IMM eSign 2022

Release Notes

End of Support Notices

- Microsoft SQL Server 2012
- Microsoft Windows 8.1
- Citrix XenApp and XenDesktop 7.17
- VMware Horizon 7.4
- iOS 12

Deprecated Features

- eSign Client 2016.8

New Supported Environments

- Microsoft Windows 11
- Microsoft Windows Server 2022
- Microsoft Windows Server 2022 Remote Desktop Services
- Citrix Virtual Apps and Desktops Version 7 2203
- VMware Horizon 8 2203

Notes

- Refer to the system requirements for the latest prerequisites.
- Some features and fixes listed here may not be applicable to you.

Release Notes

eSign 2022.4.2

New In This Release

- eSign Server 2022.4.2

Supported Server Upgrades

eSign Server 2022.4.2 supports upgrades from these versions:

- eSign Server 2020.1.3 SP5 or higher

Compatible Client Versions

eSign Server 2022.4.2 is compatible with these eSign Client versions:

- eSign Client 2020 or higher is supported.

Compatible eSignPlus Versions

eSign 2022.4.2 is compatible with these eSignPlus versions (if applicable):

- eSignPlus 2022.4.2

Features

Signature Pad Improvements

- The buttons that are displayed on signature pad screens are improved for better responsiveness. (ES-2522)

Speed and Performance Improvements

- Internal updates were made to improve speed and performance. (ES-2401)

Standalone Ad Hoc Downloader

- Easily edit the database name of the standalone Ad Hoc Downloader during eSign installation. The database name is not editable during upgrades. (ES-2443, ES-2444)

Fixes

This is a list of issues that have been fixed in this release:

- When attempting to install Standalone Ad Hoc Downloader on a server that does not have eSign, installation fails. (ES-2546)
- After upgrading, some sessions will not open. (ES-2559, ES-2560)

eSignPlus 2022.4.2

Prerequisites

- eSign Server 2022.4.2

Upgrade Requirements

To upgrade to eSignPlus 2022.4.2, these requirements must be met:

- The current eSign Server version must be eSign Server 2020.1.3 SP5 or higher.
- The current eSignPlus version must be eSignPlus 2020.1.2 SP2.

Compatible Client Versions

eSignPlus 2022.4.2 is compatible with these eSign Client versions:

- eSign Client 2020 or higher

Features

Change a Workflow

- When a session is created, users have the flexibility to change the assigned workflow based on the needs of the document set before continuing with the session. (ES-1638)
- The workflow can be changed using the Change Workflow button on the Session Details page during the "Start" step.
- New settings are available from the eSignPlus tab on the General Settings page to give users the ability to change the workflow.
    - **Allow to Change Workflow at Start Step**: This setting is turned off by default. The Allow to Change Workflow at Start Step setting must be selected for users to change the workflow.
    - **Auto Launch Select Workflow (API Sessions Only)**: This setting is only applicable for sessions created using eSign API. The Allow to Change Workflow at Start Step setting must be selected to configure this setting. If the Auto Launch Select Workflow setting is selected, the Select Workflow pop-up window will appear when the Session Details page loads the first time.

Branding Updates

- The term "eSignPlus" replaces instances of "eSign plus" in the user interface. (ES-2232)

Fixes

This is a list of issues that have been fixed in this release:

- Previously, documents included in a workflow rule could not be exported from the Document Maintenance (RTS) page. Using the new Delete Template / Export Template toggle, documents can be exported from the Document Maintenance (RTS) page regardless of their inclusion in a workflow rule. (ES-1732)
- After eSignPlus 2020.1.2 SP2 is installed, the workflow purge scheduled task will not run. (ES-2324)

Release Notes

eSign 2022.4.1 SP1

New In This Release

- eSign Server 2022.4.1 SP1 (Cumulative Patch)

Prerequisites

Refer to the eSign 2022.4.1 Release Notes for additional requirements and compatibility. eSign Server 2022.4.1 SP1 supports upgrades from these versions:

- eSign Server 2022.4.1 or higher

Fixes

This is a list of issues that have been fixed in this release:

- When attempting to install Standalone Ad Hoc Downloader on a server that does not have eSign, installation fails. (ES-2546)
- After upgrading, some sessions will not open. (ES-2559, ES-2560)

eSign 2022.4.1

New In This Release

- eSign Server 2022.4.1
- eSign Client 2022.4.1

Supported Server Upgrades

eSign Server 2022.4.1 supports upgrades from these versions:

- eSign Server 2018.2 or higher

Compatible Client Versions

eSign Server 2022.4.1 is compatible with these eSign Client versions:

- eSign Client 2018.2 or higher is supported.
- eSign Client 2022.4.1 is required to get all of the latest features and fixes in this release. Upgrade to eSign Client 2022.4.1 from eSign Client 2018 or higher.
- eSign Client 2022.4.1 is not compatible with eSign server versions released before eSign Server 2022.4.1.

Compatible eSignPlus Versions

eSign 2022.4.1 is compatible with these eSignPlus versions (if applicable):

- eSignPlus 2020.1.2 SP2

Features

Printer Port Number Configuration

- The eSign Client printer port number and printer service endpoint port can be configured during eSign Client installation or upgrade. (ES-526)

- During eSign Client upgrade, existing port numbers will be retained automatically. If upgrading from an eSign Client version older than eSign Client 2020, the Printer Service Endpoint Port will be set to the first available port number that is not in use.
- If the printer ports are not assigned to port numbers, the ports are assigned to the first available port numbers that are not in use.
- If the port number is not available, invalid, or left blank, an error message is displayed to alert the user to fix it.
- To fix printer port number issues when an eSign Client installation or upgrade is not being performed, run the eSign Client Port Configuration utility. The existing port numbers will be displayed in the eSign Client Port Configuration utility for easy reference.

eSign Client Parameters Window

- When changing the eSign Server URL from the eSign Client Parameters window, the existing URL is displayed for easy reference. (ES-1124)
- For improved usability, a notification message is displayed to alert the user that they must exit and relaunch eSign Client for the new eSign Server URL to take effect. (ES-1124)
- To open the eSign Client Parameters window, open the *GetClientParams.exe* file.

Password Improvements (eSign Client)

- eSign Client supports ampersands (&) and equal signs (=) in user passwords. (ES-484)
- To make the login process more intuitive, the fields to create a new password are hidden from the eSign Client Login user interface when they are not applicable. (ES-988)

eSign Client Version Tracking

- From the eSign Client system tray icon, quickly find detailed eSign Client version information (iteration number) and the eSign Server URL when the About option is clicked. (ES-1082)
- Starting with this release, the version of eSign Client that you are using will be saved so that you can receive upgrade and end-of-support notifications in future releases of eSign Client. (ES-2164)

eSign Client Notifications

- eSign Client notification messages are improved for clarity. (ES-1514)

User Friendly Messages

- The informational messages displayed in the eSign web browser are updated to be more user friendly when these scenarios occur:
  - The user logs out using the Logout button. (ES-2273)
  - Multiple eSign web browsers are open. (ES-2273)
  - A window has been inactive for an extended amount of time. (ES-2273)
  - An attempt to open eSign takes too long. (ES-2328)
- Provide a link to return to eSign when a user logs out, when multiple eSign web browsers are open, and when a window is inactive. From the General Settings page, enable Display eSign Link to Log Back In to use this feature (disabled by default). It is recommended to work in one eSign web browser at a time. (ES-2273)

Signature Lines on Signature Pads

- The ability to display signature lines at the bottom of certain signature pads is removed due to the way the signatures appeared for different users. This behavior will be reviewed for future implementation.

Fixes

This is a list of issues that have been fixed in this release:

- If there are spaces in the Allowed Domains list for the eSign Client, eSign Client is unable to connect. (ES-1487)
- When previewing a signed LaserPro document that has a text field, the signature is not shown. (ES-2174)
- Custom logos are not uploaded on the first attempt. (ES-2254)
- When the first document in a session is in portrait orientation and the second document is in landscape orientation, the Confirm Review button is not visible in the second document. (ES-2271)
- There is a blank option in the Remote Signature Service URL dropdown menu. (ES-2321)
- When a session is created using eSign RTS API, certain fields are deleted depending on the setting configurations. (ES-2357)
- When an eSign RTS API session is created with more than two documents, extracted party fields are deleted from all of the documents except the first and the last documents depending on how the fields were added. (ES-2356)
- When signature pads are configured to display messages during in-person signing, buttons on the signature pads are not displayed as expected in some environments. (ES-2242, ES-2054)
- During the in-person signing process, an Unexpected Device error message is displayed in eSign if the document name is too long to fit on one line of the signature pad display screen. (ES-2262)
- When multiple eSign windows are open and a new session is launched, there is a Session Timeout message displayed on the Login page. (ES-2272)
- Signatures are not being displayed in the correct location in CUNA attachments. (ES-2331)
- In rare scenarios, the Accept button is displayed on the Consumer Disclosure page. (ES-2124)
- When GemView features are enabled for the institution, users that do not have a GemView device are receiving pop-up messages in some scenarios. (ES-2189)

eSign 2022.4

Supported Client Versions

- eSign Client 2018.2 or higher is supported.
- eSign Client 2020.1.6 or higher is required to enable all of the latest features and fixes.

Features

Topaz GemView Enhancements

- The Topaz GemView signing experience is enhanced. (ES-925)
    - Before starting the signing process, GemView devices can be detected automatically, which allows eSign to tailor the FI representative and consumer signing experience for better service and productivity. Enable the Detect GemView Device feature from the eSignature Settings page.

- When a GemView device is automatically detected, eSign can be configured to automatically display the eSign browser on the GemView device without any involvement from the FI representative. Enable the Auto Push to GemView feature from the eSignature Settings page.
  - If Detect GemView Device is not selected, the Detect GemView Device setting will be automatically selected when Auto Push to GemView is selected.
  - If Detect GemView Device is selected but Auto Push to GemView is not selected, the eSign browser is not automatically displayed on the GemView device. FI representatives must click the Push to GemView button on the Consent page before the consumer can take control using the GemView device.
- Instead of manually moving the eSign browser back and forth between workstation and GemView screen, the GemView screen is duplicated on the workstation to allow the FI representative to follow along with the consumer and assist as needed.

Messages on Signature Pads

- The default signature pad messages are updated for consistency and improved clarity. (ES-2134)

Adobe Sign Domain Name Change

- Adobe Sign updated the domain name from echosign.com to adobesign.com. New financial institutions will be automatically assigned to the adobesign.com domain in eSign. Existing financial institution administrators can manually update the domain name in eSign using the Remote Signatures Service URL setting in the Other Remote Settings tab on the eSignature Settings page. Alternatively, host administrators can update the domain name in eSign using the Remote Signatures Service URL setting in the Remote Signatures tab on the Add or Edit Financial Institution page. (ES-1762)

Scanner

- Personalize the eSign browser to show or hide eSign's scanning capabilities. When enabled, FI administrators and FI representatives within the institution will be able to use scanners to add documents to sessions, and they can modify scanner settings as needed. When disabled, FI administrators and FI representatives will not have the option to scan documents or modify scanner settings. (ES-1175)

Copy Users and Groups

- Rather than manually creating a new user or group, administrators can save time and effort by copying an existing one. Copy an existing user from the User Maintenance page or copy an existing group from the Group Maintenance page, and apply the desired settings from the existing user or group to the new user or group. (ES-1377)

Default Authentication Improvements

- Improvements are made to the processes for configuring which authentication types are available to a financial institution representative and setting the default authentication type. (ES-1711)
- Using the Allowed Authentication Types setting, host administrators can configure which authentication types will be available to financial institution representatives on the eSignature Management page, in the Default eSign Authentication Type setting, and in the API. Previously, a text field (Skip Services) was used for this feature.
- Tailor the default authentication type to your specific financial institution's needs to reduce the number of steps your financial institution representatives must perform to get sessions reviewed and signed. To set the default authentication type for the FI, navigate to the eSignature Settings page and select an option from the Default eSign Authentication Type menu. If your environment does not have the Remote Signing feature, only In-Person will be displayed.

General Settings Page Updates

- The General Settings page is updated for better organization and to support help text. (ES-1099)

API Keys

- Generate an API key automatically to avoid manual text entry. The API key can be generated from the General Settings page (FIAdmin) or the Add or Edit Financial Institution page (HostAdmin). (ES-1935)

CSI CenterDoc Imaging System

- New integration with CenterDoc API allows institutions to submit documents directly to a CenterDoc API endpoint without the need to use the generic Index.txt imaging system. Once CenterDoc is configured for the institution, administrators simply select the CenterDoc imaging system from the Imaging System Settings page and configure the settings as needed. Indexing is supported for PDF documents only. (ES-1689)

Provide Current Document Date and Time to Imaging System

- Convert the current date and time to a specific time zone and send the document information to your imaging system when archiving a session. On the Imaging System Settings page, use the GetCurrentDateTime function to take advantage of this feature. If the time zone parameter is not populated, the default time zone is UTC. (ES-1748)

ComplianceOne Documents

- When the keyword "By:____" is detected in a ComplianceOne document, a guarantor signature field is automatically added to the underscored area. (ES-611)

eDelivery

- eDelivery is enhanced. After documents are reviewed and signed in person, choose who receives the documents via secure email delivery. Previously, all signers/reviewers received the documents. (ES-1140)
    - On the eSignature Management page, checkboxes are provided next to each signer. By default, all signers/reviewers are selected as eDelivery recipients to receive the documents. Unselect anyone who should not receive the documents.
    - A pop-up confirmation shows the list of recipients and a list of those excluded from eDelivery.
    - The Detail Audit includes details about all parties involved in the session. The Session Audit records who received the documents via eDelivery.

Remote Transactions

- Set custom expiration dates for time sensitive remote transactions easily in eSign. (ES-1184)
    - Using the Transaction Expires in (Days) setting on the eSignature Settings page, administrators can configure how many days until the remote transaction expires for each remote message template.
    - Financial institution representatives can manually change the expiration using the Completion Deadline on the eSignature Management page depending on the permissions assigned to them. The Detailed Audit tracks changes made to the Completion Deadline from the eSignature Management page.
    - To use this feature, confirm that the Enable Expiration setting in your Adobe portal is turned on. If changes are made to the default number of days in the Adobe portal after a remote transaction is sent to your customer, the Adobe default takes precedence and eSign will be synced with the Adobe default at the next remote session status update.

- Select a default remote message template for specific document sets and documents. To streamline the signing process and reduce guesswork for your FI representative, a remote message template will be preselected on the eSignature Management page based on the document or document set that is part of the transaction. Because certain documents and documents sets require different messages, the document or document set's default remote message template will take precedence over the institution's default remote message template. In some scenarios, the default remote message template may not be the desired remote message template; therefore, FI representatives can select a different remote message template on the eSignature Management page as needed. (ES-1181)

Remote Attachments

- The design and usability of the Remote Attachment Template Maintenance and Request Remote Attachment user interfaces are updated. (ES-1180, ES-1076)

Collected Documents Page Enhancements (RTS)

The usability of the Collected Documents page is enhanced to make it easier to identify documents that do not belong in a session. The following enhancements were made to the page:

- eSign detects mismatched document index field values to prevent documents that do not belong in the session from being added to the document set. A warning message is displayed on the Collected Documents page. A warning popup window is displayed before the user can create a session or add the documents to an existing session. The Validate Collected Documents Page setting must be enabled by a Host Administrator to use this feature.
- Designate the document index fields that eSign will use to detect mismatched document index field values. To designate document index fields, the Check for Mismatches on Collected Documents Page setting on the Index Fields Maintenance page must be turned on. When the Check for Mismatches on Collected Documents Page setting is turned on for document index fields, on the Collected Documents page, the first two chosen document index fields will be displayed for each document by default, and the user can expand the document row to view any additional index fields.
- A time stamp is displayed in the document row to indicate when the document was successfully uploaded to eSign.
- Remove all selected documents with one click instead of deleting each document one at a time.
- Before documents are deleted, a confirmation window is displayed to prevent accidentally deleting documents.
- This feature is applicable to RTS environments. (ES-1756)

Party Review Options (RTS)

- The Party Review Options setting on the Document Maintenance (RTS) page is updated (ES-1835):
  - Review by all parties defined in the session
  - Review only by parties defined in this document
  - Review only by parties assigned fields in this document
- When a document template is set to "Review only by parties assigned fields in this document," the document will only be visible to parties that have fields assigned to them. If no parties are assigned to fields within the document, the document will be hidden from all parties in the session. Institution representatives with the appropriate permissions are still able to make changes to document visibility during the session as needed. (ES-1448)
- This feature is applicable to RTS environments.

Merging Signers (RTS)

- When merging parties on the eSignature Management page, the confirmation message that is displayed before the parties are merged is updated to be more user friendly. This enhancement is applicable to RTS environments. (ES-624)

PDF Flattening (RTS with API Integration)

- PDF flattening architecture is updated. This feature is applicable to RTS environments with API integration. (ES-1098)

Document Maintenance (XML)

- The exported CSV file from the Document Maintenance (XML) page provides details about criteria conditions. This enhancement is applicable to XML environments. (ES-401)

Get Document Set Lists (XML Using eSign REST API)

- Using GetDocumentSetList via eSign REST API, retrieve a list of document sets from eSign. (ES-853)

Security

- Password security and protocol is strengthened for internal file sharing. (ES-1721, ES-1920)
- Additional security enhancements are included in this release.

Fixes

This is a list of issues that have been fixed in this release:

- When verifying identity for an existing agreement created by eSign via Adobe Sign API, the country code +1 is associated with Canada instead of the United States in the Adobe Portal. (ES-1707)
- Radio button labels are missing during signing when templates are defined in eSign but the session is created via API. (ES-879)
- Radio groups in attachments shift positions during preview and signing when in landscape mode. (ES-959)
- On the Session Details page, the Display / Do Not Display icon is missing for attachments that have radio buttons. (ES-976)
- If a document is set to Always Archive and no parties are defined in it, the document is not displayed on the eSignature Management page for eSign API sessions. (ES-881)
- After deleting documents from an eSign API document set, signature fields are not identified and remote parties receive the wrong documents to sign. (ES-858)
- eSign API documents with short names or full names with spaces caused an error. To fix this, short names and full names in eSign API documents can have spaces. (ES-619)
- When a document is edited in Document Designer, eSign increases the date field font size, which causes the date field to be cut off. (ES-1865, ES-1949)
- When uploading the Starter Checks ZIP file, some PDFs are not uploaded to the source folder, and after manually updating the source folder with the missing PDFs, the Create Starter Checks menu option is not available. (ES-1718)
- eSign API is not validating the Partner ID when a URL to retrieve a saved session is called (GetURL). (ES-1127)
- When previewing an archived document in any web browser except Internet Explorer, signatures overlap photos if a signature pad was used. (ES-1782)

- When an index.txt file is in use by other applications, the index.txt file is reported as successfully sent to the imaging system even though it cannot be sent to the imaging system while in use. (ES-1913)
- If the Design button is clicked on the Session Details page, there is an error if the session was created using TeSignLite and the session has third-party attachments. (ES-2009)
- When an RTS document that is sent via eSign or TeSignLite API is matched to a template based on the document's full name (long name) instead of document type, an error occurs if there is party information associated with the template. (ES-2082)
- On the Search Completed Sessions page, index fields cannot be edited because the Save and Cancel buttons are not displayed. (ES-2083)
- After the signing process is completed, a sample image is displayed on the GemView device instead of a blank screen. (ES-2151, ES-2152)
- The Audit PDF is placed in the archive folder on the server in error scenarios when the database cannot be updated. (ES-1790)
- The Session History page displays the index title but does not display the index value when the indexes are not in sequential order in the database. (ES-2079)
- Session Status Push service does not automatically process queued documents when the database connection is lost and restored. (ES-1714)
- When phone authentication is selected, the session audit report lists the recipient's email address instead of the phone number. (ES-1765)
- eSign Client connectivity is lost after Retain Audit Trail (Days) are elapsed (default is 90 days) if Retain Audit Trail (Days) is set to a value less than the eSign Client Access Valid for (Days) setting (default is 365 days). (ES-1744)
- In some scenarios, the externally mapped index values provided in XML files are being replaced with other index values. (ES-1728)
- When a TrueImage imaging system XML file is generated, the Imaging Index Title is not used. (ES-1750)
- When the archived time and date index values of a document are converted to Universal Coordinated Time (UTC) before being sent to the imaging system, the time difference causes the document to have an archived time and date that occurs on the next day. For example, a document that is archived at 5:01 PM on May 1 in Pacific Time will be converted to 12:01 AM May 2 UTC. To fix this, the imaging system settings can be configured to follow the preferred time zone of the institution using the Imaging Default Time Zone setting on the Imaging System Settings page. (ES-1560)
- During in-person signing, the signature/initial date is generated based on the server time zone instead of the local workstation time zone. (ES-1142)
- The signature date field is missing in ComplianceOne documents. (ES-859)
- Dynamic anchor fields are displayed as unmapped fields in ComplianceOne documents. (ES-1651)