



Trust the Asset. Trust the Transaction.™

Command Center Administrator Guide



Table of Contents

Introduction	1
Command Center User Types	1
How to Use This Guide	1
Concepts and Actions	2
Guide Conventions	2
Scope	3
Global Configuration	3
Transaction-Level Configuration	3
SmartSign Web	5
Completion Statuses	5
Custom Errors.....	6
Destination Site.....	7
Default Signer Authentication Data	7
Destination Site Login.....	8
Destination Site Branding	8
Email Templates.....	10
Invitation Templates.....	10
ACTION: Adding Invitation Email Templates	12
ACTION: Editing Invitation Email Templates	13
ACTION: Deleting Invitation Email Templates	13
Receipt Templates.....	14
ACTION: Adding Receipt Email Templates	16
ACTION: Editing Receipt Email Templates	17

ACTION: Deleting Receipt Email Templates	17
Role Mapping Configurations.....	17
ESIGN Consent	18
Using eOriginal’s Consent Language.....	18
Overriding eOriginal’s ESIGN Consent Language	18
Customizing eOriginal’s ESIGN Consent Language	19
Embedded ESIGN Consent.....	20
Identity Verification	21
Out-Of-Wallet Authentication	21
Text/SMS Authentication	23
Signature Appearance	24
Signature Capture Options	24
Signature Appearance.....	25
URL Redirects	26
User Instructions	27
Custom Instructions	27
Receipt Page Instructions	28
User Interface Preferences	29
User Interface Preferences	29
Signer Receipts	30
Signing Room Button Color.....	31
Signature Reason.....	31
Command Center	32
Field Branding.....	32
Brandable Transaction Fields	32

Default Transaction Fields	33
User Interface.....	33
Workflow Rules.....	34
Email Notifications	34
External System Sync	35
Configuring Push Notifications.....	35
Adding Custom Headers.....	37
Failed External Sync Messages.....	38
Vault Actions	39
Automated Property Changes.....	39
Automated Custom Events	40
Automated Batch Actions	41
Accept Transfer.....	41
Confirm Transfer	42
Initiate a Paper Out	43
Initiate Transfer	44
Request MERS eDelivery.....	45
Submit Destruction.....	45
Watermark Rules.....	46
Configuring Watermark Rules.....	46
Adding a Watermark Rule.....	47
Editing A Watermark Rule	48
Deleting a Watermark Rule	49
Watermark Templates	50
Configuring Watermark Templates	51

PDF Properties	51
Obscure Signature Blocks Properties	52
Obscure Text Blocks Properties.....	52
Obscure Protected Blocks Properties.....	53
Watermark Properties	53
Previewing Watermarks	54
ACTION: Adding a Watermark Template	55
ACTION: Editing A Watermark Template	55
ACTION: Deleting a Watermark Template	55
Organization Administration	56
Organization Configuration	56
Organization Names	56
Address and Phone Information.....	56
Organization Contacts.....	57
Settings	57
Organization Links	58
Inviting a Parent Organization.....	59
Accepting a Parent Organization Invitation	59
ACTION: Sending a Parent Organization Invitation	60
ACTION: Accepting a Parent Organization Invitation	61
Configuring Child Organizations.....	62
Assigning Permissions in Child Organizations	63
ACTION: Assigning Container Permissions to Parent Organization Users in Child Organizations	63
Managing Child Organization Transactions in Workspace	64
Editing Organization Links	65

Deleting Organization Links	65
Organization Security	66
Security Settings	66
Password Complexity Policy	67
Concurrent Session Warning	67
Authorized IP Addresses.....	68
Vault Administration	69
API Users	69
Configuring API Users.....	69
ACTION: Adding API Users	71
ACTION: Editing API Users	71
Certificates	72
Certificate Validation	72
Certificate Configuration	73
Container Permissions	74
Configuring Container Permissions.....	75
Container Permission Definitions	76
ACTION: Adding a New Container Permission Set	78
ACTION: Editing a Container Permission Set	79
ACTION: Deleting a Container Permission Set	79
Custom Fields	80
ACTION: Adding a New Custom Field	81
ACTION: Editing a Custom Field	81
ACTION: Deleting a Custom Field	82
Document Retention Policies.....	83

Configuring Document Retention Policies	84
ACTION: Adding a New Document Retention Policy	85
ACTION: Editing a Document Retention Policy	86
ACTION: Deleting a Document Retention Policy	86
Document Types	87
Configuring Document Types	88
ACTION: Adding a New Document Type	90
ACTION: Editing a Document Type	91
ACTION: Deleting a Document Type	91
Group Permissions	92
Configuring Groups	93
Group Permission Definitions	94
ACTION: Adding a Group	95
ACTION: Editing a Group	95
ACTION: Deleting a Group	96
Signature Templates	97
Creating a New Template	97
Global Template Library	98
ACTION: Create an Unmapped Global Signature Template	100
Templates Mapped to Document Type	101
ACTION: Creating a Signature Template Mapped to an Existing Document Type	102
Status Values	103
Configuring Status Values	104
ACTION: Adding Status Values	104

ACTION: Editing Status Values.....	105
ACTION: Deleting Status Values.....	105
Transaction Retention Policies.....	106
Configuring Transaction Retention policies	107
ACTION: Adding a New Transaction Retention Policy.....	108
ACTION: Editing a Transaction Retention Policy	109
ACTION: Deleting a Transaction Retention Policy.....	109
Transaction Types.....	110
Configuring Transaction Types	110
Adding a New Transaction Type.....	113
Editing a Transaction Type	114
Deleting a Transaction Type.....	114
Transfer Partners.....	115
Inviting Transfer Partners.....	116
Accepting Transfer Partner Invitations.....	118
Editing a Sender Transfer Partner	120
Editing a Recipient Transfer Partner	120
ACTION: Inviting a Transfer Partner.....	121
ACTION: Accepting a Transfer Partner Invitation	121
Users.....	122
Configuring Command Center Users.....	122
Assigning Users to Groups.....	123
ACTION: Adding a User.....	124
ACTION: Editing a User.....	124
Appendix A: Business Entity Functions.....	125

Using the Business Entity Organization Menu	125
Viewing business entity organizations	126
Downloading a CSV-format file of business entity organizations	126
Viewing business entity users	127
Downloading a CSV-format file of business entity organizations	127
Adding business entity users	128
Editing business entity users	130
Linking business entity user accounts	130
Deactivating and reactivating business entity user accounts	131
Unlocking business entity user accounts	132
Viewing and editing business entity groups	132
Configuring security settings for business entity organizations	133
Appendix B: Configuring Adobe Connect	135
Document Mapping	135
Failed Messages	136
Adobe Webhook Configuration	137
Configuring Webhooks	137
Adding an Adobe Webhook	138
Deleting a Webhook	138

Introduction

Welcome to the Command Center Administrator Guide.

Command Center User Types

Command Center is a graphic user interface that is used to perform actions involving your organization's transactions and documents. The actions you perform using Command Center are largely determined by your company's workflow and the tasks that you perform in that workflow:

- *Users* prepare transactions for signature using Command Center SmartSign features and perform post-signing actions using Command Center eAsset Management features.
- *Administrators* create and manage user accounts. *Administrators* also manage all Command Center SmartSign and eAsset Management configuration settings.

This *Administrator Guide* provides information needed to perform your work as an Administrator of Command Center.

How to Use This Guide

This Administrator Guide describes all *Preferences* menu options needed to configure Command Center for your organization. The *Preferences* menu is organized into the following groups.

- SmartSign Web
- Command Center
- Workflow Rules
- Organization Administration
- Vault Administration

NOTE: The options contained in your Command Center Preferences menu will vary depending on your eCore implementation type and system permissions. Please contact Support (Help > Support in Command Center) if you have a problem accessing any Command Center features.

Concepts and Actions

This Guide uses two content types to provide information:

- *Concepts* – Text and graphical information define business terms and describe system functionality.
- *Actions* – Numbered steps guide users through specific tasks and processes in the software workflow.

As you proceed through the topics in this Guide, conceptual information is presented at the start of each section and is followed by associated actions. Command Center user interface features are described as you move through each section.

Actions are labeled (ACTION) in the headings and in the Table of Contents to distinguish them from concepts and to help you find information when you want to revisit a topic. In this way, the Command Center User Guide serves as both a tutorial for newer users and as a reference guide for more experienced users.

Guide Conventions

The following conventions are used throughout this Guide to help with navigation and comprehension.

<i>Italics</i>	Italics are used when referring to a specific Command Center feature such as a page, window, or field.
<u>Underline</u>	Underlined text contains linked references to other related sections in the Guide.
Bold	Bolded text is used to emphasize key aspects of the Command Center user interface.
ACTION	Stepped-out tasks/processes performed in Command Center are marked ACTION in both the section headings and the Table of Contents.
NOTE	The NOTE label alerts readers to context-sensitive and case-dependent system behavior.

Scope

The *Scope* drop-down menu allows you to apply configuration settings in two ways: globally, across all of your organization's transactions, or selectively, to individual transaction types.

Global Configuration

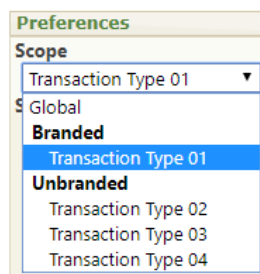
Select the *Global* option from the *Scope* drop-down menu when you want to make configuration changes that are applied universally to all transactions in your vault.

NOTE: When the *Global* option is selected, the *Preferences* menu displays a set of configuration options that are available based on your organization's implementation.

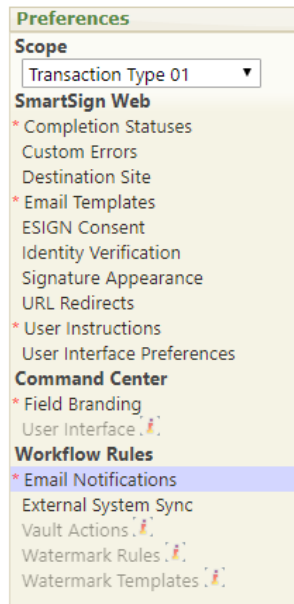
Transaction-Level Configuration

The *Scope* drop-down menu displays all active transaction types currently configured for your organization. When you select a transaction type from the *Scope* menu and make configuration changes, the changes are applied only to the selected transaction type (see [Transaction Types](#) for information).

When you apply configuration changes to an individual transaction type, that transaction type is moved from under the *Unbranded* heading to the *Branded* heading in the *Scope* drop-down menu.



Any *Preferences* option that has been changed for the selected transaction type displays a red asterisk.



SmartSign Web

This section describes all *SmartSign Web* Preferences options.


Completion Statuses

The *Completion Statuses* page is used to specify the transaction or document status that is applied when specific system events occur. Drop-down menus display options based on the statuses that are saved in the *Status Values* page. See [Status Values](#) for more information.

For transactions, status changes can be specified for completion, withdrawal, and expiration. For documents, status changes can be specified for completion, withdrawal, and document void.

Each option can also be set to *No Change*.

These settings are used as your **Global Settings**.

Completion Statuses: 

Transaction complete status:	<input type="text" value="--- No Change ---"/>
Transaction withdraw status:	<input type="text" value="--- No Change ---"/>
Transaction expired status:	<input type="text" value="--- No Change ---"/>
Document complete status:	<input type="text" value="--- No Change ---"/>
Document withdraw status:	<input type="text" value="--- No Change ---"/>
Document voided status:	<input type="text" value="--- No Change ---"/>

- Complete
- Expired
- Incomplete
- Signed
- Voided
- Withdrawn

Custom Errors

The *Custom Errors* page is used to compose and save message text to be displayed instead of the default SmartSign message in the event of a processing error. If no text is saved here, the default SmartSign message is used.

Configure error messages using the following fields:

- *Auto-text* - Click the buttons to place dynamic text fields in the *Error contact message* window (*Transaction ID*, *Sender First Name*, *Sender Last Name*, *Sender Email*).
- *Error contact message* - Type in the window to compose the error message content up to a maximum of 250 characters.

Error Messages:

Auto-text:

Error contact message:

Characters left: 250

Destination Site

The *Destination Site* page is used to configure the functionality and display of the SmartSign Signing Room Gateway and the Signing Room.

Default Signer Authentication Data

To gain access to the Signing Room, participants must provide authentication data (*Signer first name, Signer middle name, Signer last name, Signer email*).

Configure the Signing Room authentication fields by selecting one of the following default options:

- *No Default* - Fields are not populated when the Signing Room authentication window is displayed.
- *Default and Allow Editing* - Fields automatically populate but text can be overridden.
- *Default and Lock* - Fields automatically populate and cannot be edited.

Default Signer Authentication Data:

Signer first name:	No Default ▼
Signer middle name:	No Default ▼
Signer last name:	No Default ▼
Signer suffix:	No Default ▼
Signer email:	No Default ▼

Note: In the image, the dropdown menu for the 'Signer email' field is expanded, showing the following options: 'No Default' (highlighted in blue), 'Default and Allow Editing', and 'Default and Lock'.

Destination Site Login

The *Destination Site Login* section is used to enable or disable specific features used to sign in to the SmartSign signing room.

Configure the destination site login features using the following fields:

- *Allow participant to reassign on login* - Displays a *Send to someone else?* link that opens a *Reassign to another person* window.
- *Require a security code* - Requires a security code to be input when mapping participants during transaction creation. Once created, participants must input the security code during authentication to access the signing room.

Destination Site Login:

- Allow participant to reassign on login
- Require a security code

Destination Site Branding


The *Destination Site Branding* section is used to add custom branding to the destination site used to sign in to the SmartSign signing room.

Configure the destination site branding features using the following fields:

- *Text color* - Sets the color of the site title text.
- *Site title* - Used to input the text displayed at the top of the signing room window.
- *Company logo* - Click the *Choose File* button to browse for and select an image file to display in the signing room.
- *Logo preview* - Displays the active signing room Logo. Clicking *Remove Logo* deletes the active logo and results in no logo being displayed in the signing room. Clicking *Use Default Logo* displays an eOriginal logo in the signing room.


- *Title preview* - Displays the active signing room title based on the color and text you selected.
- *Send reminder ___ days before expiration* - Specifies when reminder emails are sent to participants based on the *Signing Rules Expiration Date* set during transaction creation.

Destination Site Branding:

Text color: 

Site title:

Company logo: No file chosen
Recommended image dimensions: 150 x 75 pixels

Logo preview:  [Remove Logo](#)

Title preview:

Send reminder days before expiration

Email Templates

The *Email Templates* page is used to create and manage invitation and receipt templates. You can also enable or disable the role mapping address book on this page.

Invitation Templates

SmartSign sends invitation emails to participants that when documents are ready to be viewed and signed. Each email contains an individualized link to the signing room.

Invitation email templates can be created and managed in the *Invitation Templates* area of the *Email Templates* page. Once created, users can select the pre-defined templates when creating a transaction.

Configured templates are displayed in table rows in the *Invitation Templates* area. A checkmark identifies the default template for the organization. Checkmarks also identify templates that use SmartSign standard language.

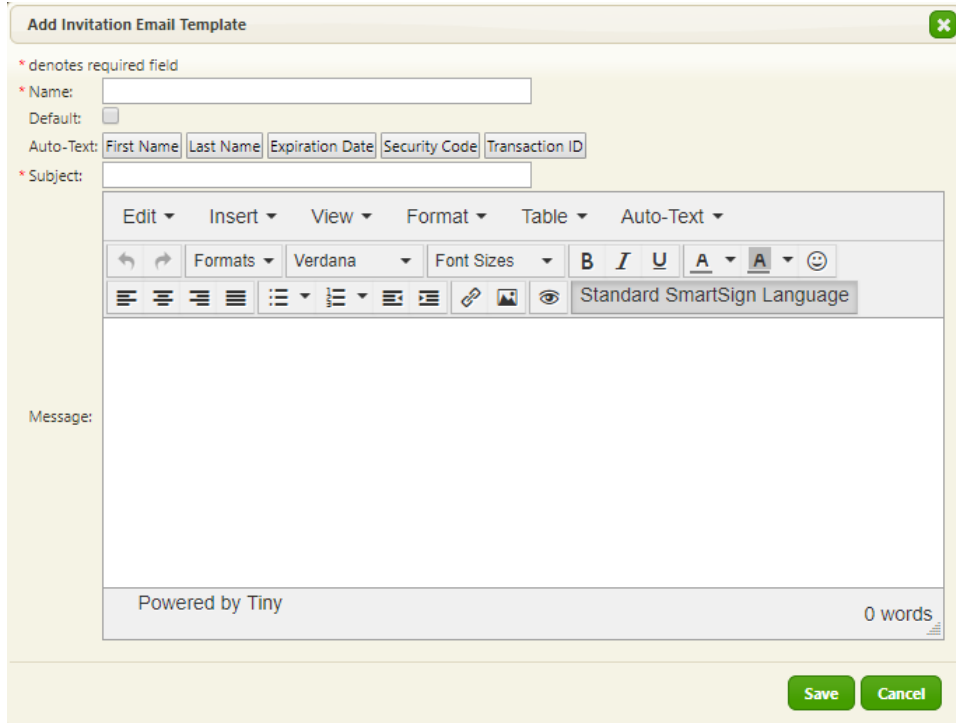
Invitation Templates:

[Add Invitation Template](#)

Template Name	Default	Include Standard Language	Actions
Sample Email Template 01	✓	✓	Preview Edit Delete Unset as default
Sample Email Template 02		✓	Preview Edit Delete Set as default
Sample Email Template 03			Preview Edit Delete Set as default

The following fields are used to create and manage invitation email templates in Command Center:

- *Name* - Input a unique identifier for the template.
- *Default* - Check to make the template the default template. Content from the default template is automatically included in the email editor when you compose the invitation email for a transaction.
- *Auto-Text* - Used to populate the *Subject* line with participant-specific data.
- *Subject* - Input subject content to be displayed at the top of every invitation email based on this template.
- *Message* - Input message content to be included in every invitation email based on this template. The *Standard SmartSign Language* option pre-selects a standard message introducing the applicant to the SmartSign Web service.



The screenshot shows a web form titled "Add Invitation Email Template" with a close button in the top right corner. The form includes several input fields and a large text editor. A legend indicates that an asterisk (*) denotes a required field. The "Name" field is required and is currently empty. The "Default" field is a checkbox that is unchecked. The "Auto-Text" field is a dropdown menu with options: "First Name", "Last Name", "Expiration Date", "Security Code", and "Transaction ID". The "Subject" field is required and is currently empty. Below the input fields is a rich text editor with a menu bar containing "Edit", "Insert", "View", "Format", "Table", and "Auto-Text". The editor toolbar includes icons for undo, redo, font face (Verdana), font size, bold, italic, underline, text color, background color, and a smiley face. The "Auto-Text" dropdown is set to "Standard SmartSign Language". The main text area is empty. At the bottom of the text area, it says "Powered by Tiny" and "0 words". At the bottom right of the form are "Save" and "Cancel" buttons.

ACTION: Adding Invitation Email Templates

To add a new invitation email template:

1. From the *Preferences* menu, click *Email Templates*.
2. Under *Invitation Templates*, click *Add Invitation Template*.

The *Add Invitation Email Template* window is displayed.

3. In the *Name* field, type a unique identifier for the template.
4. Optionally, check the *Default* checkbox to make the template you are creating the default template.
5. Type a custom message using the *Subject* and *Message* fields. Use the *Auto-Text* buttons to populate the email with participant-specific data as needed.

NOTE: When composing a custom email message, you **MUST** select the *URL Link* option from the *Auto-Text* pull-down menu to include the URL and token information as a link in the email invitation. Without this information, participants will not be able to access the signing room.

6. Click the *Save* button to finish adding the template.

ACTION: Editing Invitation Email Templates

To edit an existing invitation email template:

1. From the *Preferences* menu, click *Email Templates*.
2. Under *Invitation Templates*, click *Edit* in the row of the template you want to edit.

The *Edit Email Template* window is displayed.

3. Input or change information as needed.
4. Click *Save* to finish editing the template.

ACTION: Deleting Invitation Email Templates

To delete an invitation email template:

1. From the *Preferences* menu, click *Email Templates*.
2. Under *Invitation Templates*, click *Delete* in the row of the template you want to delete.
3. In the confirmation window, click *OK* to confirm the deletion.

Receipt Templates

The *Receipt Templates* area is used to create and edit email templates for receipt emails sent to participants following a signing event. Receipt templates that you configure here can be selected as the default template for signer notification emails on the [User Interface Preferences](#) page.

Configured templates are displayed in table rows in the *Receipt Templates* area. Checkmarks identify templates that use SmartSign standard language.

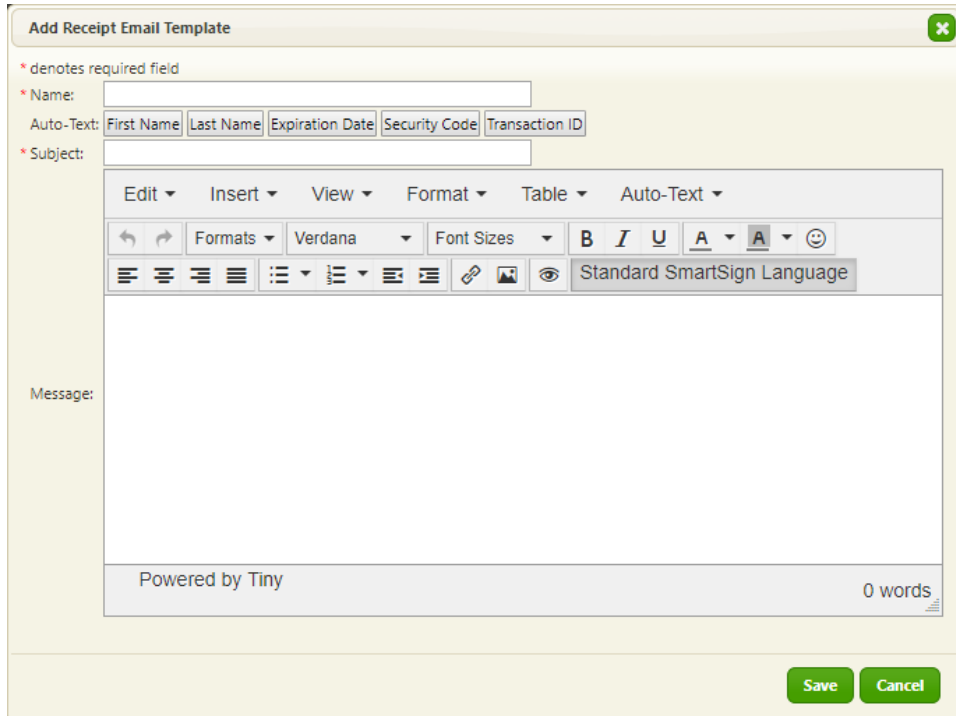
Receipt Templates:

[Add Receipt Template](#)

Template Name	Include Standard Language	Actions
Test receipt email 01	✓	Edit Delete
Test receipt email 02	✓	Edit Delete

The following fields are used to create and manage receipt email templates in Command Center:

- *Name* - Input a unique identifier for the template.
- *Auto-Text* - Used to populate the *Subject* line with participant-specific data.
- *Subject* - Input subject content to be displayed at the top of every receipt email based on this template.
- *Message* - Input message content to be included in every receipt email based on this template.



Add Receipt Email Template ✕

* denotes required field

* Name:

Auto-Text: First Name Last Name Expiration Date Security Code Transaction ID

* Subject:

Message:

Powered by Tiny 0 words

Save **Cancel**

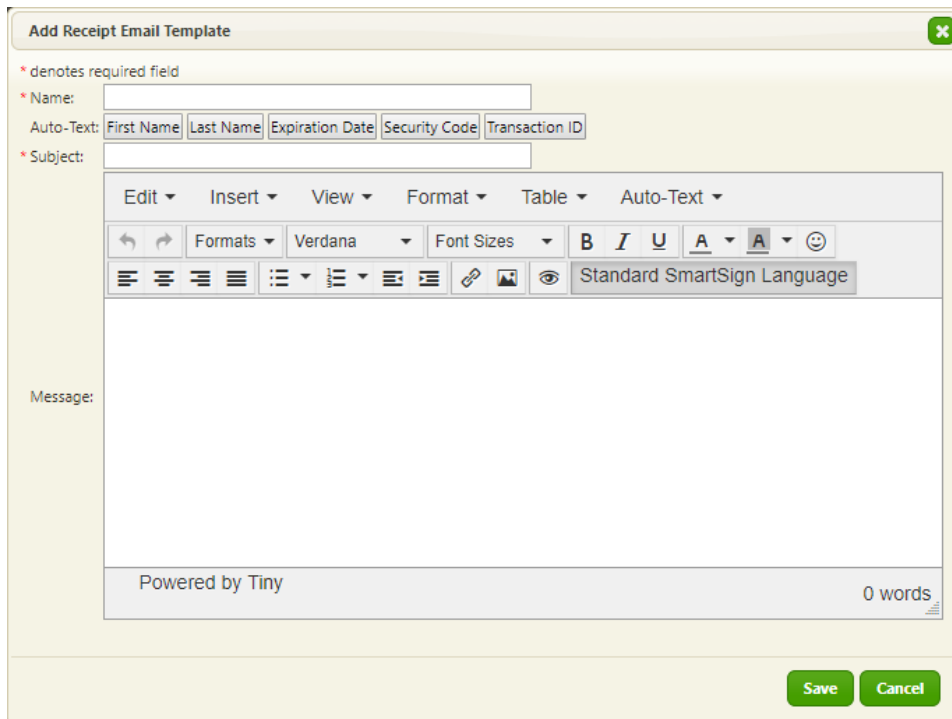
ACTION: Adding Receipt Email Templates

To add a new receipt email template:

1. From the *Preferences* menu, click *Email Templates*.
2. Under *Receipt Templates*, click *Add Receipt Template*.

The *Add Receipt Email Template* window is displayed.

3. In the *Name* field, type a unique identifier for the template.
4. Type a custom message using the *Subject* and *Message* fields. Use the *Auto-Text* buttons to populate the email template with dynamic participant-specific data as needed.



5. Click the *Save* button to finish adding the template.

ACTION: Editing Receipt Email Templates

To edit an existing receipt email template:

1. From the *Preferences* menu, click *Email Templates*.
2. Under *Receipt Templates*, click *Edit* in the row of the template you want to edit.

The *Edit Email Template* window is displayed.

3. Input or change information as needed.
4. Click *Save* to finish editing the template.

ACTION: Deleting Receipt Email Templates

To delete an receipt email template:

1. From the *Preferences* menu, click *Email Templates*.
2. Under *Reciept Templates*, click *Delete* in the row of the template you want to delete.
3. In the confirmation window, click *OK* to confirm the deletion.

Role Mapping Configurations

When the *Enable the role mapping address book* checkbox is checked, the first name, last name, and email address are auto-populated when mapping transaction participants based on the active address book.

Role Mapping Configurations: 

Enable the role mapping address book:

See *Account Information* in the *Command Center SmartSign User Guide* for more information on address book settings.

ESIGN Consent

The *ESIGN Consent* page is used to compose the *Consumer Disclosure and Consent* language that participants must review and agree to during signing room authentication. Organizations can choose from three options for composing the consent language:

- Use eOriginal's ESIGN Consent language
- Override eOriginal's ESIGN Consent language
- Customize eOriginal's ESIGN Consent language

Each time you edit the consent language using these options, you must click the *Save New ESIGN Consent Version* button to save the changes with a new version number. Using the *Retrieve ESIGN Consent Version* drop-down menu, you can select any saved version to be viewed on screen with the *Preview* button or downloaded as a PDF file with the *Download* button.

ESIGN Consent:

ESIGN Consent Preview

Retrieve ESIGN Consent Version:

Using eOriginal's Consent Language

This option presents signing room participants with the standard eOriginal consent language with no edits or additions.

Overriding eOriginal's ESIGN Consent Language

This option is used to present signing room participants with an alternative to eOriginal's consent language.

The *I will override...* option requires that an organization administrator acknowledges the company's responsibility to ensure that the language complies with applicable laws.

The *External Url* field is used to input the location where signing room participants can accessed the consent language.

- I will override eOriginal's ESIGN Consent language with my company's own.**

* denotes required field

I understand that it becomes our responsibility to ensure the language satisfies the requirements of ESIGN and other applicable laws.

Auto-text:

* External Url:

Customizing eOriginal's ESIGN Consent Language

The *I will customize...* option is used to edit eOriginal's consent language to include customized information.

Under *Purpose Statement*, you can input the following information to add a custom purpose statement to the consent language.

Under *Custom Paragraph*, you can add heading and body text to add a new, custom paragraph to the consent language.

The *Contact Information* fields are used to identify the company name and contact information. Information added to these fields is included in customized ESIGN Consent Language.

NOTE: You must provide your company contact information when using this option.

I will customize eOriginal's ESIGN Consent language.

Purpose Statement:

Transaction type:

Company name:

Purpose:

Purpose statement preview:

- You agree that your electronic signature indicates your intent to execute the <transaction type> with or at the request of <company name> for purposes of <purpose>.

Custom Paragraph:

Heading:

Paragraph text:

Characters left: 2500

Contact Information:

Company name:

Contact information:

Characters left: 250

Embedded ESIGN Consent

The *Embedded ESIGN Consent* section provides a checkbox used by organization administrators to acknowledge the company's responsibility to ensure that the language complies with applicable laws.

Embedded ESIGN Consent:

I will manage ESIGN Consent externally as part of my company's application that embeds the signing room. I understand that it becomes our responsibility to ensure our application and our ESIGN Consent language satisfies the requirements of ESIGN and other applicable laws.

Identity Verification

The *Identity Verification* page is used to enable and set up two different methods of secondary identify verification for transaction participants.

- Out-of-wallet (Electronic Verification Systems or EVS)
- Text/SMS

NOTE: Identity Verification options incur additional charges.

Out-Of-Wallet Authentication

Out-of-wallet authentication requires participants to answer challenge questions based on personal information including financial history and vehicle registration.

NOTE: This type of authentication is also called Know Your Customer (KYC) and Knowledge-Based Authorization (KBA) depending on the industry that is using it.

Configure the identity verification features using the following fields:


- *Out-of-wallet authentication* - Select *Electronic Verification Systems* to activate out-of-wallet authentication.
- *Number of attempts* - Sets the number of times a participant can attempt to verify identity before being locked out of the signing room.
- *Enable in-session retries for failed ID verifications* - Allows multiple attempts to pass the ID Challenge response questions, up to the number configured in *Maximum challenge questions*.
- *Maximum challenge questions* - Specifies the maximum number of challenge questions that can be asked (up to 10).
- *Maximum answer choices* - Specifies the maximum number of answers presented for each challenge question (up to 10).
- *Passing score* - Specifies how many challenge questions must be answered correctly to allow the participant to pass the challenge test. This setting defaults to 100%.

- *Store results report* - Saves a PDF report of the challenge questions, answers, and pass/fail results.
- *Document type* - Defines the document type used to store the challenge response report.

Identity Verification:


Please note that using one of our third party identity verification providers will incur an additional per use authentication fee.

* denotes required field

Out-of-wallet authentication: 

*Number of attempts:

Enable in-session retries for failed ID verifications:

*Maximum challenge questions: 

Maximum answer choices:

*Passing score: %

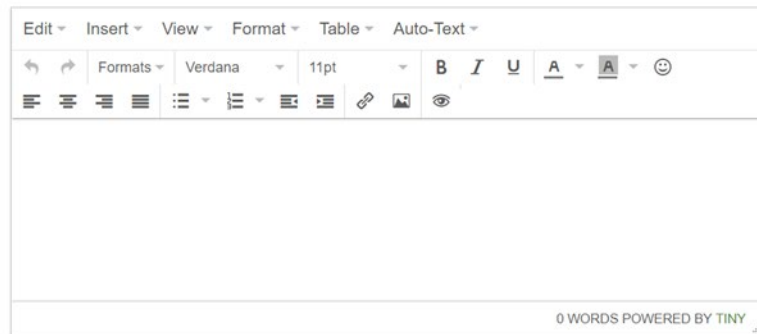
Store results report:

Document type:

You can input custom message text to be displayed in the user information and authentication challenge pages of the Signing Room. You can also format the custom text using toolbars and select dynamic text fields using the *Auto-Text* menu.

EVS ID Verification:

Authentication user information:




Text/SMS Authentication

Text/SMS authentication requires participants to input a PIN sent via text.

Configure the identity verification features using the following fields:

- *Text/SMS authentication* - Select *One-Time Use PIN* to activate Text/SMS authentication.
- *Number of attempts* - Maximum number of allowed PIN input attempts.
- *Enable in-session retries for failed PIN verifications*
- *Enable delivery of security code via text message* - Displays a *Send Security Code Via Text Message* field when mapping participants (see *Configuring the Signing Event* in the Command Center SmartSign User Guide for more information). The field is used to input the phone number where the security code should be sent.

Text/SMS authentication: 

Number of attempts:

Enable in-session retries for failed PIN verifications:

Enable delivery of security code via text message:

You can input custom message text to be displayed in the user information and authentication challenge pages of the Signing Room.

Click the *Auto-text* buttons to place dynamic text fields (*First* or *Last Name*, *Expiration Date*, *Security Code*, or *Transaction ID*) in any of the instruction message windows.

SMS/Text Authentication:

Auto-text:

Authentication user information:

Characters left: 2000

Authentication challenge:

Characters left: 2000

Signature Appearance

The *Signature Appearance* page is used to configure signing room features.


Signature Capture Options

The *Signature Capture Options* section contains options used to configure device behavior during a signing event.

Configure signature capture options using the following fields:

- *Signature capture mode* - Sets the default mode:
 - *Manual* – Requires participants to type or draw a signature in each signature location of the transaction.
 - *Acknowledged* – Prompts participants to accept system-generated electronic signatures in each signature area. Participants click to apply the accepted signature.
- *Do not optimize text signatures for devices with touch screens*
- *Collect biometric voice verification when possible* - Activates the ability to record a statement and secure the recording to the document.
- *Collect biometric picture verification when possible* - Activates the ability to take a picture of the participant at signing and secure the picture to the document.
- *Use participant's local time zone for dates and times* - Applies dates and times from the participant's local time zone when signatures are captured.

Signature Capture Options:


- Signature capture mode: Manual Acknowledged
- Do not optimize text signatures for devices with touch screens: 
 - Collect biometric voice verification when possible
 - Collect biometric picture verification when possible
 - Use participant's local time zone for dates and times

Signature Appearance

The *Signature Appearance* section contains options used to define participant signature display characteristics during a signing event.


Configure signature appearance options using the following fields:


- Default signature type - Sets the default method for applying a signature to an electronic document:
 - *Type (keyboard)* – The participants name is spelled out in cursive script as it is typed into the *First Name*, *Middle*, and *Last Name* fields.
 - *Draw (mouse or pad device)* – The participant must click in the *Signature* box and draw a signature using a mouse or a stylus.
- *Font and color*
- *Text signature preview* - Provides a sample signature based on the font and color selected.
- *Font size*
- *Horizontal/Vertical alignment* - Sets the default position of participant signatures.
- *Apply border to signature*
- *Drawn signature preview and color*


Signature Appearance: 

Default signature type:

Lock signature to default type:

Font and color: 



Text signature preview: 

Font size: 

Horizontal alignment:

Vertical alignment:

Apply border to signature:

Drawn signature preview and color:  


URL Redirects

The *URL Redirects* page is used to map pages that are displayed in a participant's browser window following specific signing room events.

The following fields are used to input URLs for specific redirect pages.

- *Completion forward URL*
- *Save progress forward URL*
- *Opt-out forward URL*
- *On error forward URL*

Auto-text buttons can be used to add dynamic participant-specific information to the URL, including *First Name*, *Last Name*, *Email*, *Role*, *Transaction Vault ID*, *Error Message*, and *Error Code*.

URL Redirects: 

Auto-text:

First Name	Last Name	Email	Role	Transaction Vault ID	Error Message	Error Code
------------	-----------	-------	------	----------------------	---------------	------------

Completion forward URL:

Save progress forward URL:

Opt-out forward URL:

On error forward URL:

User Instructions

The *User Instructions* page is used to compose message content that is presented to participants in the signing room and in the signing room receipt page.

Custom Instructions

The *Custom Instructions* section is used to compose and save message text to be displayed in the following areas:

- *Attach document instructions* - Content displays when a participant is required to upload a document into a transaction.
- *Wet-ink instructions* - Content displays when a participant is required to wet-ink sign a document.
- *Data collection instructions* - Content displays when a participant is required to input data in a form.
- *Withdraw consent instructions* Content displays in the window that is displayed when a participant clicks the *I decline to eSign* link.

Custom Instructions:

Auto-text:	<input type="text"/> First Name	<input type="text"/> Last Name	<input type="text"/> Expiration Date	<input type="text"/> Security Code	<input type="text"/> Transaction ID
Attach document instructions:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>				
	Characters left: 2500				
Auto-text:	<input type="text"/> First Name	<input type="text"/> Last Name	<input type="text"/> Expiration Date	<input type="text"/> Security Code	<input type="text"/> Transaction ID
Wet-ink instructions:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>				
	Characters left: 2500				
Data collection instructions:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>				
	Characters left: 2500				
Withdraw consent instructions:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>				
	Characters left: 500				

Receipt Page Instructions

Text input here displays in receipt page that is displayed at the end of a signing event.

NOTE: The *Display receipt page in the signing room* checkbox in the *User Interface Preferences* page must be checked for participants to view this text.

Receipt Page Instructions:

Receipt page text:

Characters left: 500

User Interface Preferences

The *User Interface Preferences* page is used to enable and disable specific signing room features.

User Interface Preferences

Configure signing room UI features using the following fields:

- *Allow the signer to exit and come back later* - Displays a *Save And Exit* option in the signing room menu on the left side of the window.
- *Allow retrieval of documents in the "Your Progress" menu option* - Displays a *Download All Documents* option in the *Your Progress* window.
- *On Mobile/Tablet Device, Allow In-Session Save A Copy Option Via ____* - Select one of the following options:
 - *Email to Signer*
 - *Open in Browser*
- *Disable document zooming and always display the document at ____% of its original size* - Removes the *Zoom Out/Zoom In* options from the signing room menu and sets document viewer to a specific zoom value.
- *Continue to allow user re-entry into the signing room after all users have completed their required actions*
 - *Require signer authentication upon user re-entry into the signing room after all users have completed their required actions* - The *Continue to allow user re-entry...* option must also be checked for this option to be activated.
- *Show SSL Secured logo* - Displays the SSL Secured logo at the bottom of the signing room menu.
- *Show page thumbnails for navigation* - Displays a thumbnail version of each document page on the right side of the signing room. Clicking a thumbnail opens the associated page in the page viewer.
- *Enable Google Translation Services* - Displays a drop-down menu used to select a language to translate the signing room UI text.

User Interface Preferences: 

-
- Allow the signer to exit and come back later
 - Allow retrieval of documents in the "Your Progress" menu option
 - On Mobile/Tablet Device, Allow In-Session Save A Copy Option Via:
 - Disable document zooming and always display the document at % of its original size
 - Continue to allow user re-entry into the signing room after all users have completed their required actions
 - Require signer authentication upon user re-entry into the signing room after all users have completed their required actions
 - Show SSL Secured logo
 - Show page thumbnails for navigation
 - Enable Google Translation Services

Signer Receipts

The *Signer Receipts* section is used specify how participants are notified when a signing session is completed.

Configure signer receipt options using the following fields:


- *Notify all participants upon completion* - Sends a notification email when all participants have signed transaction documents.
- *Notify all participants upon completion and attach all documents* - Sends a notification email with pdf copies of the transaction documents attached when all participants have signed transaction documents.
- *Display receipt page in the signing room* - Checking this option enables the following sub-options:
 - *Email Documents*
 - *Email Documents Upon Completion*
 - *Display "Download As A Single PDF" link on receipt page*
 - *Display "View/Print" link on receipt page*
- *Receipt email template* - Select the default template for signer notification emails. This drop-down menu includes the names of all the receipt templates you have created and saved in the *Email Templates* page.

Signer Receipts:

- Notify all participants upon completion
- Notify all participants upon completion and attach all documents
- Display receipt page in the signing room
 - Email Documents
 - Email Documents Upon Completion
 - Display "Download As A Single PDF" link on receipt page
 - Display "View/Print" link on receipt page
- Receipt email template:

Signing Room Button Color


The *Signing Room Button Color* section is used to set the color of the buttons displayed in the signing room.

Signing Room Button Color: 

Blue Green Light Blue Orange Red White

Signature Reason

Text that you input in the *Signing Reason* field is displayed and must be agreed to prior to clicking the *Apply Signature* button in the signing room.

Signature Reason: 

Signing reason:

Command Center

This section describes all *Command Center* Preferences options.


Field Branding

The *Field Branding* page is used to customize the Command Center user interface field labels and layout.

Brandable Transaction Fields

The *Brandable Transaction Fields* area contains a list of fields that you can customize with terms suited to your industry and workflow.

When you change a field name here, the new field name is displayed throughout the Command Center user interface, including the *Create Transaction* page, in *Workspace*, and in the Snapshot View.

Brandable Transaction Fields: 

Transaction type:	<input type="text"/>
Transaction ID:	<input type="text"/>
Description:	<input type="text"/>
Status:	<input type="text"/>
External reference 1:	<input type="text"/>
External reference 2:	<input type="text"/>
External reference 3:	<input type="text"/>

Default Transaction Fields

The *Default Transaction Fields* area is used to customize the *Create Transaction* page to support your company’s workflow. For each field in the list, you can specify the following:

- Check the *Required* checkbox for any field you want to be mandatory when creating transactions.
- Select either *Primary Information* or *Additional Information* in the *Display* drop-down menu to determine where the field is placed in the *Create Transaction* page.

Changes to the *Default Transaction Fields* can be applied globally or at the transaction type level. See *Scope* for more information.

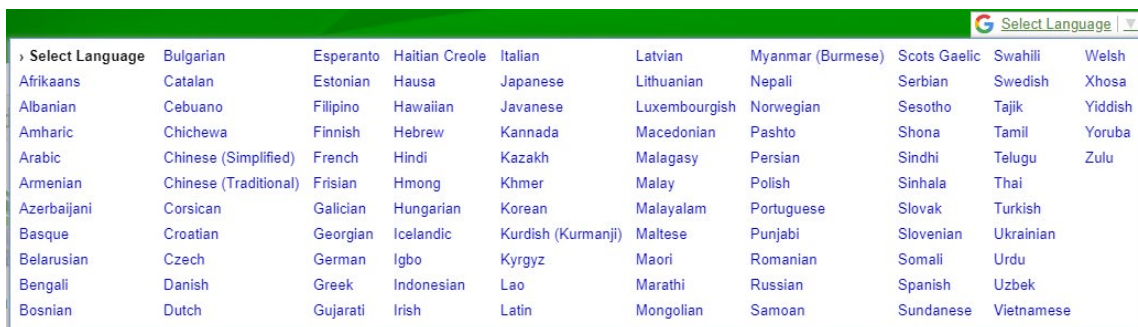
Default Transaction Fields: ⓘ

Field	Required	Display
Transaction ID:	<input checked="" type="checkbox"/>	Primary Information
Description:	<input checked="" type="checkbox"/>	Primary Information
Status:	<input type="checkbox"/>	Primary Information
Signing rules expiration date:	<input type="checkbox"/>	Primary Information
External reference 1:	<input type="checkbox"/>	Primary Information
External reference 2:	<input type="checkbox"/>	Primary Information
External reference 3:	<input type="checkbox"/>	Additional Information
Container permissions:	<input checked="" type="checkbox"/>	Primary Information
Retention policy:	<input checked="" type="checkbox"/>	Primary Information
Generate multiple copies:	<input type="checkbox"/>	Primary Information

User Interface

Checking the *Enable Google Translation Services* checkbox displays a *Select Language* drop-down menu at the top right of the Command Center user interface.

If this feature is activated, clicking the *Select Language* menu and selecting a language from the list translates and displays all user interface text in the selected language.



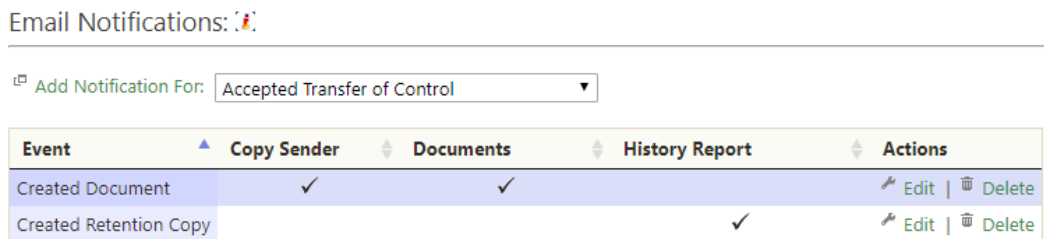
Workflow Rules

This section describes all *Workflow Rules* Preferences options.

Email Notifications

The *Email Notifications* page is used to create and edit email notifications that are sent when specific system events occur.

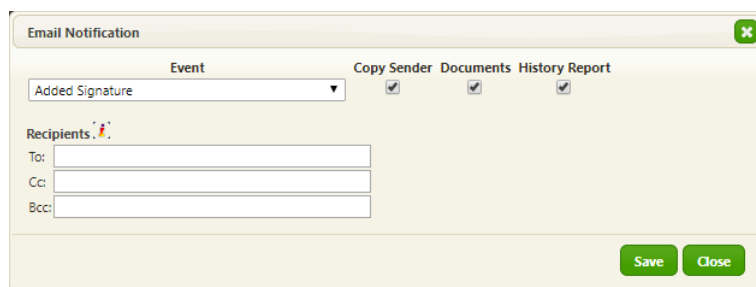
Configured notifications are displayed in table rows on the *Email Notifications* page. Checkmarks identify Copy Sender, Documents, and History Report settings for each notification.



Selecting an event name from the drop-down menu and clicking *Add Notification For* displays the *Email Notification* window.

The following fields are used to configure event-based email notifications:


- *Event* – Select the event that you want to trigger a notification.
- *Copy Sender* – If checked, sends a copy of the notification to your email address.
- *Documents* – If checked, includes transaction documents as an attachment to the notification email.
- *History Report* – If checked, includes a copy of the *Document History Report* as an attachment to the notification email.
- *Recipients* – Type email addresses of people to notify in the *To*, *CC*, and *BCC* fields. Separate addresses using commas.





External System Sync

The *External System Sync* page is used to configure push notifications that are sent to designated endpoints when specific system events occur.

Configured notifications are displayed in table rows in the *External System Sync* section. Checkmarks identify *Documents*, *Forms*, *History Report*, *Acknowledgement*, and *Forward/Delete* settings for each notification.

External System Sync:  Failed Messages

⊞ Add Notification For:

Event	WSDL Location	Documents	Forms	History Report	Acknowledgment	Forward/Delete	Actions
Transaction Fully Signed					✓		 Edit  Delete

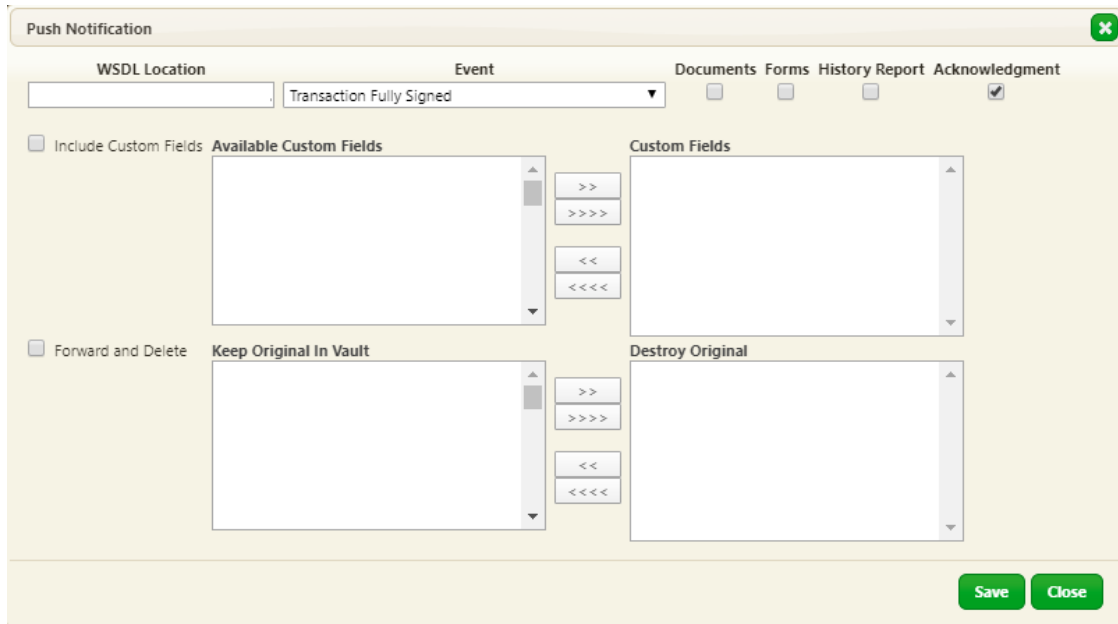
Selecting an event name from the drop-down menu and clicking *Add Notification For* displays the *Push Notification* window.

Configuring Push Notifications

The following fields are used to configure event-based push notifications:

- *WSDL Location* - Input the address of the endpoint Web Services Description Language (WSDL) file. eCore validates the *WSDL Location* during configuration.
- *Event* - Select the event that you want to trigger notifications.
- *Documents* - If checked, includes transaction documents as an attachment to the notification email.
- *Forms* - If checked, includes form field data as an attachment.
- *History Report* - If checked, includes a copy of the *Document History Report* as an attachment to the notification email.
- *Acknowledgement* - Specifies whether the configured endpoint is an acknowledgement-type WSDL.

- *Include Custom Fields* – When checked, allows specific custom field content to be included in the push notification by selecting from the *Available Custom Fields* list and moving to the *Custom Fields* list using the >> or >>>> buttons.
- *Forward and Delete* - When checked, allows specific document types to be selected from the *Keep Original in Vault* list and moved to the *Destroy Original* list using the >> or >>>> buttons.

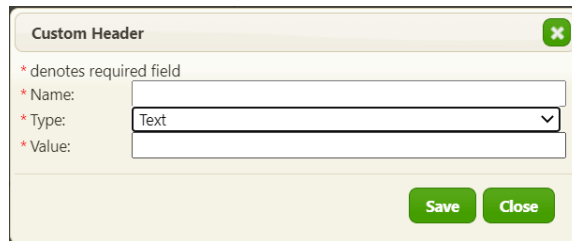


Adding Custom Headers

You can create custom HTTP headers for External System Sync messages. Saved headers are displayed in table rows in the *Custom Headers* section.



Clicking *Add Custom Header* in the *Custom Headers* section displays a window where a *Name*, *Type* (Text, Timestamp, or GUID), and *Value* can be input.



Failed External Sync Messages

The *Failed External Sync Messages* page displays failed message attempts in table rows including the following information:

- Notification Type
- Transaction Vault ID
- Failure Date
- Destination
- Error Message

A message indicates if there are no failed messages to display.

External System Sync retry logic is implemented so that, when a notification fails, a retry is sent after two minutes.

The cadence of attempted retries occurs as follows:

Retry Attempt	Wait Interval	Time Elapsed
1	2	2
2	4	6
3	8	14
4	16	30
5	32	62

Vault Actions

The *Vault Actions* section is used to configure automated workflow actions for an organization.

Automated Property Changes

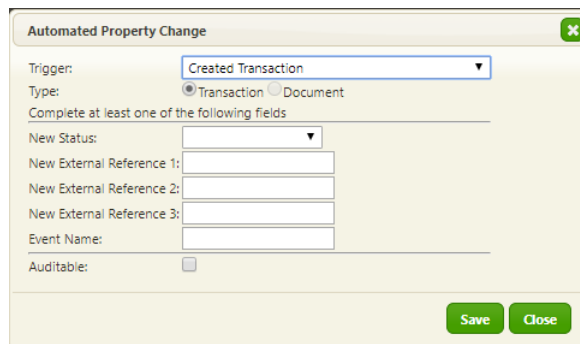
Automated property changes are used to prompt an update to a transaction or document when a specific trigger event occurs. You can configure the following property changes:

- Update a status
- Populate a specific external reference field
- Generate a custom event

Configured changes are displayed in table rows in the *Automated Property Changes* area.

Configure automated property changes using the following fields.

- *Trigger* - Used to select the action that initiates the property change.
- *Type* - Specifies whether a generic trigger occurs at the transaction or document level.
- *New Status* - Specifies the status that should be applied to the transaction or document following the trigger action.
- *New External Reference (1,2,3)* - Used to input content to populate the field following the trigger action.
- *Event Name* - Specifies an event name to be included in the transaction history following the trigger action.
- *Auditable* - When checked, the configured property change is digitally signed when the trigger actions occurs.



The screenshot shows a dialog box titled "Automated Property Change" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Trigger:** A dropdown menu with "Created Transaction" selected.
- Type:** Radio buttons for "Transaction" (selected) and "Document".
- Complete at least one of the following fields:** A section header above a group of fields.
- New Status:** A dropdown menu.
- New External Reference 1:** A text input field.
- New External Reference 2:** A text input field.
- New External Reference 3:** A text input field.
- Event Name:** A text input field.
- Auditable:** A checkbox that is currently unchecked.
- Buttons:** "Save" and "Close" buttons at the bottom right.

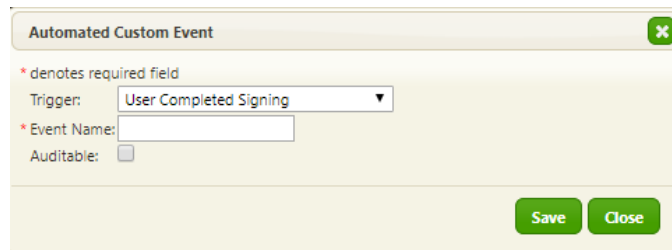
Automated Custom Events

The *Automated Custom Events* section is used to create event names that are recorded in a transaction's history when specific system events occur. Trigger events are selected from a drop-down menu list.

Configured events are displayed in table rows in the *Automated Custom Events* area.

Configure automated custom events using the following fields:

- *Trigger* - Used to select from a list of actions that causes a custom event to be recorded.
- *Event Name* - Specifies an event name to be included in the transaction history following the trigger action.
- *Auditable* - When checked, the custom event is digitally signed when the trigger action occurs.



The screenshot shows a form titled "Automated Custom Event" with a close button (X) in the top right corner. Below the title, there is a legend: "* denotes required field". The form contains three fields: "Trigger:" with a dropdown menu showing "User Completed Signing", "* Event Name:" with an empty text input field, and "Auditable:" with an unchecked checkbox. At the bottom right, there are two buttons: "Save" and "Close".

Automated Batch Actions

Automated batch actions are used to prompt a system action upon the occurrence of a specific system event.

Configured actions are displayed in table rows in the *Automated Batch Actions* area. Columns identify the *Trigger* and *Recipient* (if applicable) for each batch action.

Automated Batch Actions:

Trigger	Batch Action	Recipient	Actions
Status Changed To <i>Complete</i>	Initiate A Paper Out	John Smith	Edit Delete
Status Changed To <i>Expired</i>	Submit Destruction		Edit Delete

Accept Transfer

The *Accept Transfer* automated batch action automatically accepts transfer requests made by specified organizations.

Configure Accept Transfer automated batch actions using the following fields:

- *Batch Action* - Select the action type to be configured.
- *Transfer Initiated By* - Select the initiating organization that will trigger the *Accept Transfer* action. This menu is populated with organizations configured in [Transfer Partners](#).
- *Record of Transfer Template* - Select to use the default record of transfer template configured in [Document Types](#) or select *None*.

Automated Batch Action ✕

* denotes required field

* Batch Action:

* Transfer Initiated By:

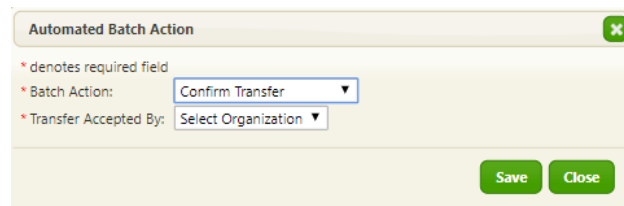
* Record of Transfer Template:

Confirm Transfer

The *Confirm Transfer* automated batch action automatically confirms transfer requests following acceptance by specified organizations.

Configure *Confirm Transfer* automated batch actions using the following fields:

- *Batch Action* - Select the action type to be configured.
- *Transfer Accepted By* - Select the accepting organization that will trigger the *Confirm Transfer* action. This menu is populated with organizations configured in Transfer Partners.



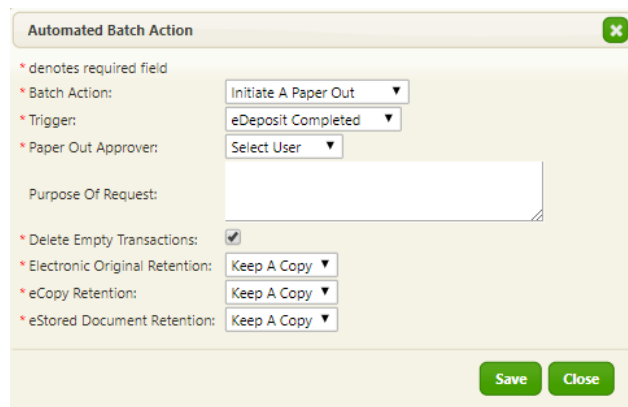
The screenshot shows a dialog box titled "Automated Batch Action" with a close button (X) in the top right corner. Below the title bar, there is a legend: "* denotes required field". There are two required fields: "Batch Action:" with a dropdown menu showing "Confirm Transfer", and "Transfer Accepted By:" with a dropdown menu showing "Select Organization". At the bottom right of the dialog box, there are two buttons: "Save" and "Close".

Initiate a Paper Out

The *Initiate a Paper Out* automated batch action automatically begins a *Paper Out* process when a specific event occurs during a transaction lifecycle.

Configure *Confirm Transfer* automated batch actions using the following fields:

- *Batch Action* - Select the action type to be configured.
- *Trigger* - Select the action that initiates the Paper Out process.
- *Paper Out Approver* - Select the approver of the request from the drop-down menu
- *Purpose Of Request* - Provide the reason for converting the document(s) to paper.
- *Delete Empty Transactions* - Check to remove transactions that contain no retention copies from the vault following the Paper Out process.
- *Retention fields* - Specify whether to retain Electronic Original, eCopy, or eStored documents or not following the action.



The screenshot shows a configuration window titled "Automated Batch Action" with a close button in the top right corner. The window contains several fields for configuring an automated batch action:

- Batch Action:** A dropdown menu with "Initiate A Paper Out" selected.
- Trigger:** A dropdown menu with "eDeposit Completed" selected.
- Paper Out Approver:** A dropdown menu with "Select User" selected.
- Purpose Of Request:** A text input field.
- Delete Empty Transactions:** A checkbox that is checked.
- Electronic Original Retention:** A dropdown menu with "Keep A Copy" selected.
- eCopy Retention:** A dropdown menu with "Keep A Copy" selected.
- eStored Document Retention:** A dropdown menu with "Keep A Copy" selected.

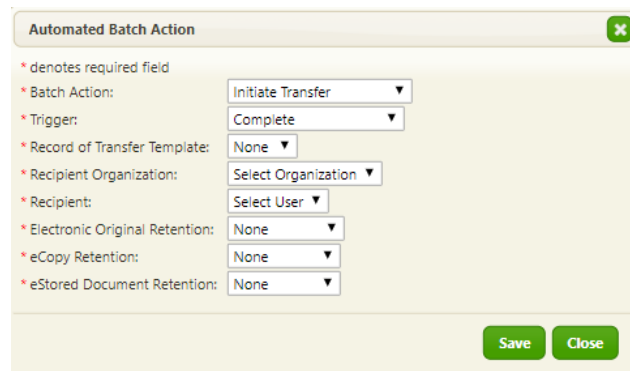
At the bottom right of the window, there are two buttons: "Save" and "Close".

Initiate Transfer

The *Initiate Transfer* automated batch action automatically starts the transfer process when a specific event occurs during a transaction lifecycle.

Configure Initiate Transfer automated batch actions using the following fields:

- *Batch Action* - Select the action type to be configured.
- *Trigger* - Select the action that initiates the Transfer process.
- *Record of Transfer Template* - Select to use the default record of transfer template configured in [Document Types](#) or select *None*.
- *Recipient Organization* - Select the recipient organization from the options in the drop-down menu. This menu is populated with organizations configured in [Transfer Partners](#).
- *Recipient* - Select the recipient user from the options in the drop-down menu.
- *Retention* fields - Specify whether to retain Electronic Original, eCopy, or eStored documents or not following the action.



The screenshot shows a dialog box titled "Automated Batch Action" with a close button (X) in the top right corner. The dialog contains several required fields, each marked with a red asterisk (*):

- Batch Action:** A dropdown menu with "Initiate Transfer" selected.
- Trigger:** A dropdown menu with "Complete" selected.
- Record of Transfer Template:** A dropdown menu with "None" selected.
- Recipient Organization:** A dropdown menu with "Select Organization" selected.
- Recipient:** A dropdown menu with "Select User" selected.
- Electronic Original Retention:** A dropdown menu with "None" selected.
- eCopy Retention:** A dropdown menu with "None" selected.
- eStored Document Retention:** A dropdown menu with "None" selected.

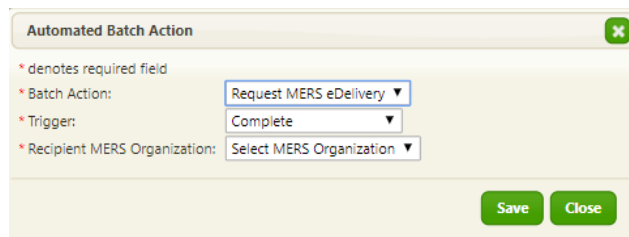
At the bottom right of the dialog, there are two buttons: "Save" and "Close".

Request MERS eDelivery

The *Request MERS eDelivery* automated batch action automatically initiates the eDelivery process when a specific event occurs during a transaction lifecycle.

Configure *Request MERS eDelivery* automated batch actions using the following fields:

- *Batch Action* - Select the action type to be configured.
- *Trigger* - Select the action that initiates the eDelivery process.
- *Recipient MERS Organization* - Select from a list of configured organizations. See the [MERS Configuration Guide](#) for information.



The screenshot shows a configuration window titled "Automated Batch Action" with a close button (X) in the top right corner. Below the title, there is a legend: "* denotes required field". The configuration fields are:

- * Batch Action: A dropdown menu with "Request MERS eDelivery" selected.
- * Trigger: A dropdown menu with "Complete" selected.
- * Recipient MERS Organization: A dropdown menu with "Select MERS Organization" selected.

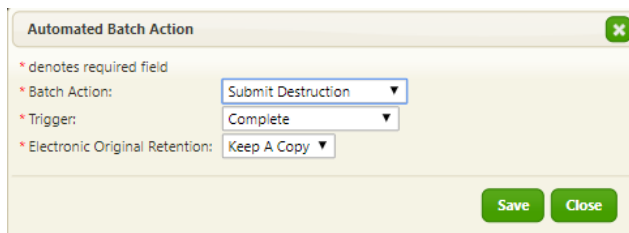
 At the bottom right of the window, there are two buttons: "Save" and "Close".

Submit Destruction

The *Submit Destruction* automated batch action automatically initiates the Destruction process when a specific event occurs during a transaction lifecycle.

Configure *Submit Destruction* automated batch actions using the following fields:

- *Batch Action* - Select the action type to be configured.
- *Trigger* - Select the action that initiates the Destruction process.
- *Electronic Original Retention* - Specify whether to retain Electronic Original documents or not following the action.



The screenshot shows a configuration window titled "Automated Batch Action" with a close button (X) in the top right corner. Below the title, there is a legend: "* denotes required field". The configuration fields are:

- * Batch Action: A dropdown menu with "Submit Destruction" selected.
- * Trigger: A dropdown menu with "Complete" selected.
- * Electronic Original Retention: A dropdown menu with "Keep A Copy" selected.

 At the bottom right of the window, there are two buttons: "Save" and "Close".

Watermark Rules

The *Watermark Rules* page provides the ability to override eOriginal’s default watermarks. This feature is used to create and edit watermark rules that trigger the application of custom watermark templates to documents. The application of a custom watermark can be set to trigger either a document status change or a transaction status change.

NOTE: You must configure at least one watermark template before creating a watermark rule. See [Watermark Templates](#) for information.

Configured watermark rules are displayed in table rows on the *Watermark Rules* page. Columns identify the *Document Type*, *Action*, *Vault Type*, and *Status* of each watermark rule.

Watermark Rules:

[Add Watermark Rule](#)

Document Type ▲	Action	Vault Type	Status	Watermark Template	Actions
All Document Types	Transfer of Control - Retention Copy	Any Vault Type	All States	Watermark Template 1	Edit Delete
All Document Types	Paper Out - Retention Copy	Any Vault Type	All States	Watermark Template 2	Edit Delete

The following actions can be performed on each rule in the list:

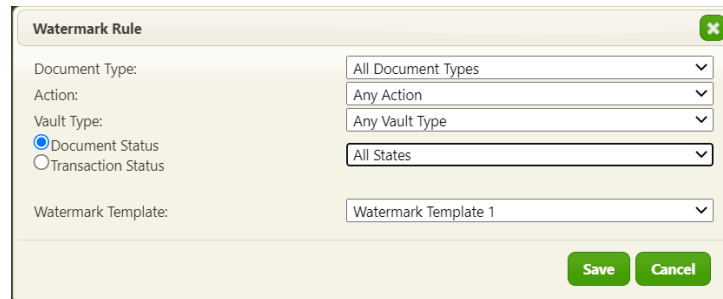
- *Edit* - Opens the configured rule in the *Watermark Rule* window.
- *Delete* - Displays a *Confirm Watermark Rule Deletion* window. Clicking *OK* removes the rule from the table.

Configuring Watermark Rules

The following fields are used to configure setting of new and existing watermark rules:

- *Document Type* - Select a configured document type to associate with the rule or select *All Document Types*.
- *Action* - Select an action to initiate the watermark rule or select *Any Action*.
- *Vault Type* - Select a vault type to associate with the rule or select *All Vault Types*.
- *Status* - Use the radio button to select *Document Status* or *Transaction Status* as the trigger for the rule. Then, select the status to associate with the rule or select *All States*. This drop-down menu populates based on statuses configured in the *Status Values* page.

- *Watermark Template* - Select the watermark template to apply when the watermark rule is initiated. This drop-down menu populates based on templates configured in the *Watermark Templates* page.



The image shows a 'Watermark Rule' configuration window. It contains the following fields:

- Document Type: All Document Types
- Action: Any Action
- Vault Type: Any Vault Type
- Document Status (selected) / Transaction Status: All States
- Watermark Template: Watermark Template 1

Buttons: Save, Cancel

Adding a Watermark Rule

To add a new watermark rule:

1. From the *Preferences* menu, click *Watermark Rules*.
2. Click *Add Watermark Rule*.

The *Watermark Rule* window is displayed.

3. Configure the watermark rule by selecting options from the following drop-down menus:
 - Document Type
 - Action
 - Vault Type
 - Document/Transaction Status

See [Configuring Watermark Rules](#) for information.

4. Select a template from the *Watermark Template* drop-down menu.

5. Click *Save* to finish adding the watermark rule.



The dialog box titled "Watermark Rule" contains the following fields:

- Document Type: All Document Types
- Action: Any Action
- Vault Type: Any Vault Type
- Document Status (selected): All States
- Transaction Status (unselected)
- Watermark Template: Watermark Template 1

Buttons: Save, Cancel

The rule is listed in the table on the *Watermark Rules* page.

NOTE: Please ensure that documents display as intended when rules are applied.

Editing A Watermark Rule

To edit an existing watermark rule:

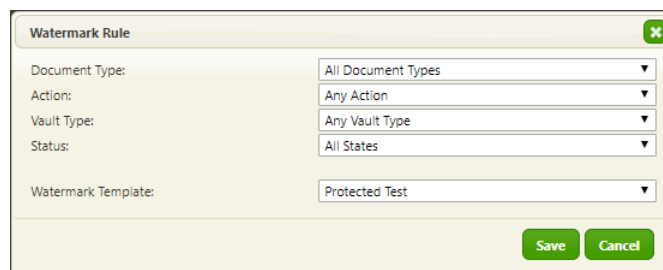
1. From the *Preferences* menu, click *Watermark Rules*.
2. Click *Edit* in the row of the rule you want to edit.

The *Watermark Rule* window is displayed.

3. Input or change information as needed.

See [Configuring Watermark Rules](#) for information.

4. Click *Save* to finish editing the rule.



The dialog box titled "Watermark Rule" contains the following fields:

- Document Type: All Document Types
- Action: Any Action
- Vault Type: Any Vault Type
- Status: All States
- Watermark Template: Protected Test

Buttons: Save, Cancel

The updated watermark rule is displayed in the table on the *Watermark Rules* page.

Deleting a Watermark Rule

To delete a watermark rule:

- 1.** From the *Preferences* menu, click *Watermark Rules*.
- 2.** Click *Delete* in the row of the rule you want to delete.
- 3.** In the confirmation window, click *OK* to confirm the deletion.

Watermark Templates

The *Watermark Templates* page is used to create and edit custom watermark templates. Watermark templates are applied to documents based on watermark rules that you configure in Command Center.

See [Watermark Rules](#) for information on creating and editing watermark rules.

Configured watermark templates are displayed in table rows on the *Watermark Templates* page.

Watermark Templates:

[Add Watermark Template](#)

Watermark Template Name ▲	Actions
Watermark Template 1	Edit Delete
Watermark Template 2	Edit Delete
Watermark Template 3	Edit Delete

The following actions can be performed on each template in the list:

- *Edit* - Opens the template in the *Watermark Template* window.
- *Delete* - Displays a *Confirm Watermark Template Deletion* window. Clicking *OK* removes the template from the table. **You cannot delete a watermark template if it is mapped to a watermark rule.**

Configuring Watermark Templates

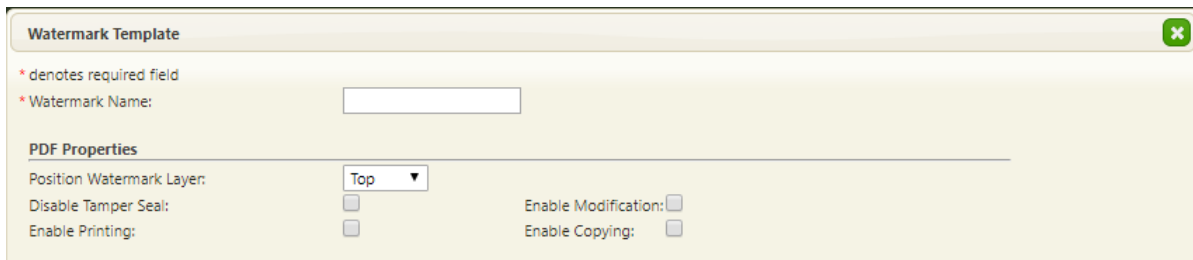
The following sections of the window are used to configure the properties of new and existing watermark templates.

PDF Properties

The *PDF Properties settings* are used to configure PDF file settings that are applied with the watermark template.

The following fields are used to change PDF properties for a watermark template:

- *Position Watermark Layer* - Select *Top* or *Bottom* from the drop-down menu.
- *Disable Tamper Seal* - **This checkbox must remain unchecked at all times.** The tamper seal is needed to meet the requirements of the Uniform Electronic Transactions Act (UETA) and Uniform Commercial Code (UCC) and to ensure that downloaded documents are not altered.
- *Enable Modification* - Allows for editing of downloaded documents.
- *Enable Printing* - Allows for printing of downloaded documents.
- *Enable Copying* - Allows for copying of content in downloaded documents.

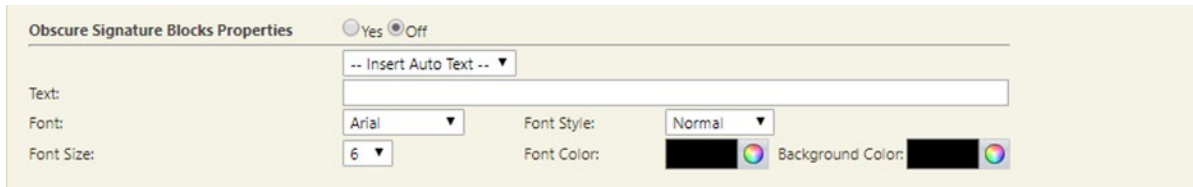


The screenshot shows a window titled "Watermark Template" with a close button in the top right corner. Below the title bar, there is a legend: "* denotes required field". The first field is "Watermark Name:" with an empty text input box. Below this is a section titled "PDF Properties" which contains four settings: "Position Watermark Layer:" with a dropdown menu set to "Top"; "Disable Tamper Seal:" with an unchecked checkbox; "Enable Modification:" with an unchecked checkbox; and "Enable Printing:" with an unchecked checkbox. The "Enable Copying:" checkbox is also present but its label is partially obscured by the "Enable Modification:" label.

Obscure Signature Blocks Properties

Selecting the *Yes* radio button for the *Obscure Signature Blocks Properties* option places text over all signature blocks when the watermark template is applied to a document.

See [Watermark Properties](#) for field descriptions.

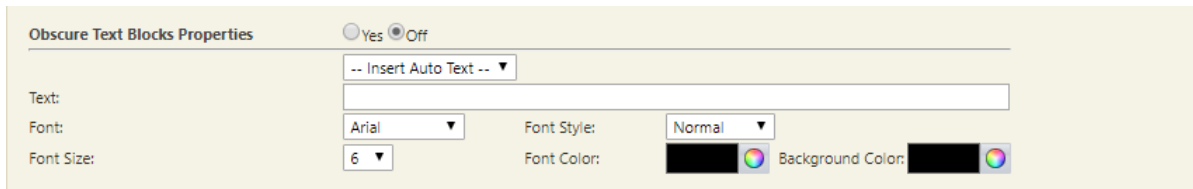


The screenshot shows the 'Obscure Signature Blocks Properties' configuration panel. At the top, there are radio buttons for 'Yes' and 'Off', with 'Off' selected. Below this is a dropdown menu with the text '-- Insert Auto Text --'. A large text input field is positioned below the dropdown. To the left of the input field are labels for 'Text:', 'Font:', and 'Font Size:'. The 'Font:' dropdown is set to 'Arial', and the 'Font Size:' dropdown is set to '6'. To the right of the input field are labels for 'Font Style:', 'Font Color:', and 'Background Color:'. The 'Font Style:' dropdown is set to 'Normal'. The 'Font Color:' and 'Background Color:' fields each have a black color swatch and a color selection icon.

Obscure Text Blocks Properties

Selecting the *Yes* radio button for the *Obscure Text Block Properties* option places text over all text blocks and multi-line text blocks when the watermark template is applied to a document.

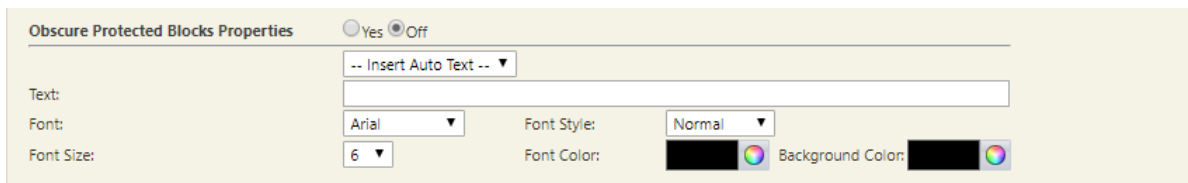
See [Watermark Properties](#) for field descriptions.



The screenshot shows the 'Obscure Text Blocks Properties' configuration panel. At the top, there are radio buttons for 'Yes' and 'Off', with 'Off' selected. Below this is a dropdown menu with the text '-- Insert Auto Text --'. A large text input field is positioned below the dropdown. To the left of the input field are labels for 'Text:', 'Font:', and 'Font Size:'. The 'Font:' dropdown is set to 'Arial', and the 'Font Size:' dropdown is set to '6'. To the right of the input field are labels for 'Font Style:', 'Font Color:', and 'Background Color:'. The 'Font Style:' dropdown is set to 'Normal'. The 'Font Color:' and 'Background Color:' fields each have a black color swatch and a color selection icon.

Obscure Protected Blocks Properties

Selecting the *Yes* radio button for the *Obscure Protected Block Properties* option places text over selected text blocks and multi-line text blocks. Text is placed over any *Text* field or *Multi-line Text* field you configured as *Protected* using the *Document Field Designer*. (see [Using the Document Field Designer](#) in the *Command Center SmartSign User Guide*).

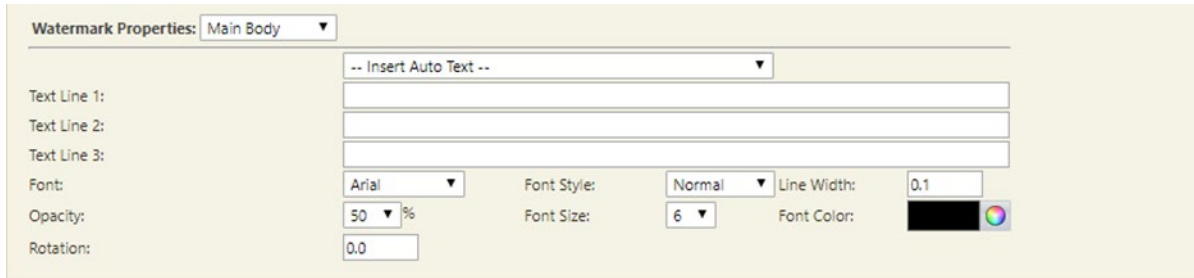


Watermark Properties

The *Watermark Properties* section is used to design and format the elements of the watermark template.

- A drop-down menu at the top of the *Watermark Properties* area is used to specify the location of the watermark:
 - *Bottom Margin*
 - *Left Margin*
 - *Main Body*
 - *Right Margin*
 - *Top Margin*
- *Text Line 1, 2, and 3* - The watermark may contain up to three lines of text. Each line must be defined individually. The text does not wrap and is limited to 250 characters per line.
- *Font* - Select one of four fonts to apply to the watermark text:
 - *Arial*
 - *Courier*
 - *Helvetica*
 - *TimesRoman*
- *Font Style* - Select one of five styles to apply to the watermark text:
 - *Bold*
 - *Bold-Italics*
 - *Italics*
 - *Normal*
 - *Outline*
- *Line Width* - Specify the thickness of the watermark characters.

- *Opacity* - Select the opacity level (0, 25, 50, 75, 100%) of the watermark text. The higher you set the opacity level, the darker the watermark text appears on the document.
- *Font Size* - Select the point size of the watermark text.
- *Font Color* - Select the color of the watermark text.
- *Rotation* - Specify the number of degrees to rotate the watermark text.



The image shows a 'Watermark Properties' dialog box. At the top, there is a dropdown menu for 'Watermark Properties' set to 'Main Body'. Below this is a dropdown menu for text selection, currently showing '-- Insert Auto Text --'. There are three text input fields labeled 'Text Line 1:', 'Text Line 2:', and 'Text Line 3:'. Below these are several configuration options: 'Font:' set to 'Arial', 'Font Style:' set to 'Normal', 'Line Width:' set to '0.1', 'Opacity:' set to '50 %', 'Font Size:' set to '6', 'Font Color:' with a black color swatch and a color picker icon, and 'Rotation:' set to '0.0'.

Previewing Watermarks

Clicking the *Preview* button opens a viewer window displaying the configured watermark against a blank background.



This image is a close-up of the bottom right portion of the 'Watermark Properties' dialog box. It shows the 'Font:' (Arial), 'Font Style:' (Normal), 'Line Width:' (0.1), 'Opacity:' (50 %), 'Font Size:' (6), and 'Font Color:' (black) settings. At the bottom right, there are three buttons: 'Preview', 'Save', and 'Cancel'. The 'Preview' button is highlighted with a red rectangular border.

ACTION: Adding a Watermark Template

To add a new watermark template:

1. From the *Preferences* menu, click *Watermark Templates*.
2. Click *Add Watermark Template*.

The *Watermark Template* window is displayed.

3. Configure the watermark template.

See [Configuring Watermark Templates](#) for information.

4. Click *Save* to finish adding the watermark template.

The template is listed in the table on the *Watermark Templates* page.

ACTION: Editing A Watermark Template

To edit an existing watermark template:

1. From the *Preferences* menu, click *Watermark Templates*.
2. Click *Edit* in the row of the template you want to edit.

The *Watermark Template* window is displayed.

3. Input or change information as needed.

See [Configuring Watermark Templates](#) for information.

4. Click *Save* to finish editing the template.

The updated watermark template is displayed in the table on the *Watermark Templates* page.

ACTION: Deleting a Watermark Template

To delete a watermark template:

1. From the *Preferences* menu, click *Watermark Templates*.
2. Click *Delete* in the row of the template you want to delete.
3. In the confirmation window, click *OK* to confirm the deletion.

Organization Administration

This section describes all *Organization Administration* Preferences options.

Organization Configuration

The *Organization Configuration* page displays account information for your organization as it is configured in eCore.

Contact Customer Support if you want to change any of the account information on the *Organization Configuration* page.

Organization Names

The following name types are used to identify organizations in Command Center:

- *Short name* – Every organization is assigned a unique, abbreviated name when it is created. This short name is only used when logging in to Command Center. **This short name should not be shared with anyone outside of your organization.**
- *Full Name* – Every organization is assigned a full name when it is created. This name serves as the primary identifier for the organization.
- *Nickname* – Optionally, a nickname can be assigned to an organization. If assigned, nicknames are displayed in parentheses next to the active username in the upper right corner of the Command Center window instead of the *Full Name*.

Address and Phone Information

The following fields are used to display contact information for the organization:

- *Address (Street address, City, State, Zip, and Country) fields*
- *Phone, Alternate phone, and Fax fields*

Organization Contacts

The following fields are used to display the names of organization personnel:

- *Executive contact*
- *Technical contact*
- *Billing contact*

Organization Configuration:

Account Information:

Short name:	Full name:
Street address:	Country:
Street address 2:	Phone:
Street address 3:	Alternate phone:
City:	Fax:
State:	Executive contact:
Zip:	Technical contact:
	Billing contact:

Settings

The *Settings* area contains time zone information for the organization based on geographical location.

Settings:

Preferred time zone: (America/New_York) Eastern Standard Time

Close

Organization Links

The *Organization Links* page is used by administrators who manage multiple organizations in Command Center. Linking organizations establishes *parent/child relationships* where parent organization users can access parent and child vaults simultaneously.

Once organization links are configured, a parent organization user can perform the following actions by signing into the parent organization:

- Configure child organizations, including granting permissions to child organization members and to himself or herself.
- Access and perform actions on transactions in the parent and child vaults.
- Generate reports that include data from transactions and documents in the parent and child vaults.

Configured organization links are displayed in table rows on the *Organization Links* page of both the parent and child organizations. The table rows contain the following information:

- *Organization* - Displays the name of a linked organization.
- *My Role* - Defines your relationship to the linked organization as either *Parent* or *Child*.

For child organizations, the *Actions* column displays a *Delete* button and an *Edit* button.

Organization Links:

Organization	My Role	Actions
Company A	Child	Edit Delete

For parent organizations, the *Actions* column displays a *Delete* button but no *Edit* option.

Organization Links:

Accept A Parent Organization Invitation

Organization	My Role	Actions
Company B	Parent	Delete
Company C	Parent	Delete

Inviting a Parent Organization

To establish a parent/child relationship, an administrator from a child organization must send an invitation to an administrator in the intended parent organization.

Clicking the *Invite a Parent Organization* button on the *Organization Links* page displays an *Invite Parent Organization* window used to input the email address for a configured administrator of the intended parent organization.

Checking the *Allow The Parent Organization To Control Its Own Access Rights* checkbox grants the parent organization the ability to configure the child organization. See [Configuring Child Organizations](#) for more information.

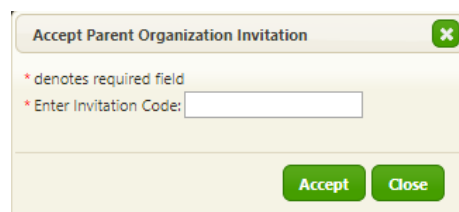


The intended parent organization receives an invitation email containing instructions for accepting the invitation, a link to Command Center, and an acceptance code.

Accepting a Parent Organization Invitation

Once the invitation email is received, clicking the *Accept a Parent Organization Invitation* in the *Organization Links* page displays the *Accept Parent Organization Invitation* window.

Inputting the *Invitation Code* from the email and clicking the *Accept* button completes the process of establishing an organization link. The child organization user receives a confirmation email once the parent organization user accepts the invitation.



Once the parent/child relationship is configured:

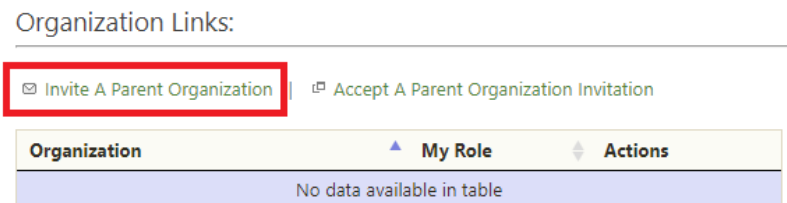
- A parent organization can accept invitations to serve as the parent to additional child organizations. A parent organization IS NOT ABLE to invite any organizations to serve as its parent.

A child organization IS NOT ABLE to act as a parent organization to another organization and can only have one parent.

ACTION: Sending a Parent Organization Invitation

To invite an organization to be a parent organization, perform the following steps:

1. Select *Preferences > Organization Links*.
2. In the *Organization Links* page, click *Invite a Parent Organization*.



3. Input an email address for a person who is a configured administrator of the intended parent organization.
4. Optionally, check the *Allow The Parent Organization To Control Its Own Access Rights* checkbox.

See [Configuring Child Organizations](#) for information.



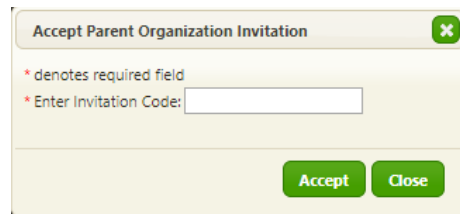
5. Optionally, type a note to include with the invitation email content.

Clicking the *Send* button sends an email containing instructions for accepting the invitation, a link to Command Center, and an acceptance code.

ACTION: Accepting a Parent Organization Invitation

To accept an invitation as a parent organization, perform the following steps

1. Select *Preferences > Organization Links*.
2. In the *Organization Links* page, click *Accept a Parent Organization Invitation*.
3. In the window that is displayed, input the *Invitation Code* from the email and click the *Accept* button.

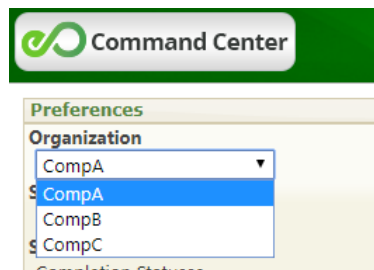


Once accepted, an email notification is sent to the child organization user, informing them that organization link has been established.

Configuring Child Organizations

To allow parent organization administrators the ability to configure child organizations, a drop-down menu is added to the Command Center *Preferences* page of a parent organization once it is linked to a child organization and the *Allow The Parent Organization To Control Its Own Access Rights* checkbox is checked.

Once configured, an *Organization* drop-down menu is displayed at the top of the *Preferences* menu for the parent organization. This menu includes the names of the parent organization and all linked child organizations that have *Allow The Parent Organization To Control Its Own Access Rights* checkbox checked.



The *Organization* menu allows administrators to make changes to *Preferences* settings for parent and child organizations while logged in to the parent organization. Preference setting changes are applied **ONLY TO** the organization that is currently selected in the *Organization* drop-down menu.

Assigning Permissions in Child Organizations

If the *Allow The Parent Organization To Control Its Own Access Rights* checkbox is checked by a child organization, a parent organization administrator can assign container permissions to users and groups within each linked child organization.

Additionally, an administrator can assign permissions to members of his or her own organization within a child organization.


ACTION: Assigning Container Permissions to Parent Organization Users in Child Organizations

To assign container permissions to members of a parent organization within a child organization:

1. Sign in to a parent organization.
2. Select a child organization from the *Organization* menu at the top of the *Preferences* menu.
3. From the *Preferences* menu, select *Container Permissions*.
4. On the *Container Permissions* page, click *Edit Permissions* for the permission set you want to update.

The *Edit Container Permissions* window is displayed.

5. In *Organization* column, select the name of the parent organization from the drop-down menu.



Organization Users/Groups	Status	Actions
CompB	-- Select --	All States
CompA		
CompB		

Save Close

6. Add permissions as needed, ensuring that the parent organization name is selected from the *Organization* drop-down menu for each added permission.

See [Container Permissions](#) for information.

7. Click Save to finish.

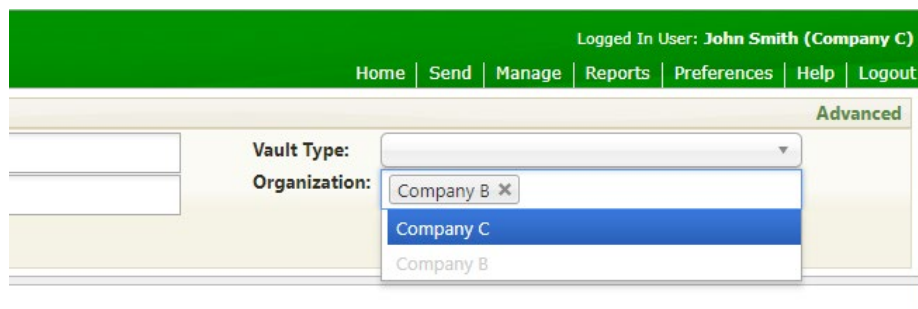
Managing Child Organization Transactions in Workspace

To allow parent organization users the ability to view, manage, and perform actions on transactions contained in child vaults, a drop-down menu is added to Command Center Workspace once it is linked to a child organization and the *Allow The Parent Organization To Control Its Own Access Rights* checkbox is checked.

Once configured, an *Organization* search field is displayed in the parent organization's Workspace page. The *Organization* search field replaces the *Signer Email* field under *Find Transactions*.

You can choose to include transactions from a parent vault and any child vault in search results by selecting the organization's name in the *Organization* drop-down menu. To remove an organization from the search criteria, click the X next to that organization's name in the menu list.

NOTE: Parent organization users must be assigned the necessary permissions in the child vault to view transactions in that vault. See [Assigning Permissions in Child Organizations](#) for information.



You can also display an *Organization* column in Workspace by selecting it from the *Show/hide columns* list. This column allows you to sort transactions based on the names of the child organizations selected in the *Organization* drop-down menu.

Editing Organization Links

In the *Organization Links* page of each child organization, clicking *Edit* in the *Actions* column displays the *Organization Link Settings* window.

You can check or uncheck the *Allow The Parent Organization To Control Its Own Access Rights* checkbox as needed.

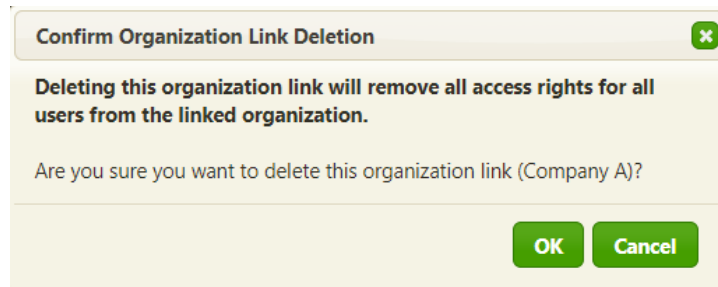
To send notification email(s) upon making a setting change, click *Send Alert* and populate the email address(es), subject, and body of the message.



Deleting Organization Links

A link between a parent and a child organization can be deleted at any time. The deletion can be performed by either the parent or the child organization.

In the *Organization Links* page, clicking *Delete* in the *Actions* column displays the *Confirm Organization Link Deletion* window. Clicking *OK* completes the deletion.



Organization Security

The Organization Security page is used to configure access and security settings.

Security Settings

The *Security Settings* fields are used to configure system access rules for all Command Center users

The following fields are used to change security settings for an organization:

- *Maximum bad logins before lockout* – Specifies the number of failed sign in attempts that can occur before user access is locked.
- *Lockout duration in minutes* – Specifies the number of minutes that a user is unable to sign in following a lockout. This field is grayed out if the *Lockout until an administrator unlocks* checkbox is checked.
- *Lockout until an administrator unlocks* – Requires that an administrator create a new temporary password for a user following a lockout. Overrides the *Lockout duration in minutes* value when checked.
- *Password expires in days* – Specifies the number of days that can pass before a password reset is required.
- *Number of saved passwords* – Sets the number of previously-used passwords that cannot be reused.
- *Enforce password expiration on API users* – When checked, applies the *Password expires in days* to API users.
- *Use two-factor authentication for login from untrusted devices* – When checked, sends an email with a PIN that must be entered when logging in to Command Center. Successive login attempts do not require entry of a PIN, provided the digital fingerprint of the device remains the same.

Settings:

* Maximum bad logins before lockout:	<input type="text"/>
* Lockout duration in minutes:	<input type="text"/>
Lockout until an administrator unlocks:	<input type="checkbox"/>
* Password expires in days:	<input type="text"/>
* Number of saved passwords:	<input type="text"/>
Enforce password expiration on API users:	<input type="checkbox"/>
Use two-factor authentication for login from untrusted devices:	<input type="checkbox"/>

Password Complexity Policy

Administrators configure password complexity rules for organizations, including:

- Minimum number of characters required
- Number of upper and lower case letters required
- Number of numeric characters required
- Number of special characters required

Password entry is case-sensitive and must adhere to the following set of strength requirements:

- Minimum eight characters in length
- Must contain **at least one** of each of the following:
 - Uppercase letter
 - Lowercase letter
 - Number
 - Special character

Concurrent Session Warning

The *Concurrent Session Warning* section is used to enable or disable a warning message that is displayed when a Command Center user account is accessed from more than one device simultaneously.

To activate, check the *Enable warnings for concurrent user logins to Command Center* checkbox.

Concurrent Session Warning: 
Enable warnings for concurrent user logins to Command Center:

Authorized IP Addresses

The Authorized IP Addresses section is used to input a range of authorized IP addresses for three different eCore user types:

- Command Center
- eCore Post API
- eCore SOAP API

Requests that are made from IP addresses outside of the configured range for each user type are denied and an error is returned.

Authorized IP Addresses:

System Name	Start	End	Action
Command Center	<input type="text"/>	<input type="text"/>	
Command Center			
eCore Post API			
eCore SOAP API			

On:

Clicking *Add New Range* displays a new row in the table. Create a new range by inputting information in the following fields:

- *System Name* - Select a user type for the range.
- *Start* - Input the first IP address in the range.
- *End* - Input the last IP address in the range

Once a range is added, a *Delete* button is displayed in the *Action* column. Clicking *Delete* removes the range.

Vault Administration

This section describes all *Vault Administration* Preferences options.

API Users

The *API Users* page is used to create “API Only” users (without Command Center access).

Configured API Users are displayed in table rows on the *API Users* page. Columns identify the Login ID, email address, and last login for each API User.

Configuring API Users

Input account information for the user using the fields in the *API User* window:

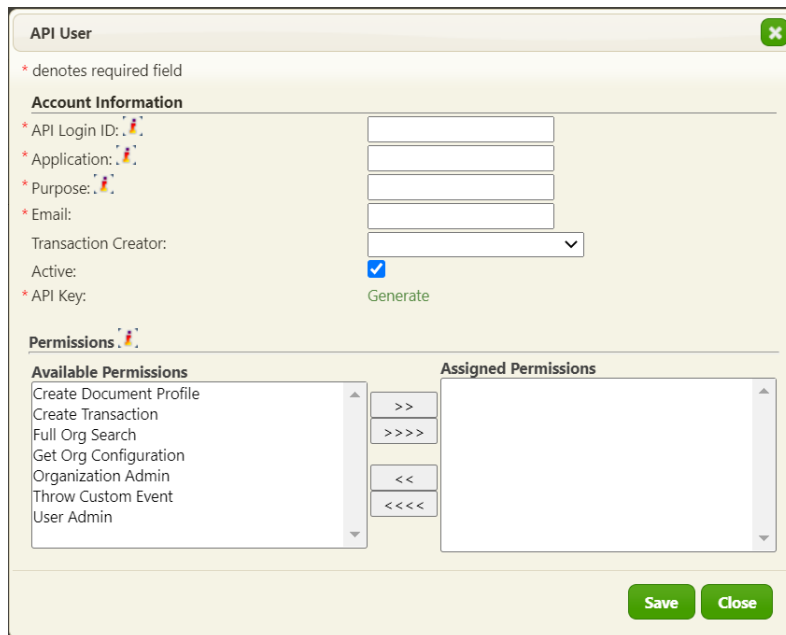
- *API Login ID* - The user name used to access the API via the eoLogin loginUsername parameter.
- *Application* - The name of the application using the API to be recorded in the eOriginal audit trail.
- *Purpose* - The reason the application is accessing eOriginal to be recorded in the eOriginal audit trail.
- *Email* - A valid email address that can accept emails from the notification system to be recorded in the eOriginal audit trail. This should be a generic email and not a personal email.
- *Transaction Creator* - Specifies a Transaction Creator value for a user. This value is logged in the audit trail of every transaction created by an API user. If no value is configured, the associated system name is logged upon transaction creation instead.

NOTE: API Users cannot sign into Command Center.

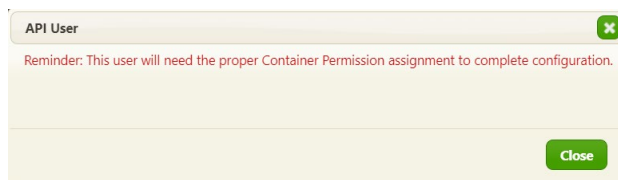
API users cannot be assigned to groups and must have permissions assigned directly. The permissions available to assign to API Users are:

- Create Document Profile
- Create Transaction
- Full Org Search
- Get Org Configuration
- Throw Custom Event
- Industry Admin
- Organization Admin
- User Admin

Clicking *Generate* in the API Key field generates a new API key. If an API key already exists for the user, it is replaced by the new key that is generated. A window is displayed warning that previous keys are no longer valid and that the new key will not be visible again.



Prior to saving a newly-created API user in Command Center, a message is displayed prompting the administrator to assign container permissions. This feature is intended to ensure that API users are correctly configured to receive complete API responses.



ACTION: Adding API Users

Perform the following steps to create an API user:

1. From the *Preferences* menu, select *API Users*.
2. In the *API Users* page, click *Add User*.
3. In the *API Login ID* field, type a unique username for the user.
4. In the *Application* field, type the user's first name.
5. In the *Purpose* field, type the user's last name.
6. Click *Generate* in the *API Key* field to create a new API key.
7. Assign permissions by selecting from the *Available Permissions* list and moving to the *Assigned Permissions* list using the >> or >>>> buttons. Permissions can be unassigned using the << or <<<< buttons.
8. Click *Save* to finish creating the user.

ACTION: Editing API Users

Perform the following steps to edit an API user:

1. From the *Preferences* menu, select *API Users*.
2. In the *API Users* page, under *Actions*, click *Edit* in the row of the user you want to edit.
3. Input or change information in the fields as necessary.

See [Configuring API Users](#) for information.

4. Optionally, click *Generate* in the *API Key* field to create a new API key.
5. Assign permissions by selecting from the *Available Permissions* list and moving to the *Assigned Permissions* list using the >> or >>>> buttons. Permissions can be unassigned using the << or <<<< buttons.
6. Click *Save* to finish editing the user.

Certificates

The Certificate Configuration page is used to activate certificate validation and manage .p12 file certificates for an organization.

Certificate Validation

The *Validation* section is used to configure a vault to either accept or reject documents that were signed using expired certificates. Checking the *Validate Signed Document Certificates* checkbox activates two radio buttons:

- *Accept Signed Documents That Don't Pass Validation*
- *Reject Signed Documents That Don't Pass Validation*

Certificate Configuration:

Validation:

Certificate validation settings will not take effect on any currently logged in user until their session renews.

Validate Signed Document Certificates:

Accept Signed Documents That Don't Pass Validation

Reject Signed Documents That Don't Pass Validation

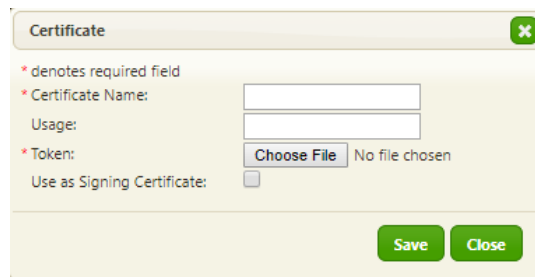
Certificate Configuration

The *Certificates* section is used to upload a private/public key set stored in a password-protected .p12 file. The keys are used to digitally sign PDF files.

Configured certificates are listed in a table. Clicking *Add Certificate* displays the *Certificate* window with the following fields:

- *Certificate Name* - Input a unique identifier for the certificate.
- *Usage* - Optionally, input a description for the certificate.
- *Token* - Click the *Choose File* button to select a .p12 file to upload. Command Center prompts for a certificate password.
- *Use as Signing Certificate* - Enables digital signing of documents using SmartSign.

If the checkbox is left unchecked, the certificate password is not stored in eCore. This is typically used for digitally signing documents via the eOriginal API.



The screenshot shows a window titled "Certificate" with a close button (X) in the top right corner. Below the title bar, there is a legend: "* denotes required field". The form contains the following fields and controls:

- * Certificate Name:** A text input field.
- Usage:** A text input field.
- * Token:** A file selection button labeled "Choose File" followed by the text "No file chosen".
- Use as Signing Certificate:** A checkbox.

At the bottom right of the window, there are two buttons: "Save" and "Close".

NOTE: eOriginal recommends using eOriginal's system certificates for signing PDFs in SmartSign rather than uploading .p12 files. If you do upload a file, you are responsible for maintaining it. If you let uploaded certificates expire or become invalid, you will not be able to sign documents.

Container Permissions

Command Center uses two types of permissions to provide system access to users: Container Permissions and [Group Permissions](#).

Group permissions can only be mapped to groups of users, but container permissions can be mapped to EITHER groups OR individual users. Container permissions are also more granular than group permissions. Typically, container permissions grant users the ability to perform a single transaction-level or document-level function.

The *Container Permissions* page is used to create container-level permission sets and assign them to Command Center users and groups. Container permission sets are mapped to every transaction and transaction type created in Command Center - **every organization must have a least one configured container permission set.**

Configured container permission sets are displayed in table rows on the *Container Permissions* page. A checkmark identifies the default set for the organization.

Container Permissions:

[Add Container Permissions](#)

Container Permissions in use cannot be deleted.

Name	Description	Default	Actions	In Use
Default Container Permissions		✓	Edit	✓ Where?

The following actions can be performed on each permission set in the list:

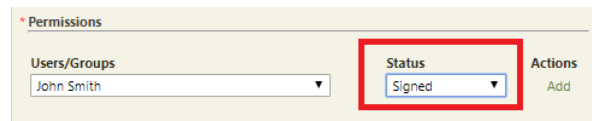
- Edit - Opens the permission set in the *Edit Container Permissions* window.
- *Where?* - Clicking this button displays a *Data Associated with Container Permission* window that lists containers and transaction types associated with the container permission set.

Configuring Container Permissions

Input information about the container permission set using the fields in the *Edit Container Permissions* window:

- *Name* – Input a unique identifier for the container permission set.
- *Description* – Optionally, input information describing the container permission set.
- *Active* – Specifies whether a document type is eligible to be mapped to transactions.
- *Default* – A container permission set as default is automatically selected when transactions are created.

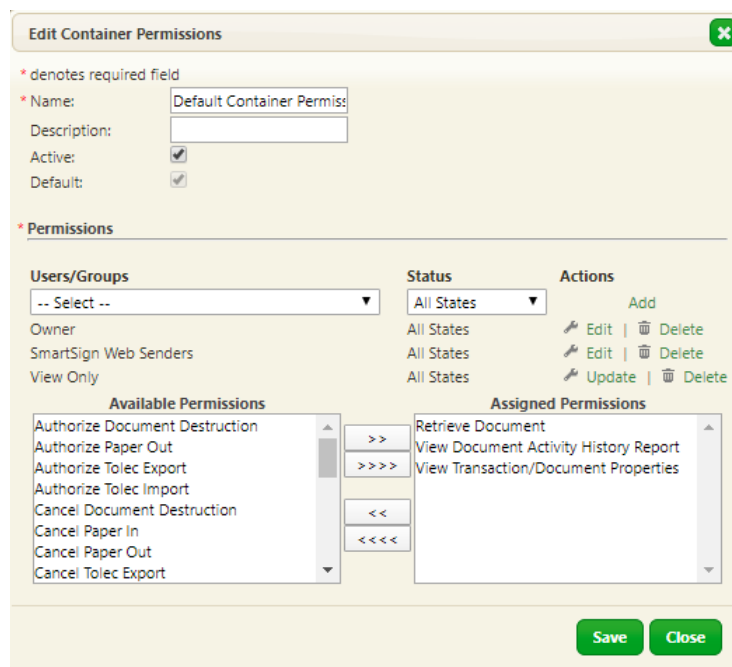
Container permissions can also be mapped to a transaction's status. You can assign one or more container permissions to be active **ONLY** for a specific transaction status.



The screenshot shows a section of the 'Edit Container Permissions' window. It includes a 'Users/Groups' dropdown menu with 'John Smith' selected, a 'Status' dropdown menu with 'Signed' selected (highlighted with a red box), and an 'Actions' section with an 'Add' button.

Assigning Container Permissions

Assign container permissions to groups by selecting from the *Available Permissions* list and moving to the *Assigned Permissions* list using the >> or >>>> buttons. Permissions can be unassigned using the << or <<<< buttons. See [Group Permissions](#) for information on Groups.



The screenshot shows the 'Edit Container Permissions' window. It includes a 'Name' field with 'Default Container Permissi...', a 'Description' field, and 'Active' and 'Default' checkboxes. Below is the 'Permissions' section with a 'Users/Groups' dropdown set to '-- Select --', a 'Status' dropdown set to 'All States', and an 'Actions' section with 'Add', 'Edit', and 'Delete' buttons. At the bottom, there are two lists: 'Available Permissions' and 'Assigned Permissions'. The 'Available Permissions' list includes 'Authorize Document Destruction', 'Authorize Paper Out', 'Authorize Tolec Export', 'Authorize Tolec Import', 'Cancel Document Destruction', 'Cancel Paper In', 'Cancel Paper Out', and 'Cancel Tolec Export'. The 'Assigned Permissions' list includes 'Retrieve Document', 'View Document Activity History Report', and 'View Transaction/Document Properties'. Between the lists are buttons for '>>', '>>>>', '<<', and '<<<<'. At the bottom right, there are 'Save' and 'Close' buttons.

Container Permission Definitions

The following table describes assignable container permissions.

Permission Name	Description
View Transaction/Document Properties	Allows a user to view values associated with a transaction or document.
Edit Transaction/Document Properties	Allows a user to change values associated with a transaction or document.
Retrieve Document	Allows a user to download a copy of any document.
View Document Activity History Report	Allows a user to view document history for any document.
Create New Version	Allows a user to perform any action that creates a retention copy (including uploading a document, performing a transfer of ownership, performing a paper out, or destroying a document).
Edit Encrypted Custom Field	Allows a user to change values associated with an encrypted custom field.
Get Encrypted Custom Field	Allows a user to view values associated with an encrypted custom field.

Additional container permissions permit specific actions and sub-actions on transactions and documents. The following table lists the container permissions required to perform these actions. The permission names describe the action being performed.

Action/Process	Container Permissions
Transfer of Control	Seller Initiate Transfer Seller Confirm Transfer Seller Cancel Transfer
Transfer of Location	Authorize Tolec Export Cancel Tolec Export Authorize Tolec Import Cancel Tolec Import
Certified Print	Certified Print
Paper In	Request Paper In Verify Paper In Cancel Paper In
Paper Out	Request Paper Out Authorize Paper Out Verify Paper Out Cancel Paper Out
Document Destruction	Request Document Destruction Reject Document Destruction Authorize Document Destruction Cancel Document Destruction
Delete Document Profile	Delete Document Profile
Delete Transaction	Delete Transaction

ACTION: Adding a New Container Permission Set

Perform the following steps to create a container permission set:

- 1.** From the *Preferences* menu, select *Container Permissions*.
- 2.** In the *Container Permissions* page, click *Add Permissions*.
- 3.** In the *Name* field, type a unique identifier for the permission set.
- 4.** If you want the permission set to be inactive, click the *Active* checkbox to uncheck it. The default status for a new permission set is *Active*.
- 5.** If you want to set the permission set as the default set, click the *Default* checkbox to check it.
- 6.** To add container permissions to the set:
 - a. In the *Permissions* area, select a user or a group from the *Users/Groups* drop-down menu.
 - b. If you want to restrict permissions to a specific transaction status, select it from the *Status* drop-down menu. The default status is *All States*.
 - c. Click the *Add* button.
 - d. Add permissions by selecting them from the *Available Permissions* list and moving them to the *Assigned Permissions* list using the >> or >>>> buttons.
 - e. Permissions can be removed from the set using the << or <<<< buttons.
- 7.** Repeat steps 6a through 6e to continue mapping permissions to users and groups.
- 8.** Click *Save* to finish creating the container permission set.

ACTION: Editing a Container Permission Set

Perform the following steps to edit a container permission set:

1. From the *Preferences* menu, select *Container Permissions*.
2. In the *Container Permissions* page, under *Actions*, click *Edit* in the row of the container permission set you want to edit.
3. Input or change information in the *Name*, *Description*, *Active*, or *Default* fields as necessary.

See [Configuring Container Permissions](#) for information.

4. To edit container permissions:
 - a. In the *Permissions* area, under *Actions*, click *Edit* for the user or group you want to edit.
 - b. Add permissions by selecting from the *Edit Container Permissions* list and moving to the *Assigned Permissions* list using the >> or >>>> buttons.
 - c. Remove permissions using the << or <<<< buttons.
5. Repeat steps 4a through 4c to continue editing permissions.
6. Click *Save* to finish editing the container permission set.

ACTION: Deleting a Container Permission Set

Perform the following steps to delete a container permission set:

1. From the *Preferences* menu, select *Container Permissions*.
2. In the *Container Permissions* page, under *Actions*, click *Delete* in the row of the container permission set you want to delete.

NOTE: The *Delete* option is not displayed if a container permission set is in use or if it is set as the default.

Custom Fields

Organizations use Command Center custom fields to collect and store information as part of their business workflow.

You can create three types of custom fields:

- *Transaction* - Configured custom fields are displayed in the *Create Transaction* page during transaction origination. Field content is displayed in the SnapShot view and can be edited in the *Update Transaction Properties* window following transaction creation. You can search in Workspace based on transaction-level custom field content and content can be displayed in search result columns in Workspace.
- *Document* - Custom field content can be input, viewed, and edited in the *Update Transaction Properties* window following transaction creation. Field content can also be input in the *Add New Document* window.
- *Global* - Selecting Global creates a separate transaction-level and document-level custom field with the same name.

Each custom field that you create is listed in the *Custom Fields* table along with the associated Scope and Type.

Custom Fields:

[Add New Custom Field](#)

Name	Scope	Type	Actions
Test Custom Field 1	Global	Text	Edit Delete
Test Custom Field 2	Global	Text	Edit Delete

For newly-created custom fields, options for editing and deleting are displayed in the *Actions* column. However, once a custom field is populated for a transaction or document, the *Edit* and *Delete* options are no longer available.

Configure custom fields using the following fields:

- *Name* - Input a unique identifier for the field.
- *Scope* - Define the field as transaction-level, document-level, or global.
- *Type* - Identifies the custom field as either a text or number field.

Custom Field ✕

* denotes required field

* Name:

* Scope:

* Type:

ACTION: Adding a New Custom Field

Perform the following steps to add a custom field:

1. From the *Preferences* menu, select *Custom Fields*.
2. In the *Custom Fields* page, click *Add New Custom Field*.
The *Custom Field* window is displayed.
3. Input a unique identifier for the custom field.
4. Specify whether the custom field is transaction-level, document-level, or both using the *Scope* drop-down menu.
5. Define the custom field as a text or number field using the *Type* drop-down menu.
6. Click *Save* to finish adding the custom field.

ACTION: Editing a Custom Field

Perform the following steps to edit a custom field:

NOTE: Only custom fields that have not been populated can be edited. Once a custom field has been populated for one or more transactions, the *Edit* option is no longer available.

1. From the *Preferences* menu, select *Custom Fields*.
2. In the *Custom Fields* page, click *Edit* in the *Actions* column for the custom field you want to edit.
The *Custom Field* window is displayed.
3. Make changes using the *Name*, *Scope*, and *Type* fields.
4. Click *Save* to finish editing the custom field.

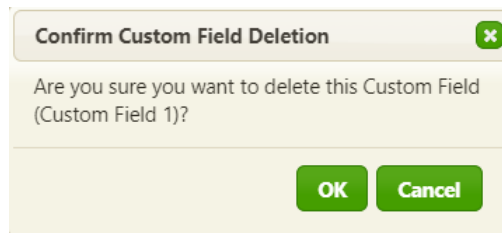
ACTION: Deleting a Custom Field

Perform the following steps to delete a custom field:

NOTE: Only custom fields that have not been populated can be deleted. Once a custom field has been populated for one or more transactions, the *Delete* option is no longer available.

1. From the *Preferences* menu, select *Custom Fields*.
2. In the *Custom Fields* page, click *Delete* in the *Actions* column for the custom field you want to edit.

The *Confirm Custom Field Deletion* window is displayed.



3. Click *OK* to confirm the deletion.

Document Retention Policies

The *Document Retention Policies* page is used to configure and maintain retention policies to be applied at the document level. Each retention policy defines expiration dates that are activated when specific statuses are applied during a document's lifecycle.

NOTE: You must define at least one default document retention policy for your organization. Every document and document type in your vault must be mapped to a document retention policy.

With retention policies defined, you can search and find documents in Workspace based on scheduled expiration dates using the *Expiring After* and *Expiring Before* search fields.

Configured retention policies are displayed in table rows in the *Document Retention Policies* page. Checkmarks identify the default retention policy and default transfer retention policy for the organization.

Document Retention Policies:

[Add Document Retention Policy](#)

Name	Description	Default	Default Transfer	Actions
Default Document Retention Policy		✓		Edit Delete
Policy 1			✓	Edit Delete
Policy 2				Edit Delete

The following actions can be performed on each policy in the list:

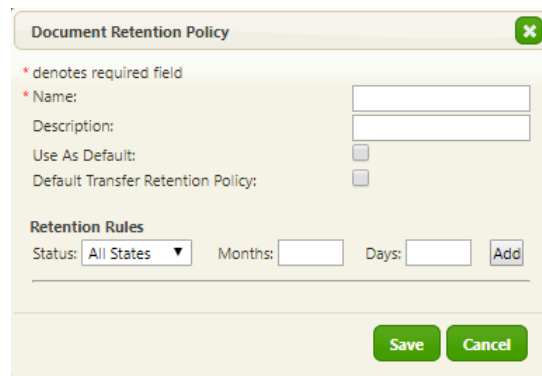
- *Edit* - Opens the policy in the *Document Retention Policy* window.
- *Delete* - Displays a *Confirm Retention Policy Deletion* window. Clicking *OK* removes the template from the table.

Clicking *Add Document Retention Policy* displays the *Document Retention Policy* window.

Configuring Document Retention Policies

The following fields are used to configure document retention policies:

- *Name* – Input a unique identifier for the retention policy.
- *Description* – Optionally, input text to differentiate the retention policy.
- *Use As Default* – Sets the policy as the default retention policy. This policy is automatically mapped to documents and document types when no other policy is selected.
- *Default Transfer Retention Policy* – Sets the policy as the default retention policy for transfer receipts.
- *Retention Rules* – Used to set the time period (in *Months* and *Days*) for retaining documents from the time a specific document status is achieved. Click the *Add* button to save the rule.



The screenshot shows a dialog box titled "Document Retention Policy" with a close button (X) in the top right corner. Below the title bar, there is a legend: "* denotes required field". The form contains the following fields and controls:

- Name:** A required text input field.
- Description:** A text input field.
- Use As Default:** A checkbox.
- Default Transfer Retention Policy:** A checkbox.
- Retention Rules:** A section containing:
 - Status:** A dropdown menu currently set to "All States".
 - Months:** A text input field.
 - Days:** A text input field.
 - Add:** A button to save the rule.

At the bottom of the dialog box, there are two buttons: "Save" and "Cancel".

ACTION: Adding a New Document Retention Policy

To create a new document retention policy:

1. From the *Preferences* menu, select *Document Retention Policies*.
2. In the *Document Retention Policies* page, click *Add Document Retention Policy*.

The *Document Retention Policy* window is displayed.

3. In the *Name* field, type a unique identifier for the transaction type.
4. Optionally, input a description for the policy.
5. In the *Document Retention Policy* window, under *Retention Rules*, select a status from the *Status* pull-down menu.
6. Use the *Months* and *Days* fields to specify the retention period for the selected status.
7. Click the *Add* button.
8. Repeat steps 5 through 7 to create additional retention rules.
9. Click *Save* to finish adding the document retention policy.

The new document retention policy is displayed in the *Document Retention Policies* page and the new policy is available to be mapped to document types.

ACTION: Editing a Document Retention Policy

To edit an existing document retention policy:

1. From the *Preferences* menu, select *Document Retention Policies*.
2. In the *Document Retention Policies* page, under *Actions*, click *Edit* in the row of the policy you want to edit.

The *Document Retention Policy* window is displayed.

3. Input or change information in the fields to edit the policy.

See [Configuring Document Retention Policies](#) for information.

4. Click *Save* to finish editing the policy.

ACTION: Deleting a Document Retention Policy

To delete a document retention policy:

1. From the *Preferences* menu, select *Document Retention Policies*.
2. In the *Document Retention Policies* page, under *Actions*, click *Delete* in the row of the policy you want to delete.

A confirmation window is displayed.

3. Click *OK* to confirm the deletion.

The policy is deleted and is no longer displayed in the *Document Retention Policies* page.


NOTE: You cannot delete a document retention policy once it is assigned to a document type.





Document Types

Document types are reusable document templates. Information and settings are pre-configured and saved in a document type, alleviating the need to input data each time a document is added to a transaction.

Configured document types are displayed in table rows in the *Document Types* page. Checkmarks specify whether a source file is mapped to the document type and whether the document type is active or not. *Signature Template* and *Versioning Policy* settings are identified for each document type, as defined later in this section.

Document Types:

 Add Document Type

Name ▲	Source File ⇅	Signature Template ⇅	Versioning Policy ⇅	Active ⇅	Actions
Sample 1			Keep most current version	✓	 Edit  Delete
Sample 2	✓		Keep most current version	✓	 Edit  Delete

The following actions can be performed on each document type in the list:

- *Edit* - Opens the type in the *Document Type* window.
- *Delete* - Displays a *Confirm Document Type Deletion* window. Clicking *OK* removes the document type from the table.

Clicking *Add Document Type* displays the *Document Type* window.

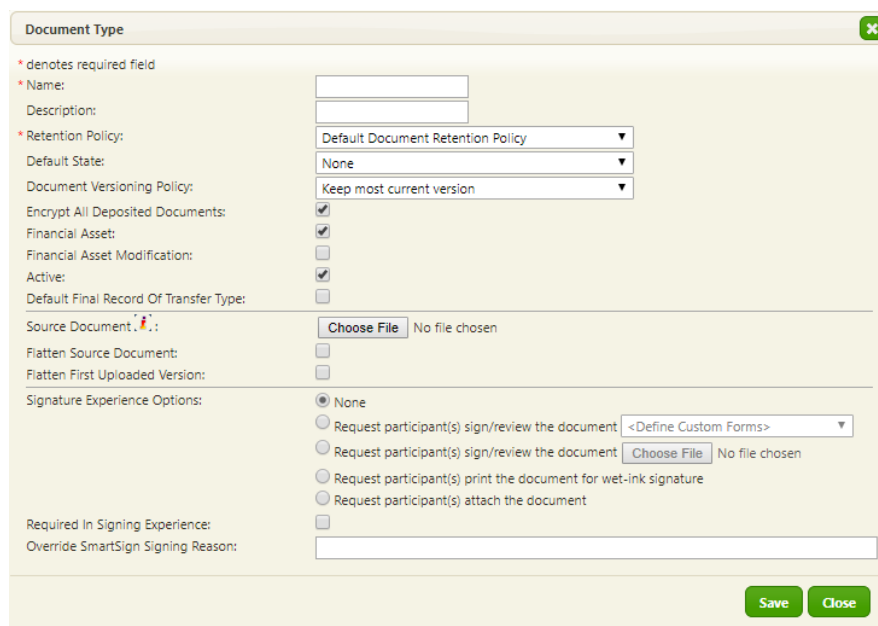
See [Document Types](#) in the *Command Center SmartSign User Guide* for more information.

Configuring Document Types

Document types can be configured using the following fields:

- *Name* – Input a unique identifier for the document type.
- *Description* – Optionally, input text to describe the document type.
- *Retention Policy* – Select a configured retention policy to associate it with the document type. See [Document Retention Policies](#) for information.
- *Default State* – Sets the initial status for documents created based on this document type.
- *Document Versioning Policy* – Select from a list to specify the document versions to retain throughout the document’s lifecycle:
 - Keep all signature versions
 - Keep all versions
 - Keep executable and all signature versions
 - Keep executable and last signature version
 - Keep most current version
- *Encrypt All Deposited Documents* – **This checkbox must remain checked at all times.**
- *Financial Asset* – A document that defines the financial terms of a transaction. **You can check either the Financial Asset checkbox OR the Financial Asset Modification checkbox. You cannot check both.**
- *Financial Asset Modification* – A document that amends the original Financial Asset. **You can check either the Financial Asset checkbox OR the Financial Asset Modification checkbox. You cannot check both.**
- *Active* – Specifies whether a document type is eligible to be included in transactions. The *Active* checkbox is checked by default for new document types. If the checkbox is unchecked, the document type cannot be selected when creating a transaction or a transaction type.
- *Default Final Record of Transfer Type* – When checked, the name of the document type is displayed in the *Record of Transfer Template* drop-down menu in the *Transfer of Control Request* window.
- *Source Document* – Optionally, select and upload a document file using the *Choose File* button. Once a source document is mapped to the document type, a *Retrieve* button can be clicked to open a PDF version of the document or a *Remove* button can be clicked to unmap the source document from the document type.

- *Flatten Source Document* – When checked, interactive elements in the source document are converted to static PDF elements when the source document is added to the document type.
- *Flatten First Uploaded Version* - When checked, interactive elements in the source document are converted to static PDF elements when the document type is mapped to a signature template.
- *Signing Experience Options* – Select a radio button to configure the signing experience for the document type. For more information on these options, see [Adding New Documents](#) in the Command Center SmartSign Web User Manual.
- *Required in Signing Experience* – When checked, this document cannot be skipped in the signing room. This box is checked by default for new document types.
- *Override SmartSign Signing Reason* – Used to input text to replace the default text that is displayed before clicking the *Apply Signature* button in the signing room.



The screenshot shows the 'Document Type' configuration form. It includes fields for Name, Description, Retention Policy (set to 'Default Document Retention Policy'), Default State (set to 'None'), and Document Versioning Policy (set to 'Keep most current version'). There are checkboxes for 'Encrypt All Deposited Documents', 'Financial Asset', 'Active', and 'Default Final Record Of Transfer Type'. The 'Source Document' field has a 'Choose File' button and 'No file chosen' text. Below this are checkboxes for 'Flatten Source Document' and 'Flatten First Uploaded Version'. The 'Signature Experience Options' section has radio buttons for 'None', 'Request participant(s) sign/review the document' (with a '<Define Custom Forms>' dropdown), 'Request participant(s) sign/review the document' (with a 'Choose File' button and 'No file chosen' text), 'Request participant(s) print the document for wet-ink signature', and 'Request participant(s) attach the document'. There are also checkboxes for 'Required In Signing Experience' and 'Override SmartSign Signing Reason'. 'Save' and 'Close' buttons are at the bottom right.

ACTION: Adding a New Document Type

To add a new document type:

- 1.** From the *Preferences* menu, click *Document Types*.
- 2.** In the *Document Types* page, click *Add Document Type*.
- 3.** In the *Name* field, type a unique identifier for the document type.
- 4.** Optionally, input a description.
- 5.** Select the default *Retention Policy*, initial *Default State*, and default *Document Versioning Policy* using the drop-down menus.
- 6.** Ensure that the *Encrypt All Deposited Documents* checkbox is checked.
- 7.** Specify if the document type is either a *Financial Asset* or *Financial Asset Modification* using the checkboxes. Leave both checkboxes blank for all other document types.
- 8.** Optionally, select and upload a document file using the *Choose File* button.
- 9.** Optionally, check the *Default Final Record of Transfer Type* checkbox.
- 10.** Optionally, check the *Flatten Source Document* and *Flatten First Uploaded Version* checkboxes.
- 11.** Select a default *Signature Experience Option*.
- 12.** Optionally, check the *Required in Signing Experience* checkbox.
- 13.** Click *Save* to finish creating the document type.

ACTION: Editing a Document Type

To edit an existing document type:

1. From the *Preferences* menu, click *Document Types*.
2. In the *Document Types* page, under *Actions*, click *Edit* in the row of the document type you want to edit.
3. Input or change document type information as needed.

See [Configuring Document Types](#) for information.

4. Click *Save* to finish editing the document type.

ACTION: Deleting a Document Type

To delete a document type:

1. From the *Preferences* menu, click *Document Types*.
2. In the *Document Types* page, under *Actions*, click *Delete* in the row of the document type you want to delete.
3. In the confirmation window, click *OK* to confirm the deletion.

Group Permissions

Command Center uses two types of permissions to provide system access to users: Container Permissions and Group Permissions.









Group-level permissions are always assigned to groups of users, never to individual users. Once assigned to a group, a user is assigned all permissions assigned to the group.

The *Groups* page is used to configure groups and assign permissions to the groups.

Configured groups are displayed in table rows on the *Groups* page.

Groups:

 Add Group

Name	Description	Actions
Organization Administrator	eOriginal default organization admin group	 Edit  Delete
Owner	eOriginal default owner group	 Edit  Delete
SmartSign Web Senders		 Edit  Delete
View Only	eOriginal default view only group	 Edit  Delete

The following actions can be performed on each group in the list:

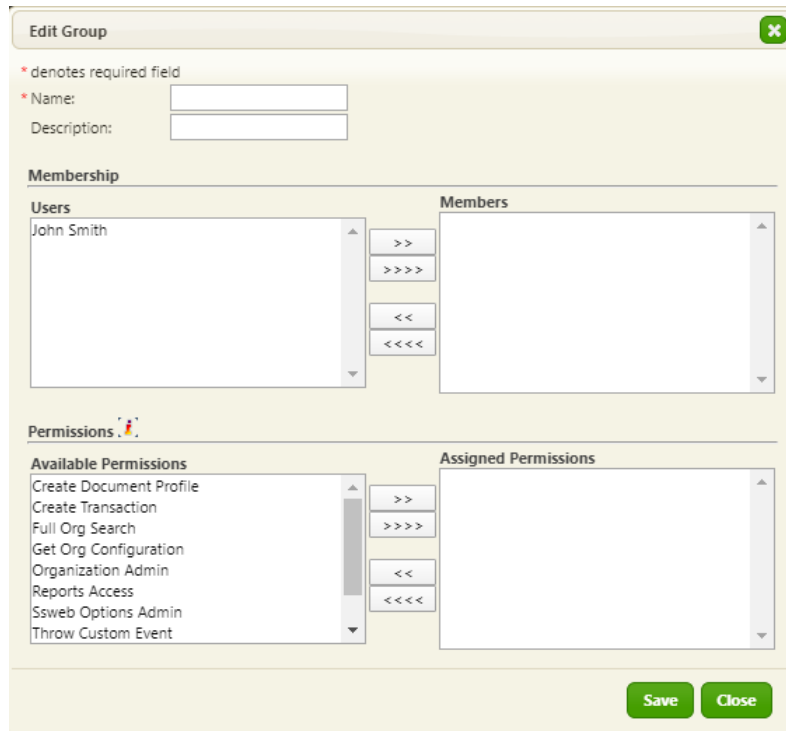
- *Edit* - Opens the group in the *Edit Group* window.
- *Delete* - Displays a *Confirm Group Deletion* window.

Clicking *Add Group* displays the *Edit Group* window.

Configuring Groups

In the *Edit Group* window, add users to a group by selecting names from the *Users* list and moving them to the *Members* list using the >> or >>>> buttons. Users can be removed from a group using the << or <<<< buttons.

Assign permissions to groups by selecting them from the *Available Permissions* list and moving them to the *Assigned Permissions* list using the >> or >>>> buttons. Permissions can be unassigned using the << or <<<< buttons.



The screenshot shows the "Edit Group" window with the following sections:

- Name:** [Text input field]
- Description:** [Text input field]
- Membership:**
 - Users:** [List containing "John Smith"]
 - Members:** [Empty list]
 - Buttons: >>, >>>>, <<, <<<<
- Permissions:**
 - Available Permissions:** [List containing "Create Document Profile", "Create Transaction", "Full Org Search", "Get Org Configuration", "Organization Admin", "Reports Access", "Sswab Options Admin", "Throw Custom Event"]
 - Assigned Permissions:** [Empty list]
 - Buttons: >>, >>>>, <<, <<<<
- Buttons:** Save, Close

Group Permission Definitions

The following table describes all assignable group permissions.

Permission Name	Description
Get Org Configuration	Allows a user to retrieve organization configurations including document types and status values. This permission is also required for specific actions (creating transactions, searching transactions). The Get Org Configuration permission is required for Command Center and API access.
Full Org Search	Allows a user to access all of an organization's transactions.
Create Document Profile	Allows a user to upload a document.
Create Transaction	Allows a user to originate a transaction.
Organization Admin	Allows access to the Command Center, Workflow Rules, Organization Administration, and Vault Administration sections of the <i>Preferences</i> menu in Command Center.
Reports Access	Allows access to reporting features.
Ssweb Options Admin	Allows access to the SmartSign Web section of the <i>Preferences</i> menu.
User Admin	Allows a user to create and modify users.
Throw Custom Event	Allows users to call eoThrowEvent through the API.
Tie Certificate	Currently unused.

ACTION: Adding a Group

To add a new group:

1. From the *Preferences* menu, click *Groups*.
2. In the *Groups* page, click *Add Group*.
The *Edit Group* window is displayed.
3. In the *Name* field, type a unique identifier for the group.
4. Add users by selecting names from the *Users* list and moving them to the *Members* list using the >> or >>>> buttons.
5. Add permissions to the group by selecting them from the *Available Permissions* list and moving them to the *Assigned Permissions* list using the >> or >>>> buttons.
6. Click *Save* to finish creating the group.

ACTION: Editing a Group

To edit an existing group:

1. From the *Preferences* menu, click *Groups*.
2. In the *Groups* page, under *Actions*, click *Edit* in the row displaying the group you want to edit.
The *Edit Group* window is displayed.
3. Add users by selecting names from the *Users* list and moving them to the *Members* list using the >> or >>>> buttons.
4. Remove users using the << or <<<< buttons.
5. Add permissions to the group by selecting them from the *Available Permissions* list and moving them to the *Assigned Permissions* list using the >> or >>>> buttons.
6. Remove permissions using the << or <<<< buttons.
7. Click *Save* to finish editing the group.

ACTION: Deleting a Group

To delete an existing group:

- 1.** From the *Preferences* menu, click *Groups*.
- 2.** In the *Groups* page, under *Actions*, click *Delete* in the row displaying the group you want to delete.
- 3.** In the *Confirm Group Deletion* window, click OK to finish deleting.

Signature Templates

Electronic documents requiring signatures must have signature-collection blocks and other data-collection fields placed in the appropriate places on the pages prior to signing. *Signature templates* are used to collect and store this information in Command Center.

Administrators can create *signature templates* in one of two ways in Command Center:


- *Unmapped* – Signature blocks and fields are placed into a sample document (not a *document type*).
- *Mapped* – Signature blocks and fields are placed into a configured *document type*.

Creating a New Template

The *Create a new template* section is used to create signature templates using either individual documents or document types. Begin creating a new template by selecting one of two document sources:

- *Upload* - Used to open individual documents in the *Document Field Designer*. Once signature blocks and fields are added, you are prompted to save the template to the *Global Template Library*, as described later in this section.
- *Use sample from* - Used to open unmapped document types in the *Document Field Designer*. Once saved, the signature template is displayed in the *Templates Mapped To Document Type* list.

Create a new template:

Document Source: Upload:  No file chosen

Use sample from: ▼

Global Template Library

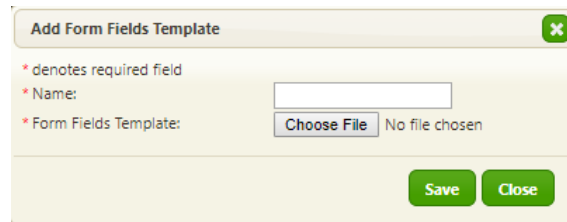
The *Global Template Library* stores template files that are not mapped to a document type. Saved templates are displayed in table rows.

Global Template Library:

[Add Form Fields Template](#)

Signature Template Name ▲	Actions
Sample Template 01	↓ Download ↗ Edit 🗑 Delete 📄 Clone
Sample Template 02	↓ Download ↗ Edit 🗑 Delete 📄 Clone
Sample Template 03	↓ Download ↗ Edit 🗑 Delete 📄 Clone
Sample Template 04	↓ Download ↗ Edit 🗑 Delete 📄 Clone
Sample Template 05	↓ Download ↗ Edit 🗑 Delete 📄 Clone

Clicking *Add Form Fields Template* displays a window used to add a template file directly to the library.



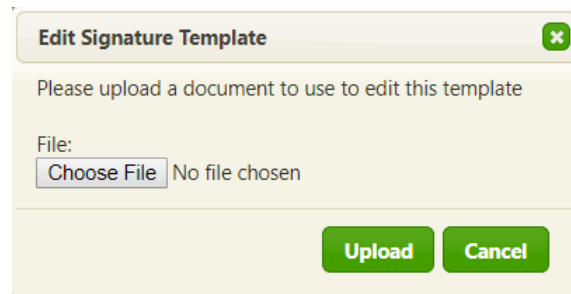
The dialog box titled "Add Form Fields Template" contains the following fields and controls:

- A legend: * denotes required field
- Name:
- Form Fields Template: No file chosen
- Buttons: Save, Close

NOTE: Attempting to add a file that does not meet the specific XML format requirements displays an error message.

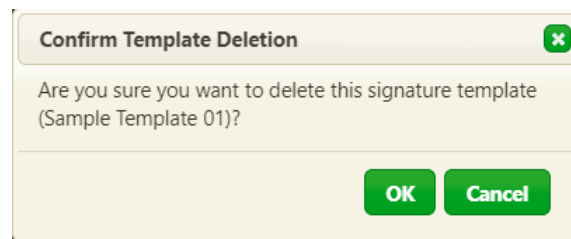
The following actions can be performed on each template in the list:

- *Download* - Places an electronic copy of the signature template XML file on a user's computer or network.
- *Edit* - Displays an *Edit Signature Template* window used to upload a document for editing the selected template. Selecting a file and clicking the *Upload* button opens the signature template in the *Document Field Designer* page.



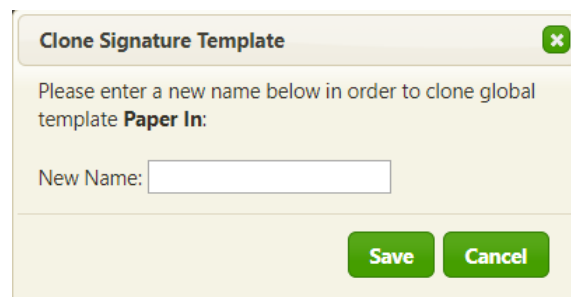
The screenshot shows a dialog box titled "Edit Signature Template" with a close button (X) in the top right corner. The main text reads "Please upload a document to use to edit this template". Below this, there is a "File:" label followed by a "Choose File" button and the text "No file chosen". At the bottom of the dialog, there are two green buttons: "Upload" and "Cancel".

- *Delete* - Displays a *Confirm Template Deletion* window. Clicking *OK* removes the template from the table.



The screenshot shows a dialog box titled "Confirm Template Deletion" with a close button (X) in the top right corner. The main text reads "Are you sure you want to delete this signature template (Sample Template 01)?". At the bottom of the dialog, there are two green buttons: "OK" and "Cancel".

- *Clone* - Displays a *Clone Signature Template* window. Inputting a name and clicking *Save* creates a copy of the selected template and adds it to the table.



The screenshot shows a dialog box titled "Clone Signature Template" with a close button (X) in the top right corner. The main text reads "Please enter a new name below in order to clone global template **Paper In**:". Below this, there is a "New Name:" label followed by an empty text input field. At the bottom of the dialog, there are two green buttons: "Save" and "Cancel".

ACTION: Create an Unmapped Global Signature Template

To create a new unmapped signature template and place it in the *Global Template Library*:

1. From the *Preferences* menu, click *Signature Templates*.
2. Under *Create a new template*, select the *Upload* radio button option.
3. Click the *Choose File* button, select the file you want to use, and click the *Open* button.
4. Click the *Go* button to display the *Document Field Designer* window.
5. Add fields to the document as needed. See *Using the Document Field Designer* in the *Smartsign User Guide*.

NOTE: You must place at least one field in the document to save it as a signature template.

6. Type a name for the signature template in the *Template Name* field.
7. Click the *Save* button to finish creating the signature template.

The signature template name is displayed in the *Global Template Library* list.

Templates Mapped to Document Type

The *Templates Mapped To Document Type* table contains every document type that is mapped to a signature template for your organization.

Templates Mapped To Document Type:

Document Type ▲	Actions
Sample Document 01	↓ Download ✎ Edit 🗑 Delete
Sample Document 02	↓ Download ✎ Edit 🗑 Delete
Sample Document 03	↓ Download ✎ Edit 🗑 Delete
Sample Document 04	↓ Download ✎ Edit 🗑 Delete
Sample Document 05	↓ Download ✎ Edit 🗑 Delete

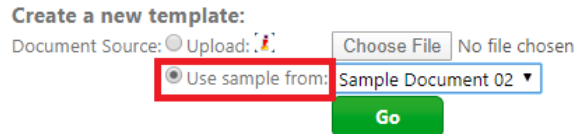
The following actions can be performed on each document in the list:


- *Download* - Places an electronic copy of the mapped XML file on the user's computer.
- *Edit* - Opens the mapped signature template in the *Document Field Designer* page.
- *Delete* - Displays a *Confirm Template Deletion* window. Clicking *OK* removes the template from the table.

ACTION: Creating a Signature Template Mapped to an Existing Document Type

To create a signature template and map it to an existing document type:

1. From the *Preferences* menu, click *Signature Templates*.
2. Under *Create a new template*, select the *Use sample from* radio button option.



Create a new template:
Document Source: Upload:  No file chosen
 Use sample from: Sample Document 02 ▼

3. Select the document type you want to map to the signature template from the *Use sample from* pull-down menu.
4. Click the *Go* button to display the *Document Field Designer* window.
5. Add fields to the document as needed. See *Using the Document Field Designer* in the *SmartSign User Guide*.

NOTE: You must place at least one field in the document to save it as a signature template.

6. Click the *Save* button to finish creating and mapping the signature template.

The mapped signature type name is displayed in the *Templates Mapped To Document Type* list.

Status Values

A status indicates the workflow stage that a transaction or document has reached. An organization can create and maintain as many statuses as needed.

Transaction and document statuses can be updated manually or automatically using vault actions.

You can define a status to be applicable to transactions, documents, or both using the *Scope* drop-down menu. Select *Global* if you want the status to be applicable to both transactions and documents.

Configured templates are displayed in table rows on the *Status Values* page.

Status Values:

[Add Status Value](#)

Name	Description	Scope	Actions
Complete		Global	Edit Delete
Expired		Global	Edit Delete
Inactive		Transaction	Edit Delete
Incomplete		Global	Edit Delete
Pending Transfer In		Transaction	Edit Delete
Signed		Global	Edit Delete
Voided		Document	Edit Delete
Withdrawn		Global	Edit Delete

The following actions can be performed on each status value in the list:

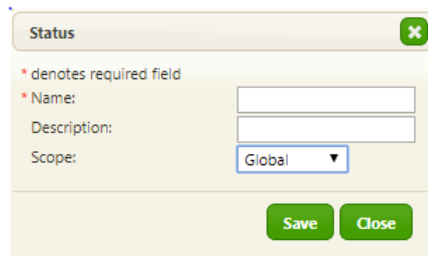
- *Edit* - Opens the status value in the *Status* window.
- *Delete* - Displays a *Confirm Status Deletion* window

Clicking *Add Status Value* displays the *Status* window.

Configuring Status Values

The following fields are used to configure a status value:

- *Name* – Input a unique identifier for the status value.
- *Description* – Optionally, input a description for the status value.
- *Scope* – Define the status value as applicable to transactions, documents, or both. Selecting *Global* makes the status available as a document and a transaction status.



The screenshot shows a dialog box titled "Status" with a close button (X) in the top right corner. Inside the dialog, there is a legend: "* denotes required field". Below this, there are three input fields: "Name:" (with an asterisk), "Description:", and "Scope:". The "Scope:" field is a dropdown menu currently set to "Global". At the bottom of the dialog, there are two buttons: "Save" and "Close".

ACTION: Adding Status Values

To add a new status value:

1. From the *Preferences* menu, click *Status Values*.
2. In the *Status Values* page, click *Add Status Value*.
3. Specify whether the status value is applicable to transactions, documents, or both using the *Scope* drop-down menu.
4. Click *Save* to finish adding the status value.

ACTION: Editing Status Values

To edit an existing status value:

1. From the *Preferences* menu, click *Status Values*.
2. In the *Status Values* page, under *Actions*, click *Edit* in the row of the policy you want to edit.
3. Update the status value using the *Name*, *Description*, and *Scope* fields.

See [Configuring Status Values](#) for information.

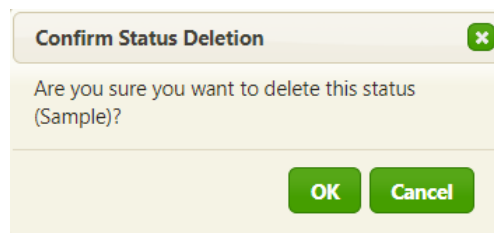
4. Click *Save* to finish editing.

ACTION: Deleting Status Values

To delete an existing status value:

1. From the *Preferences* menu, click *Status Values*.
2. In the *Status Values* page, under *Actions*, click *Delete* in the row of the policy you want to delete.

A confirmation window is displayed.



3. Click *OK* to confirm the deletion.

NOTE: Status values that are in use cannot be deleted. An error message is displayed if you attempt to delete a status value that is associated with a transaction or document.

Transaction Retention Policies

The *Transaction Retention Policies* page is used to configure and maintain retention policies to be applied at the transaction level. Each retention policy defines expiration dates that are activated when specific statuses are applied during a transaction's lifecycle.

With retention policies defined, you can search and find transactions in Workspace based on scheduled expiration dates using the *Expiring After* and *Expiring Before* search fields.

Configured retention policies are displayed in table rows in the *Transaction Retention Policies* page. Checkmarks identify the default retention policy and default transfer retention policy for the organization.

Transaction Retention Policies:

[Add Transaction Retention Policy](#)

Name	Description	Default	Default Transfer	Actions
Sample Policy 1		✓		Edit Delete
Sample Policy 2			✓	Edit Delete

The following actions can be performed on each policy in the list:

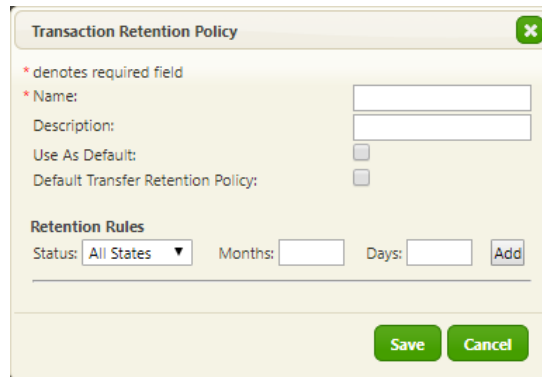
- *Edit* - Opens the policy in the *Transaction Retention Policy* window.
- *Delete* - Displays a *Confirm Retention Policy Deletion* window. Clicking *OK* removes the template from the table.

Clicking *Add Transaction Retention Policy* displays the *Transaction Retention Policy* window.

Configuring Transaction Retention policies

The following fields are used to configure transaction retention policies:

- *Name* – Input a unique identifier for the retention policy.
- *Description* – Optionally, input text to differentiate the retention policy.
- *Use As Default* – Sets the policy as the default transaction retention policy. This policy is automatically mapped to transactions and transaction types when no other policy is selected.
- *Default Transfer Retention Policy* – Sets the policy as the default retention policy for transfer receipts.
- *Retention Rules* – Used to set the time period (in *Months* and *Days*) for retaining documents from the time a specific document status is achieved. Click the *Add* button to save the rule.



The screenshot shows a dialog box titled "Transaction Retention Policy" with a close button (X) in the top right corner. Below the title, there is a legend: "* denotes required field". The form contains the following fields and controls:

- Name:** A required text input field.
- Description:** A text input field.
- Use As Default:** A checkbox.
- Default Transfer Retention Policy:** A checkbox.
- Retention Rules:** A section containing:
 - Status:** A dropdown menu currently set to "All States".
 - Months:** A text input field.
 - Days:** A text input field.
 - Add:** A button to save the rule.

At the bottom of the dialog box, there are two buttons: "Save" and "Cancel".

Each retention policy that you create is listed in the *Document Retention Policy* table along with the associated *Description*.

A checkbox in the *Default* column identifies the default retention policy. A checkmark in the *Default Transfer* column identifies the default transfer retention policy, if one is configured.

For each retention policy, options for editing and deleting are displayed in the *Actions* column.

NOTE: You cannot delete a transaction retention policy once it has been assigned to a transaction.

Transaction Retention Policies:

[Add Transaction Retention Policy](#)

Name ▲	Description ◆	Default ◆	Default Transfer ◆	Actions
Default Policy		✓		Edit Delete
Policy A			✓	Edit Delete

ACTION: Adding a New Transaction Retention Policy

To create a new transaction retention policy:

1. From the *Preferences* menu, click *Transaction Retention Policies*.
2. In the *Transaction Retention Policies* page, click *Add Transaction Retention Policy*.
3. In the *Name* field, type a unique identifier for the transaction type.
4. Optionally, input a description.
5. In the *Transaction Retention Policy* window, under *Retention Rules*, select a status from the *Status* pull-down menu.
6. Use the *Months* and *Days* fields to specify the retention period for the selected status.
7. Click the *Add* button.
8. Repeat steps 2 through 7 to create additional retention rules.
9. Click *Save* to finish.

The new retention policy is displayed in the *Transaction Retention Policies* page and is ready to be mapped to document types.

ACTION: Editing a Transaction Retention Policy

To edit an existing transaction retention policy:

1. From the *Preferences* menu, click *Transaction Retention Policies*.
2. In the *Transaction Retention Policies* page, under *Actions*, click *Edit* in the row of the policy you want to edit.

The *Transaction Retention Policy* window is displayed.

3. Input or change information in the fields to edit the policy.

See [Configuring Transaction Retention policies](#) for information.

4. Click *Save* to finish editing.

ACTION: Deleting a Transaction Retention Policy

To delete a transaction retention policy:

1. From the *Preferences* menu, click *Transaction Retention Policies*.
2. In the *Transaction Retention Policies* page, under *Actions*, click *Delete* in the row of the policy you want to delete.
3. In the confirmation window, click *OK* to confirm the deletion.

The policy is deleted and is no longer displayed in the *Transaction Retention Policies* page.

NOTE: You cannot delete a transaction retention policy once it has been assigned to a transaction.


Transaction Types









Transaction types are reusable transaction templates. Data, settings, and document types are pre-configured and saved in a transaction type, alleviating the need to input data and add documents each time a transaction is created.

The *Transaction Types* page is used to configure and maintain transaction types.

Configured transaction types are displayed in table rows on the *Transaction Types* page. Columns identify the initial status and associated container permission set for each transaction type.

Transaction Types:

 Add Transaction Type

Name	Description	Status	Container Permissions	Active	Actions
Transaction Type 01		All States	Default Container Permissions	✓	 Edit  Delete
Transaction Type 02		All States	Default Container Permissions	✓	 Edit  Delete
Transaction Type 03		All States	Default Container Permissions	✓	 Edit  Delete
Transaction Type 04		All States	Default Container Permissions	✓	 Edit  Delete

The following actions can be performed on each transaction type in the list:

- *Edit* - Opens the transaction type in the *Transaction Type* window.
- *Delete* - Displays a *Confirm Transaction Type Deletion* window.

Clicking *Add Transaction Type* displays the *Transaction Type* window.

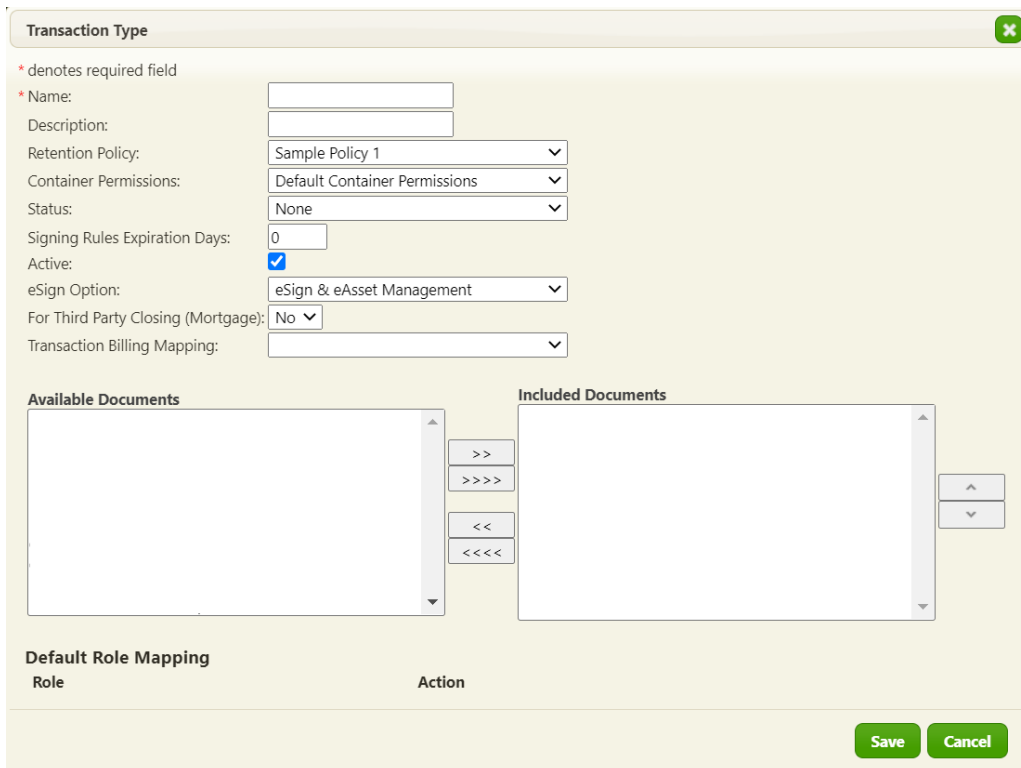
Configuring Transaction Types

The following fields are used to configure transaction types in the *Transaction Type* window:

- *Name* – Input a unique identifier for the transaction type.
- *Description* – Optionally, input a description for the transaction type.
- *Retention Policy* – Optionally, select a configured transaction retention policy to associate it with the transaction type. See [Transaction Retention Policies](#) for information.
- *Container Permissions* – Select a configured container permission set to associate with the transaction type.
- *Status* – Optionally, select an initial status for transactions created based on this transaction type.

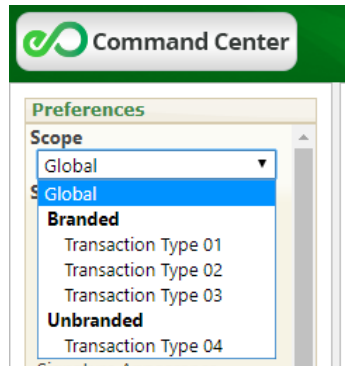
- *Signing Rules Expiration Days* – Select a default duration for signing room access.
- *Active* – Specifies whether a transaction type is included on the *Transaction Type* menu when creating new transactions in Command Center. The *Active* checkbox is checked by default for new transaction types.
- *eSign Option* – Specifies the business function to associate with the transaction type.
- *Transaction Billing Mapping* – Specifies the transaction billing mapping to associate with the transaction type. If a billing mapping is specified for a transaction type, it overrides the default billing mapping during transaction creation when the transaction type is selected.

Add document types to a transaction type by selecting them from the *Available Documents* list and moving them to the *Included Documents* list using the >> or >>>> buttons. Document types can be removed from a transaction type using the << or <<<< buttons. See [Document Types](#) for information.



The screenshot shows the "Transaction Type" configuration form. It includes fields for Name, Description, Retention Policy (Sample Policy 1), Container Permissions (Default Container Permissions), Status (None), Signing Rules Expiration Days (0), Active (checked), eSign Option (eSign & eAsset Management), For Third Party Closing (Mortgage) (No), and Transaction Billing Mapping. Below these fields are two lists: "Available Documents" and "Included Documents". Between the lists are buttons for moving documents (>>, >>>>, <<, <<<<) and buttons for adding (+) and removing (-) documents from the included list. At the bottom, there is a "Default Role Mapping" table with columns for "Role" and "Action", and "Save" and "Cancel" buttons.

For each transaction type that you create, you can create custom Command Center configurations using the Preferences *Scope* menu.

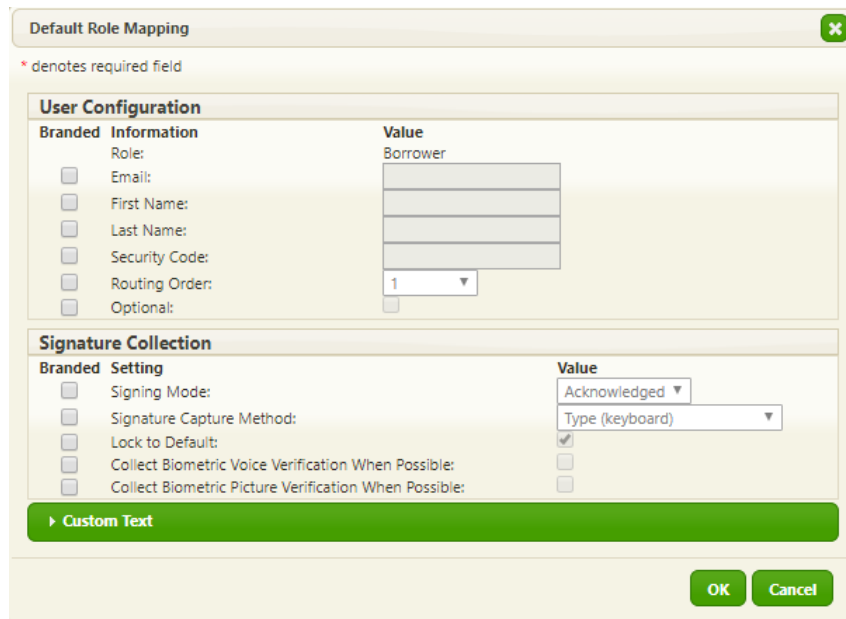


See [Scope](#) for more information.

Default Role Mapping

Any roles mapped within the document types are displayed in the *Default Role Mapping* area. Clicking *Edit* next a role displays the *Default Role Mapping* window.

Checking the *Branded* checkbox and inputting a value in a field pre-populates the corresponding field in the *Map User to Role* window whenever you create a transaction using this transaction type.



Default Role Mapping

* denotes required field

User Configuration

Branded	Information	Value
<input type="checkbox"/>	Role:	Borrower
<input type="checkbox"/>	Email:	
<input type="checkbox"/>	First Name:	
<input type="checkbox"/>	Last Name:	
<input type="checkbox"/>	Security Code:	
<input type="checkbox"/>	Routing Order:	1
<input type="checkbox"/>	Optional:	<input type="checkbox"/>

Signature Collection

Branded	Setting	Value
<input type="checkbox"/>	Signing Mode:	Acknowledged
<input type="checkbox"/>	Signature Capture Method:	Type (keyboard)
<input type="checkbox"/>	Lock to Default:	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Collect Biometric Voice Verification When Possible:	<input type="checkbox"/>
<input type="checkbox"/>	Collect Biometric Picture Verification When Possible:	<input type="checkbox"/>

▶ Custom Text

OK Cancel

Adding a New Transaction Type

To create a new transaction type:

- 1.** From the *Preferences* menu, click *Transaction Types*.
- 2.** In the *Transaction Types* page, click *Add Transaction Type*.
- 3.** In the *Name* field, type a unique identifier for the transaction type.
- 4.** Optionally, input a description.
- 5.** Select the default *Retention Policy*, *Container Permissions* set, and initial *Status* using the drop-down menus.
- 6.** Input a number in the *Signing Rules Expiration Days* field.
- 7.** Add document types by selecting them from the *Available Documents* list and moving them to the *Included Documents* list using the >> or >>>> buttons.
- 8.** Click *Save* to finish adding the transaction type.

Editing a Transaction Type

To edit an existing transaction type:

1. From the *Preferences* menu, click *Transaction Types*.
2. In the *Transaction Types* page, under *Actions*, click *Edit* in the row of the transaction type you want to edit.
3. Input or change information in the following fields as needed:
 - *Name*
 - *Description*
 - *Retention Policy*
 - *Container Permissions*
 - *Status*
 - *Signing Rules Expiration Date*
 - *Active*

See [Configuring Transaction Types](#) for information.

4. Add document types by selecting them from the *Available Documents* list and moving them to the *Included Documents* list using the >> or >>>> buttons.
5. Remove document types using the << or <<<< buttons.
6. Click *Save* to finish editing the transaction type.

Deleting a Transaction Type

To delete an existing transaction type:

1. From the *Preferences* menu, click *Transaction Types*.
2. In the *Transaction Types* page, under *Actions*, click *Delete* in the row of the container permission set you want to delete.
3. In the confirmation window, click *OK* to confirm the deletion.

Transfer Partners

Before transfers can be performed in Command Center, partnerships must be established between the sending and receiving organizations. To configure a partnership, a sending organization user must send an invitation to a user in the receiving organization. Once the invitation is accepted, the transfer partnership is established.



The *Transfer Partners* page is used to configure and maintain an organization's transfer relationships.





Configured transfer relationships are displayed in table rows on the *Transfer Partners* page of both the sender and recipient organizations. The table rows contain the following information:

- *Organization* - Displays the name of a partner organization.
- *My Role* - Defines your relationship to the linked organization as either *Sender* or *Recipient*.

For both Sender and Recipient organizations, the *Actions* column displays a *Delete* button and an *Edit* button.



Transfer Partners:

 Invite Transfer Partner |  Accept Transfer Partner Invitation

Organization	My Role	Actions
CompB	Sender	 Edit  Delete
CompC	Sender	 Edit  Delete

Transfer Partners:

 Invite Transfer Partner |  Accept Transfer Partner Invitation

Organization	My Role	Actions
CompA	Recipient	 Edit  Delete

Inviting Transfer Partners

When a sending organization user clicks the *Invite Transfer Partner* button, an *Invite Partner* window is displayed.

Input information in the following fields to configure a pending transfer relationship:

- *Enter Partner Email* – Input an email address for a configured user of the intended transfer partner organization.
- *Document Types* – Establish transferrable document types by selecting from the *Document Types* list and moving to the *Transferable Types* list using the >> button. Remove a document type using the << button.
- *Receipt Retention* – Specify a preferred option for maintaining transfer receipts:
 - *Keep Transfer Receipt As A Separate Document*
 - *Use the Audit Trail As My Transfer Receipt*
 - *Use the Audit Trail As My Transfer Receipt and Delete The Transaction If It Is Empty*
- *Default Electronic Original Retention* – Set the default selection for Electronic Original copies to be retained as an original copy, an eCopy, or no document when a transfer is performed.
- *Default eCopy Retention* – Set the default selection for eCopy documents to be retained or not.
- *Default eStored Document Retention* – Set the default selection for eStored documents to be retained or not.

You can make transaction properties transferable to the partner organization by selecting options from the *Transaction Properties* list and moving them to the *Transferable Transaction Properties* list using the >> button.

Use the *Notes* field to input additional information to include in the invitation email.

Invite Partner

* denotes required field

* Enter Partner Email:

Document Types:

* Transferable Types:

Receipt Retention:

Default Electronic Original Retention:

Default eCopy Retention:

Default eStored Document Retention:

Transaction Properties:

Transferable Transaction Properties:

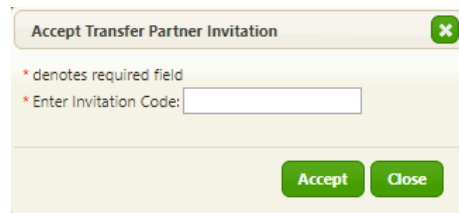
Notes:

Characters left: 2500

Accepting Transfer Partner Invitations

To accept an invitation as a transfer partner, select *Preferences > Transfer Partners*. In the *Transfer Partners* page, click *Accept a Transfer Partner Invitation*.

In the *Accept Transfer Partner Invitation* window, input the *Invitation Code* from the email and click the *Accept* button. A notification email is sent upon acceptance.



Once accepted, the *Partner Settings* window is displayed. Input information in the following fields to configure users and settings for incoming transfers:

- *Users/Groups* - Assign recipient agents by selecting them from the *Users/Groups* list and moving them to the *Recipient Agents* list using the >> button. Recipient agents can be unassigned using the << button.
- *Incoming Transaction Type* - Allows organizations that receive transactions from multiple partners to associate different container permission sets with each transfer partner using transaction types. Once a transaction type is selected, the *Incoming Transaction Status* drop-down menu becomes inactive and the transaction status defaults to the value associated with the selected transaction type.

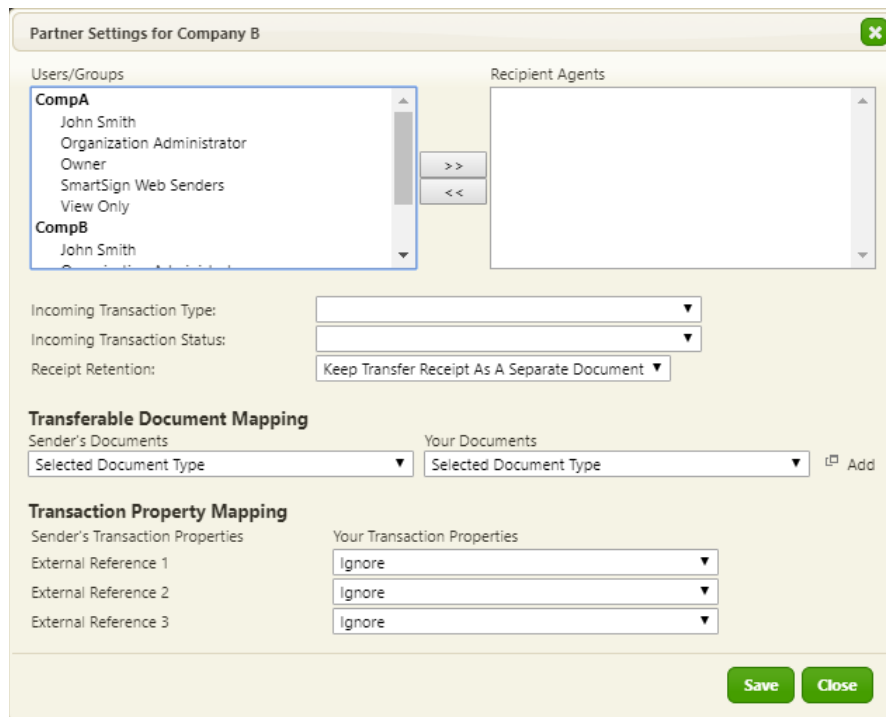
NOTE: Only transaction types with no mapped document types are displayed in the *Incoming Transaction Type* drop-down menu. The *Incoming Transaction Type* menu will not display unless there is at least one configured transaction type with no document types mapped.

- *Incoming Transaction Status* - Specifies the status of incoming transactions upon transfer.
- *Receipt Retention* - Specify a preferred option for maintaining transfer receipts:
 - *Use the Audit Trail As My Transfer Receipt* (default)
 - *Keep Transfer Receipt As A Separate Document*

- **Transferable Document Mapping** - A pair of drop-down menus is used to map a sender document type with a recipient document type. For the sender, an individual document type can be selected or you may select the *Any Type* option. For the recipient, an individual document type must be selected. Clicking *Add* saves the current selections.

NOTE: Sender organizations should notify recipients when new document types are introduced and replaced. In case changes are not communicated, a mapping of *Any Type* should be configured for each sender organization to serve as a backup.

- **Transaction Property Mapping** - Specify where external reference data from a sender's transaction is stored by selecting from the following options:
 - *Create New Custom Field*
 - *External Reference 1, 2, 3*
 - *Ignore*



Partner Settings for Company B

Users/Groups

- CompA
 - John Smith
 - Organization Administrator
 - Owner
 - SmartSign Web Senders
 - View Only
- CompB
 - John Smith

Recipient Agents

Incoming Transaction Type:

Incoming Transaction Status:

Receipt Retention:

Transferable Document Mapping

Sender's Documents: Your Documents:

Transaction Property Mapping

Sender's Transaction Properties

External Reference 1:

External Reference 2:

External Reference 3:

Editing a Sender Transfer Partner

When a sending organization user clicks the *Edit* button for a transfer partner, a *Partner Settings* window is displayed.

Use the *Partner Settings* fields to update an existing transfer relationship, including document types, retention settings, and transaction properties.

See [Inviting Transfer Partners](#) for field descriptions.

Editing a Recipient Transfer Partner

When a receiving organization user clicks the *Edit* button for a transfer partner, a *Partner Settings* window is displayed.

Use the *Partner Settings* fields to update users and settings for incoming transfers.

See [Accepting Transfer Partner Invitations](#) for field descriptions.

ACTION: Inviting a Transfer Partner

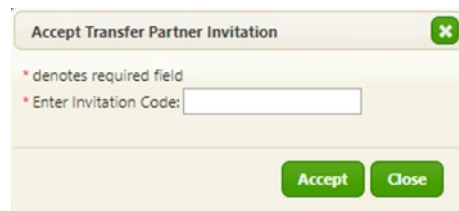
To invite a transfer partner:

1. From the *Preferences* menu, click *Transfer Partners*.
2. In the *Transfer Partners* page, click *Invite Transfer Partner*.
3. Input an email address for a configured user of the intended transfer partner organization.
4. Establish transferrable document types by selecting them from the *Document Types* list and moving them to the *Transferable Types* list using the >> button.
5. Specify a preferred option for maintaining transfer receipts using the *Receipt Retention* drop-down menu.
6. Optionally, select a retention policy for Electronic Originals, eCopies, and eStored Documents using the drop-down menus.
7. Optionally, add a note in the *Note* field.

ACTION: Accepting a Transfer Partner Invitation

To accept a transfer partner invitation:

1. From the *Preferences* menu, click *Transfer Partners*.
2. In the *Transfer Partners* page, click *Accept Transfer Partner Invitation*.



3. Input the *Invitation Code* from the email and click the *Accept* button.

Users

To access an organization's transactions, documents, and data in Command Center, a person must be registered as a user. Administrators are responsible for creating user accounts for every user in an organization.

NOTE: The default status for a newly-created user in eCore is NO ACCESS.

Configured users are displayed in table rows on the *Users* page. Columns identify the Login ID, phone number, email address, status, and last login for each user.

Configuring Command Center Users

The *User* window contains fields for inputting contact information and login credentials for users.

The *User* window is also used to add and remove users from groups. Assigning a user to a group grants all system access permissions that are associated with that group. See [Group Permissions](#) for more information on groups.

A user account can never be deleted or removed from an organization once it is created.

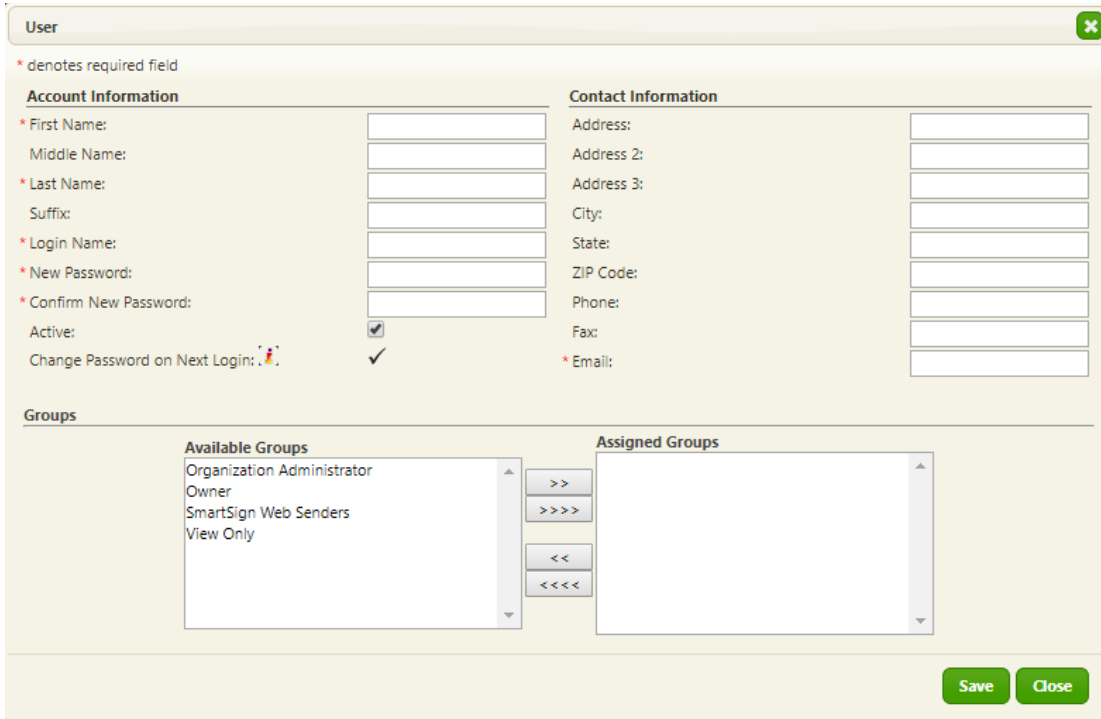
The following fields are used to configure user accounts:

- *First Name, Middle Name, Last Name, Suffix* – Populate these fields to establish a user's full name. *First Name* and *Last Name* are required fields.
- *Login Name* – Defines the Username used to authenticate a user when logging in.
- *New Password* – Defines a temporary password to be used upon the user's first log in. The user must create a new password once logged in for the first time. See [Password Complexity Policy](#) for information.
- *Confirm New Password* – Confirm the password typed in the *New Password* field. The passwords in the *New Password* and *Confirm New Password* fields must match.
- *Active* – Specifies a user's status. The *Active* checkbox is checked by default for new users. If the checkbox is unchecked, the user is prohibited from logging in to Command Center.
- *Change Password on Next Login* – Checking this option requires a user to create a new password upon next login. This option defaults to checked for new users and cannot be changed.

Provide a user's contact information using the *Contact Information* fields. **You must provide an email address before saving.**

Assigning Users to Groups

Assign users to groups by selecting from the *Available Groups* list and moving selections to the *Assigned Groups* list using the >> or >>>> buttons. Users can be unassigned using the << or <<<< buttons.



The screenshot displays the 'User' administration window. It is divided into several sections:

- Account Information:** Fields for First Name, Middle Name, Last Name, Suffix, Login Name, New Password, and Confirm New Password. There are checkboxes for 'Active' and 'Change Password on Next Login'.
- Contact Information:** Fields for Address, Address 2, Address 3, City, State, ZIP Code, Phone, Fax, and Email.
- Groups:** A section with two lists: 'Available Groups' (containing Organization Administrator, Owner, SmartSign Web Senders, and View Only) and 'Assigned Groups' (currently empty). Between the lists are buttons for moving items (>>, >>>>, <<, <<<<).

At the bottom right, there are 'Save' and 'Close' buttons.

ACTION: Adding a User

Perform the following steps to create a new user account:

1. From the *Preferences* menu, click *Users*.
2. In the *Users* page, click *Add User*.
3. Input account information for the user including name, login name, and temporary password.

NOTE: The user is required to change the account password when logging in for the first time.

4. Input contact information including address, phone, and email. **You must provide an email address before saving.**
5. Assign the user to groups based on the functions he or she performs.

See [Group Permissions](#) for information.

6. Click *Save* to finish adding a user.

ACTION: Editing a User

To edit an existing user:

1. From the *Preferences* menu, click *Users*.
2. In the *Users* page, under *Actions*, click *Edit* in the row displaying the user you want to edit.
3. Input or change information in the Account Information or Contact Information fields as needed.

See [Configuring Command Center Users](#) for information.

4. In the *Groups* area, assign the user to additional groups using the >> button. Remove the user from groups using the << button.

See [Group Permissions](#) for information.

5. Click *Save* to finish adding a user.

Appendix A: Business Entity Functions

A business entity is a structure within which multiple organizations, or vaults, can be linked together. Once organizations are linked within a business entity, authorized business entity users can access all of the linked organizations and corresponding data with one set of credentials.

Business entity administrators manage the organizations and users contained in a business entity. Business entity administrator functions are described in this appendix.

Using the Business Entity Organization Menu

Business entity administrators can make organization-level configuration changes to individual organizations by selecting them individually from the *Organization* menu. This menu contains a searchable drop-down list containing all organizations associated with the business entity.

When a business entity administrator selects an organization from the *Organization* menu and makes configuration changes, the changes are applied only to the selected organization.



NOTE: For information on specific configuration settings, see the [Command Center Administrator Guide](#).

Viewing business entity organizations

Business entity administrators can view every associated organization in the *Business Entity Snapshot* page.

You can search for organizations by typing an organization name in the *Search* field. Search results are updated as you type.

Each organization occupies a single row and each column contains the following organization data:

- Organization full name and nickname
- Organization Purpose – Indicates the primary purpose of the vault, such as Origination, Collateralization, Securitization, or Buyer.
- Functionality – Indicates the primary functionality used, such as eSign and eAsset Management, eDeposit and eAsset Management, or eAsset Management.
- Transaction Count – Provides the total number of transactions that are currently in a vault.
- ECCA Status (Yes/No)
- Organization Status (Active/Inactive)

An *Organization Count* is displayed at the top of the page. Checking the *Active Only* checkbox omits any inactive organizations from the search results.

Downloading a CSV-format file of business entity organizations

Clicking *Download CSV* downloads a file containing all of the information contained in the *Business Entity Snapshot* page

Business Entity Snapshot:

Search: Organization Count: 10 Active Only ↓ Download CSV

Show entries Previous **1** Next

Organization (Full Name)	Organization (Nickname)	Organization Purpose	Functionality	Transaction Count	ECCA?	Status
Demo Org1 Full Name	DemoOrg1			10	No	Active

Viewing business entity users

Business entity administrators can view every associated user in the *Users* page.

You can search for business entity users by typing a username, first name, last name, or email address in the *Search* field. Search results are updated as you type.

Search results can also be modified using the *Organization* and *Status* (displays *Active*, *Inactive*, and *Locked*) drop-down menus.

Users:

 Add User

Search Users

Search: Organization: Status:

 Download CSV

Current search results are displayed in a table view. Each user occupies a single row and each column contains the following organization data:

- Username
- Last and First Name
- Email
- Last Login Date
- Organization
- Status

Downloading a CSV-format file of business entity organizations

Clicking *Download CSV* displays a confirmation window with an *Include Group Details* checkbox:

- Clicking the *Download* button without checking the *Include Group Details* checkbox downloads a file containing all of the information contained in the *Users* page, except the *Organization* field.
- Clicking the *Download* button with the *Include Group Details* checkbox checked downloads a file containing a line for each group (each line represents one group membership within one organization). A *Group Scope* column identifies each user as either organization-level or business entity-level.

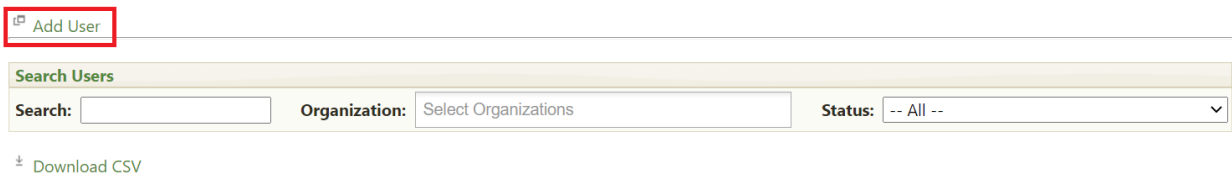
The *Actions* column displays *Deactivate/Reactivate*, *Delete*, and *Unlock* options depending on the status of the user. These options are described later in this document.

Adding business entity users

Perform the following steps to create a new business entity user account and assign the user to one or more business entity organizations:

1. From the Business Entity Settings menu, click Users.
2. In the *Users* page, click *Add User*.

Users:



Search Users

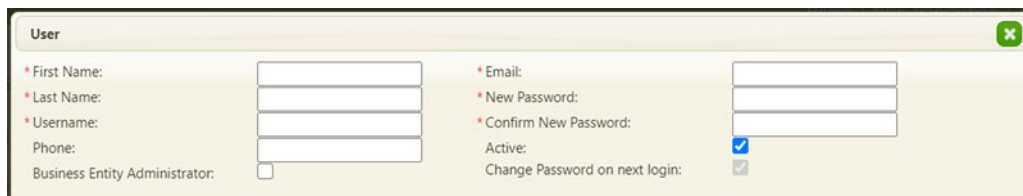
Search: Organization: Status:

[Download CSV](#)

3. Input account information for the user including
 - First Name
 - Last Name
 - Username
 - Temporary password

NOTE: The user is required to change the account password when logging in for the first time.

4. Check the *Business Entity Administrator* checkbox to grant administrator status and to provide access to the *Business Entity Settings* menu.



User

* First Name:

* Last Name:

* Username:

Phone:

Business Entity Administrator:

* Email:

* New Password:

* Confirm New Password:

Active:

Change Password on next login:

Next, you select assign the user to organizations and groups within the business entity

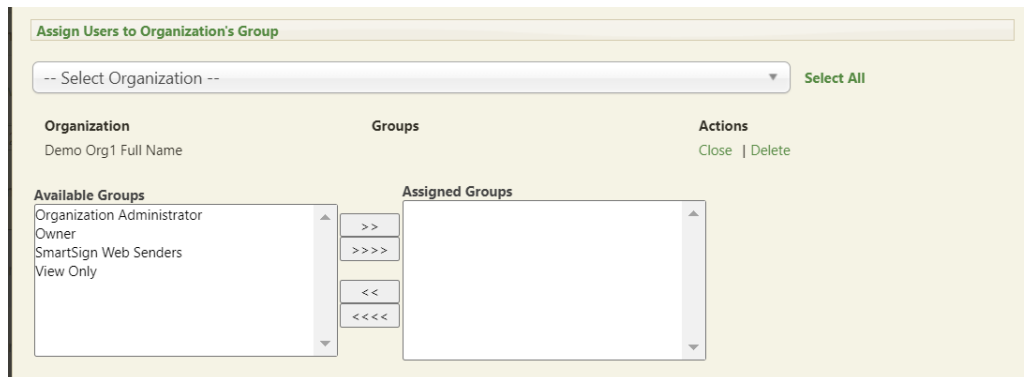
- Click the *Select Organization* drop-down menu and select from the available organizations. You also have the option of clicking *Select All*.

Selected organizations are displayed in a table below the *Select Organization* drop-down menu.

NOTE: The *Organization* column displays the organization nickname if one is configured. If no nickname is configured, the full name of the organization is displayed.

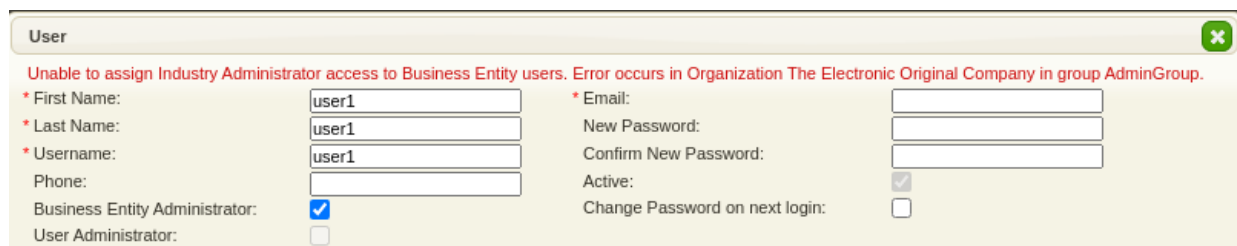
- Click the *Edit* option in the *Actions* column for each of the organizations in the table to display the available groups for the organization.
- Assign users to groups by selecting from the *Available Groups* list and moving selections to the *Assigned Groups* list using the >> or >>>> buttons. Users can be unassigned using the << or <<<< buttons.

NOTE: See *Group Permissions* in the [Command Center Administrator Guide](#) for more information on groups.



- Click *Save* to finish adding a user.

NOTE: If an administrator attempts to add a Business Entity user to a group with the Industry Admin permission, an error message is displayed on the *User* page.



Editing business entity users

To edit an existing user:

1. From the *Business Entity Settings* menu, click *Users*.
2. In the *Users* page, under *Actions*, click *Edit* in the row displaying the user you want to edit.
3. Input or change information in the *Account Information* or *Contact Information* fields as needed.
4. In the *Groups* area, assign the user to additional groups using the >> button. Remove the user from groups using the << button.

NOTE: See *Group Permissions* in the [Command Center Administrator Guide](#) for more information on groups.

5. Click *Save* to finish adding a user.

Linking business entity user accounts

When individual Command Center users have user accounts in multiple organizations within a business entity, those accounts can be linked to the user's business entity account.

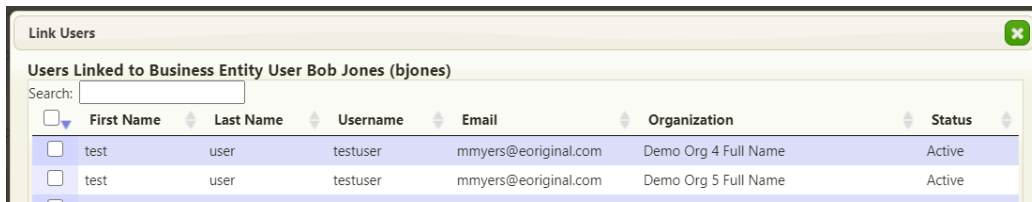
Perform the following steps to link business entity user accounts to organization-level user accounts:

1. From the *Business Entity Settings* menu, click *Users*.
2. Click *Link* in the *Actions* column for the user.

A window containing a list of all organization-level user accounts in the business entity is displayed.

3. Search for organization-level users by typing a first name, last name, username, or organization name in the *Search* field. Search results are updated as you type.

4. Check the checkboxes next to the organization-level users you want to link to the business entity user.
5. Click *Save* to finish linking all of the checked users.



Unchecking the checkbox for organization-level users unlinks the accounts from the business entity user account.

NOTE: When access to an organization is removed from a user account, the link to the business entity user account is automatically removed and no checkbox is displayed in the *Link* window for that organization-level user.

Deactivating and reactivating business entity user accounts

Perform the following steps to deactivate a business entity user:

1. From the *Business Entity Settings* menu, click *Users*.
2. Click *Deactivate* in the *Actions* column for the user.

A confirmation window is displayed.

3. Click *Yes* to confirm the deactivation.

The user's status is updated to *Inactive* and the user is prevented from signing into the account. A *Reactivate* option is displayed for that user in the *Actions* column.

NOTE: If a business entity user has never signed into a user account, a *Delete* option is displayed in the *Actions* column in place of the *Deactivate* option. Selecting the *Delete* option permanently removes the user account from the business entity.

Clicking *Reactivate* in the *Actions* column for a user returns the user's status to *Active*. The *Deactivate* option is again displayed for that user in the *Actions* column.

Unlocking business entity user accounts

A user that is locked out of an account displays an *Unlock* option. Clicking *Unlock* restores access to the user account.

Viewing and editing business entity groups

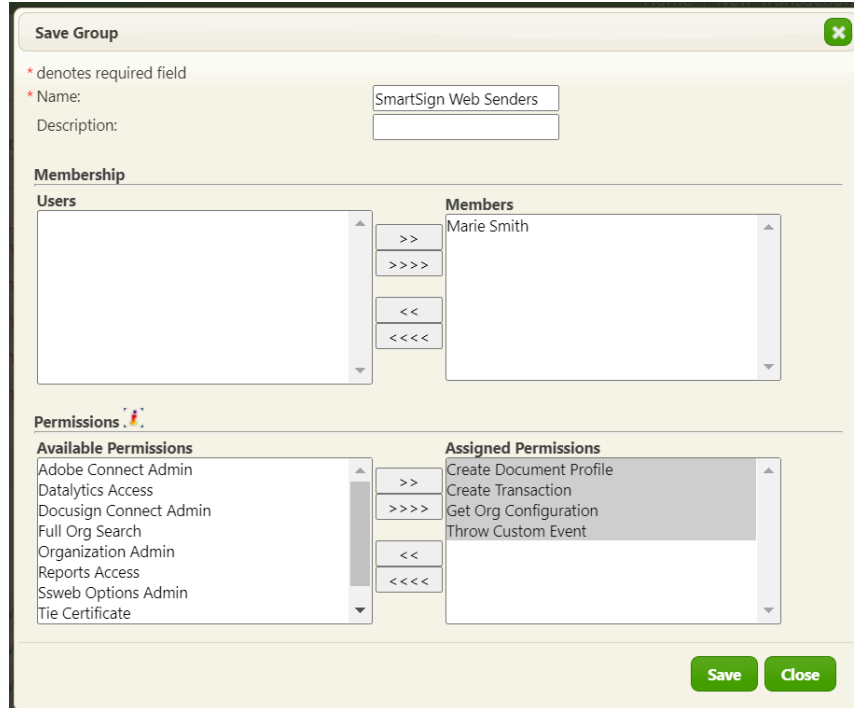
To edit an existing group:

1. From the *Business Entity Settings* menu, click *Groups*.
2. In the *Groups* page, under *Actions*, click *Edit* in the row displaying the group you want to edit.

The *Save Group* window is displayed.

3. Add users by selecting names from the *Users* list and moving them to the *Members* list using the >> or >>>> buttons.
4. Remove users using the << or <<<< buttons.
5. Add permissions to the group by selecting them from the *Available Permissions* list and moving them to the *Assigned Permissions* list using the >> or >>>> buttons.

6. Remove permissions using the << or <<<< buttons.
7. Click *Save* to finish editing the group.



Configuring security settings for business entity organizations

Business entity administrators can configure security settings for all associated users in the *Business Entity Security* page. Fields on this page are used to change general security, password complexity, preferred time zone, concurrent session warning, and authorized IP address settings.

NOTE: Standard default security settings are set for every new business entity when it is created. The default settings remain in effect unless changes are made on the *Business Entity Security* page.

To configure business entity security settings:

1. From the *Business Entity Settings* menu, select *Business Entity Security*.
2. Edit values in the *Settings*, *Password Complexity Policy*, *Concurrent Session Warning*, *Authorized IP Addresses*, and *Authorized Email Domains for Scheduled Reports* sections.

NOTE: See *Organization Security* in the Command Center Administrator Guide for more information on specific security settings.

3. Click the *Save* button to finish updating security settings for the business entity.

Business Entity Security:

Password Complexity Policy requires a minimum of the following: 8 characters, 1 uppercase letter, 1 lowercase letter, 1 number, and 1 special character.

* denotes required field

Settings:

* Maximum bad logins before logout:

* Lockout duration in minutes:

Lockout until an administrator unlocks:

* Password expires in days:

* Number of saved passwords:

Use two-factor authentication for login from untrusted devices:

Preferred time zone:

Password Complexity Policy:

* Passwords will contain at least characters in length.

* Passwords will contain at least uppercase letters.

* Passwords will contain at least lowercase letters.

* Passwords will contain at least numbers.

* Passwords will contain at least special characters.

Disable use of most common passwords:

Concurrent Session Warning:

Enable warnings for concurrent user logins to Command Center:

Authorized IP Addresses:

System Name	Start	End	Action
Command Center	<input type="text"/>	<input type="text"/>	<input type="button" value="Edit"/>

Authorized Email Domains for Scheduled Reports:

No.	Authorized Domain Names
1.	<input type="text"/>
2.	<input type="text"/>
3.	<input type="text"/>
4.	<input type="text"/>
5.	<input type="text"/>
6.	<input type="text"/>

Appendix B: Configuring Adobe Connect

The Adobe eDeposit process allows for documents signed with the Adobe Sign application to be deposited into an eOriginal vault.

The *Enable Adobe Connect* checkbox must be checked to activate the account.

The following fields are used to configure an Adobe Connect account for an organization:

- *Environment* - Used to configure the account as either *Demo* or *Production*.
- *Integration Key* – Used to input the Integration Key used to authenticate to the customer’s Adobe Sign account.
- *Transaction completed status* - Used to specify the transaction status that is applied when an Adobe document package is deposited in a vault.

Adobe Connect:

Enable Adobe Connect

* denotes required field

*Environment:

Demo

Integration Key:

3AAABLKmtbUCAmqtOQ_DKflF6PmeI-6TAKMl

*Transaction completed status:

Complete

Document Mapping

In the *Document Mapping* area, you must specify the eOriginal document type used to manage deposited documents by selecting from the *Document type* drop-down menu.

You must also specify the eOriginal document type used to manage the Adobe history for the package by selecting from the *Audit Trail* drop-down menu.

Document Mapping:

* Document type:

Coverage Test Contract

* Audit trail:

Final Record of Transfer

Failed Messages

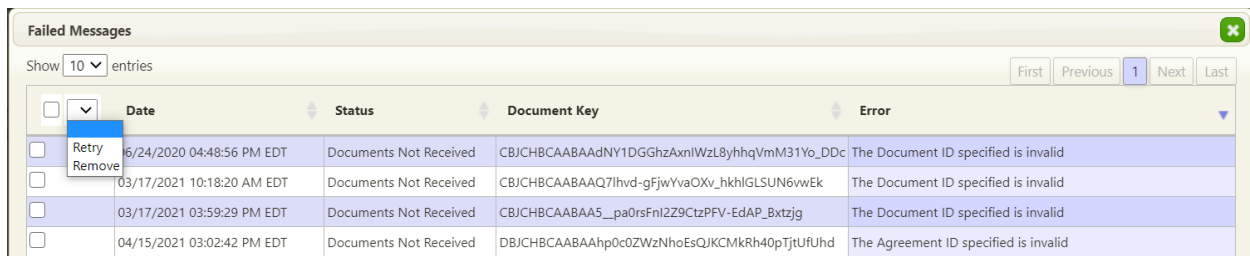
In the *Failed Messages* area, in the *Notification Email Address* field, you can specify the email address of the organization member to be notified when a document package is not properly deposited into the eOriginal vault.

Failed Messages: [View Failures](#)

*Notification email address:

Clicking *View Failures* displays a window listing failed message attempts in table rows including the following information:

- Date
- Status
- Document Key
- Error



The screenshot shows a window titled "Failed Messages" with a close button in the top right. Below the title bar, there is a "Show 10 entries" dropdown and navigation buttons: "First", "Previous", "1", "Next", and "Last". The main content is a table with the following columns: a checkbox column, a "Date" column, a "Status" column, a "Document Key" column, and an "Error" column. A dropdown menu is open over the first row, showing "Retry" and "Remove" options.

<input type="checkbox"/>	Date	Status	Document Key	Error
<input type="checkbox"/>	6/24/2020 04:48:56 PM EDT	Documents Not Received	CBJCHBCAABAAAdNY1DGGhzAxnlWzL8yhqVmM31Yo_DDc	The Document ID specified is invalid
<input type="checkbox"/>	03/17/2021 10:18:20 AM EDT	Documents Not Received	CBJCHBCAABAAQ7lhvd-gFjwYvaOXv_hkhlGLSUN6wEK	The Document ID specified is invalid
<input type="checkbox"/>	03/17/2021 03:59:29 PM EDT	Documents Not Received	CBJCHBCAABAA5_pa0rsFnl2Z9CtzPFV-EdAP_Bxtzjg	The Document ID specified is invalid
<input type="checkbox"/>	04/15/2021 03:02:42 PM EDT	Documents Not Received	DBJCHBCAABAAhp0c0ZWzNhoEsQJCMKRh40pTjtUfUhd	The Agreement ID specified is invalid

You can use checkboxes in the left-most column to select failed message attempts and select the following options from a drop-down menu at the top of the window:

- Retry
- Remove

Adobe Webhook Configuration

eOriginal receives webhook notifications when documents are signed using the Adobe Sign application. These notifications are processed in eCore and signed documents are then retrieved into an eOriginal vault.

The *Webhook Configuration* section is used to configure webhooks for an organization.

NOTE: The *Adobe Webhook Configuration* section is not displayed on the *Adobe Connect* page unless an Adobe Integration Key is input and validated for the organization.

Configured webhooks are displayed in table rows in the *Adobe Webhook Configuration* area. Columns in the table identify the *Scope*, *Group/User*, and *Webhook URL* for each webhook.

Adobe Webhook Configuration:

Scope	Group/User	Webhook URL	Actions
Account		https://test.eoriginal.org/adobesign/webhooks/6f236aae-0771-452a-95e9-6a2f4d877e52	Delete
Group	Group 1	https://test.eoriginal.org/adobesign/webhooks/6f30c473-5135-4c2b-b338-bd8304b5f4e7	Delete

[Add Webhook](#)

Configuring Webhooks

Clicking *Add Webhook* initiates the process of configuring a new webhook. A new row is created in the table and the following fields are used to configure the webhook:

- *Scope* – Specify a range of webhook recipients by selecting *Account*, *User*, or *Group* from the drop-down menu.
- *Group/User* – For a Group- or User-scoped webhook, select the name of the group or user to associate from the drop-down menu.
- *Actions* – Select options including *Configure Webhook*, *Cancel*, and *Delete*.

Adobe Webhook Configuration:

Scope	Group/User	Webhook URL	Actions
No data available in table			
User	Select User		Configure Webhook Cancel

Clicking *Configure Webhook* completes the action and the associated URL is displayed in the Webhook URL column.

Adding an Adobe Webhook

To add an Adobe Webhook to an organization:

1. From the *Preferences* menu, select *Adobe Connect*.
2. In the *Adobe Webhook Configuration* area, click *Add Webhook*.

A new row is created in the table.

3. In the *Scope* column, select *Account*, *User*, or *Group* from the pull-down menu.

If *Group* or *User* is selected, a drop-down menu is displayed in the *Group/User* column.

4. If necessary, select a group or a user from the drop-down menu.
5. In the *Actions* Column, click *Configure Webhook*.

Once completed, the webhook is displayed in a table row and the associated URL is displayed in the *Webhook URL* column. A *Delete* option is now displayed in the *Actions* column.

Deleting a Webhook

To delete an Adobe Webhook from an organization:

1. From the *Preferences* menu, select *Adobe Connect*.
2. Click *Delete* in the row of the webhook you want to delete.

A *Confirm Webhook Deletion* window is displayed.

3. Click *OK* to confirm the deletion.

The webhook listing is removed from the table.