fixes - HTTP

- Fixed an issue in HTTP/s hosts (e.g. AS2, ebMS, ...) where the SET ReuseSSLSessionsAcrossActions=False command was having no effect (i.e. the action's SSL/TLS sessions would still be reused across actions).

Bug Fixes - RNIF

- Fixed an issue in RNIF 1.1 where 'inReponseTo.ActionIdentity.InstanceIdentifier' in the acknowledgement did not match the original Request/Response message.

Bug Fixes - SSH FTP

- Fixed a problem where a valid regular expression configured for one of the system level Client SSH FTP Pattern properties could cause no client algorithms to be listed at runtime depending on which algorithms match the regular expression.
- Fixed a problem during diffie-hellman-group-exchange-sha256 key exchange where VersaLex was incorrectly ignoring a reply message, causing the next message read to be unexpected and resulting in an InvalidMessageException.

Bug Fixes - ebMS

- Fixed an issue where the ebXML Message Service was only accepting requests that used an "xlink" namespace prefix.

Enhancements and Fixed issues in version 5.8.1.1

Availability	Release Type	Release Date
Limited	Restricted	14-May-2025

Note: Contact Cleo Support for information about obtaining this patch.

Security - Framework

- This update contains security-related improvements. For customer protection, Cleo does not disclose all security update details. For further information, please contact customer support. For critical security updates or if there is a known exploit, Cleo will publish a security bulletin and notify customers.

Enhancements - Framework

- Improved performance of connectors when they contain encrypted properties.
- Cleo LexiCom only: In the FIPS edition of the product, now log a warning message when the configured SSL Minimum or Maximum Protocol Version Advanced property value is overridden at runtime. FIPS 140-3 only supports TLS 1.2 and 1.3 protocol versions.

Bug Fixes - Framework

- Fixed an issue where a Local Listener secure port configured with an Ed25519 certificate/private key would cause all incoming SSL/TLS client requests to fail. Also Ed25519 requires that the Local Listener SSL Minimum Protocol Version advanced property be set to at least TLS 1.2.

Bug Fixes - SSH FTP

- Fixed an SFTP issue where repeated "The message id 3x is not the same as the message implementation id 3x" exceptions would begin to occur and then continue until the product was restarted.