Perceptive eAuthorize

Installation and Setup Guide

Version: 2.0.x

Written by: Product Knowledge, R&D

Date: February 2021

Copyright

- Table of Contents

About Perceptive eAuthorize

The Perceptive eAuthorize solution enables you to send documents for electronic signature to any authorized signatory, including non-ImageNow users. You can send documents, residing within or outside of ImageNow, to a single or multiple authorized signatories whose signatures are required. The signed documents upload automatically and are stored in the ImageNow repository. If the signatory declines the document, you receive an email notification. A signatory can also forward the email with the link to the documents to any person inside or outside your organization.

This solution offers the following advantages.

- The electronic process of signing saves you time.
- Anyone inside or outside your organization can sign documents.
- Signatories do not need access to ImageNow.
- Signatories receive email notifications of documents to sign. The email contains a link to the document and instructions. Alternatively, documents can be immediately presented on the user's screen. You can send a single document or an envelope containing multiple related documents.

Three different levels of eAuthorize are available.

- **Standalone**. AssureSign is sold as a standalone solution, with no integration with ImageNow.
- **Post-signature integration**. A non-ImageNow document is provided to AssureSign for signature, is signed, and then the signed document is uploaded into ImageNow.
- **Full integration**. An ImageNow document is submitted to AssureSign for signature, is signed, and then the signed document is uploaded to ImageNow.

This document provides the configuration and setup guidelines for ImageNow connector for AssureSign.

Important After you finish installing and configuring eAuthorize, complete the steps in the *Perceptive eAuthorize Getting Started Guide* to test your configuration and confirm that the installation and setup is successful.

For information about using Perceptive eAuthorize, see the *Perceptive eAuthorize Getting Started Guide*.

Requirements

Software prerequisites

For ImageNow, version 6.7 or higher, before you run the eAuthorize solution, ensure that your system meets the following prerequisites.

- Perceptive Connect Runtime 1.4.50 or higher is installed.
- Content Connector 1.2.30 or higher is installed and configured to use the ImageNow Integration Server instance where the eAuthorize components are to be installed.

Note Ensure that all the Content Connector related components are in Active state.

- ImageNow or Perceptive Content Client and ImageNow or Perceptive Content Server are installed and running properly.
- You can log into an ImageNow user account with manager privileges.

- You have administrator access to the AssureSign environment to create and edit AssureSign templates.
    - Sandbox environment: https://sb.assuresign.net/documents/Default.aspx
    - Production environment: https://na1.assuresign.net/Login.aspx or the URL for the local instance of AssureSign
- Ensure that the appropriate IP ranges for AssureSign are open for inbound and outbound communiation. The currently used IP addresses are available in https://support.assuresign.net/hc/en-us/articles/224274907.
- Ensure that the appropriate ports used by PCR are open for communication with AssureSign.

License

The following licenses are required to run eAuthorize.

- Perceptive eAuthorize
- Integration Framework version 6.7 or higher
- ImageNow Server, version 6.7 or higher
- ImageNow Client, version 6.7 or higher
- Integration Server for Apps version 6.7 or higher, and Transaction Pack
- Envoy for Apps version 6.7 or higher
- iScript
- Optional. eForms and Doc Control Suite

Configure eAuthorize

If you are using ImageNow, version 6.5.1 or 6.6, use Perceptive eAuthorize 1.2.

Note eAuthorize is not supported for ImageNow Server versions lower than 6.7.

Install and configure eAuthorize for ImageNow 6.7 or higher

If you are using ImageNow, version 6.7 or higher, install Perceptive Connect Runtime and then install eAuthorize using the installation wizard. To download and complete the installation process, perform the following procedures.

1. Download the eAuthorize files
2. Install eAuthorize
3. Set up ImageNow for signing
4. Set up the AssureSign environment
5. Set up the ability to download signed documents from a third party
6. Set up the AssureSign environment for envelopes
7. Set up an eForm for Signature

Download the eAuthorize files

To obtain Perceptive product installation files, contact the Hyland Software Technical Support group. For a list of Technical Support phone numbers, go to hyland.com/pswtscontact.

Install eAuthorize

After you install the Perceptive Connect Runtime (PCR), download the eAuthorize files and run the eAuthorize installation wizard. You can also install eAuthorize manually. To install eAuthorize manually,see the Install eAuthorize manually section.

NoteYou must install PCR Content Connector and configure it with the appropriate ImageNow Integration Server.

If an older version of eAuthorize is already installed and you use Perceptive Content, version 7.1.5 or higher, you must complete the following steps before running the eAuthorize installer.

1. Navigate to **ImageNow Management Console**>**Workflow**.
2. Open the eAuthorize workflow.
3. Delete the following three Integration ASQs.
   - SubmitForSignature
   - SendToAssureSign
   - DownloadSigned Documents

Run the eAuthorize installer

As you run the eAuthorize installation wizard, you can select one of the following installation options. Regardless of the option you select, all components described in the table given below are required for eAuthorize to function correctly.

- Complete - For complete installation, the installation wizard installs the required components at once.
- Custom – For custom installation, ensure that you already installed the required software for each installation option according to the following table. Typically, you select the custom installation to install eAuthorize componentson the following machines.
  - On the machine where Perceptive Connect Runtimeis running, you can install the PCR Configuration option. You can also run the installer remotely to install the PCR Configuration feature.
  - On a separate machine where the ImageNow Server is running, you can install the Perceptive Configuration and Workflow Configuration options.

    Note For a two step installation, first install the PCR Configuration option and then the Perceptive Configuration and Workflow Configuration options. If you select Perceptive Configuration or Workflow Configuration, you must select the PCR Configuration as well, because ImageNow side configuration is not complete without the installation of eAuthorize PCR components. If you already installed eAuthorize PCR components, you can skip reinstallation of PCR components later during installation.

Custom Installation Option	Description	Software Prerequisites
Perceptive Configuration	Creates a customized Perceptive environment. Install Perceptive Configuration on the same machine as ImageNow Server.	• ImageNow Server • PCR eAuthorize components installed
Workflow Configuration	Creates a sample workflow and document types. Install Workflow Configuration on the same machine as ImageNow Server.	• ImageNow Server • PCR eAuthorize components installed
PCR Configuration	Installs all the files required for Perceptive eAuthorize PCR components on the same or different machine.	• Perceptive Connect Runtime • Content Connector on Perceptive Connect Runtime • Content Connector configured with the Integration server • All the Content Connector related components are in Active state

To install eAuthorize using the installer, complete the following steps.

1. Run the eAuthorize setup executable files.
2. In the **Welcome**page, click **Next**.
3. In the **License Agreement** page, read the License Agreement, scroll to the bottom of the agreement, select **I accept the terms in the license agreement**, and then click **Next**.
4. In the **Setup Type** page, select one of the following installation options.
    - **Complete**. Select **Complete** if you want all the components to be installed immediately. Click **Next** and continue to the next step.
    - **Custom**. Select **Custom** if you plan to install eAuthorize components in two steps. For details, see the Run the eAuthorize installer section. Click **Next** and perform the following substeps.

        1. Select from the following features to make the corresponding configuration changes. You can install PCR Configuration independently. To install, Perceptive Configuration and Workflow Configuration,the PCR Configuration must already be installed or be installed at the same time. For both of these configuration options PCR Configuration feature must be installed.
            - **Perceptive Configuration** creates a customized Perceptive environment on ImageNow Server, including custom properties, a reason list, reasons, task templates, audit history form, and ImmediatePresentment form all of which are required for eAuthorize.For ImageNow version below 7.1.5, an Envoy service is created.
            - **Workflow Configuration** creates the signature workflow and document types on ImageNow Server to get you started. For ImageNow version below 7.1.5, the workflow is created using Integration ASQ. For ImageNow version 7.1.5 and higher, the workflow contains Connect ASQ.

- **PCR Configuration** installs eAuthorize PCR Connector components on PCR. For ImageNow version 7.1.5 or higher it also configures the Connect ASQ channels, if the Workflow Configuration option is also selected. It can detect if eAuthorize connectors are already installed in PCR and provides an option to either keep the existing installation or overwrite the installation. This is a good option if the eAuthorize setup or PCR setup is distorted or partly broken.

Note If Perceptive Configuration and Workflow Configuration options are selected and PCR Configuration option is not selected, the installer displays a message that prompts you to select the PCR Configuration option as well and continue.If PCR Configuration is already installed, to install the Perceptive Configuration and Workflow Configurtaion, you must select the PCR Configuration option.

2. Click **Next**.

5. The **Perceptive Connect Runtime (PCR)Information** page allows you to enter the PCR server information and login credentials and click **Next**.

Note If PCR is installed on the same system as the eAuthorize installer, it fetches the PCR host and port information and populates the fields along with the default login credentials.If required, you can edit the field information.

6. If eAuthorize connector components are already installed on the target PCR server, a popup dialog box appears prompting you to select further installation options.
   - Click **OK** to reinstall the eAuthorize PCR components on the target PCR server.
   - Click **Cancel** to skip the connector installation, thereby keeping the existing installation unmodified.
7. In the **AssureSign Information** page, provide the following information.
   - In the **Assure Sign WSDL URL** box, enter the location of the sandbox or production instance in the AssureSign cloud or a URL to the local AssureSign web application you are using, as shown in the following examples.
     - For Sandbox, enter the location `https://sb.assuresign.net/Documents/Services/DocumentNOW/v2/DocumentNOW.svc?wsdl`
     - For production instance, enter the location `https://na1.assuresign.net/Documents/Services/DocumentNOW/v2/DocumentNOW.svc?wsdl`
     - If you use the locally installed AssureSign application, enter the following location.

       ```
       [Site Root]/AssurSign/services/documentnow/v2/documentnow.svc?wsdl
       ```

     Note For AssureSign local, the machine name and port number are where the local instance of AssureSign is installed.
   - In the **Local instance domain** box, enter the machine name where the local instance of AssureSign is installed. Leave this box blank if you are using an AssureSign cloud environment (sandbox or production).
   - In the **User Name** box, provide the user name for the account in AssureSign with which you submit documents for signature.

- In the **Context ID** box, provide the AssureSign DocumentNOW Account Context Identifier, which is a unique identifier needed in order to validate the request. If you have administrative access, you can find this identifier on the **Settings** page in AssureSign.
- In the **Template tag** box, you can provide any value (string). Use this value as the template tag when you create a template in AssureSign. For details, see the AssureSign Quick Reference Guide for instructions to create a template and the template tag.

  Note If the template tag value the in the Configuration page of Perceptive Connect Runtime dashboard does not match the same in the AssureSign template, documents cannot be submitted for signature.

8. Click **Next**.
9. In the **SMTP Information** page, provide the following information if you want to notify with an email address if the document cannot be submitted.
   - In the **Server Name/IP** box, type the name or IP address of the SMTP server that sends email notifications.
   - In the **Port** box, type the port of the SMTP server that sends email notifications.
   - In the **Sender Email ID** box, type the email ID configured on the SMTP server that sends email notifications.
   - Select the **Authentication required** check box if your SMTP email server requires authentication; otherwise, leave it unchecked.
     - If your SMTP email server requires authentication, in the **User ID** box, provide a user name for the email server.
     - If your SMTP email server requires authentication, in the**Password** box, provide the password corresponding to the user name you entered for the email server.
10. Click **Next**.
11. For Perceptive Content 7.1.5 or higher, the inputs to be provided in the **Connect ASQ Workflow Queue Information** page depends on the option selected during feature selection. During feature selection, you can select one of the following options.
    - Complete - If you select **Complete** installation option during feature selection, in the **Connect ASQ Workflow Queue Information** page, the workflow queue IDs must be left blank because the workflow queue IDs are automatically collected by the installer to create the channels in PCR.
    - Custom –If you select **Custom** installation option and **Workflow Configuration** option during feature selection, in the **Connect ASQ Workflow Queue Information** page, you must enter the relevant workflow queue IDs for **SubmitForSignature queue ID**, **DownloadSignedDocuments queue ID** and **SendToAssureSign queue ID**.

      For example, if eAuthorize 2.0 is already installed and you want to setup the Perceptive Content to be configured with a different PCR server, select **Custom** installation option and **Workflow Configuration** option and enter the workflow queue IDs in the **Connect ASQ Workflow Queue Information** page. If eAuthorize components are already installed on the target PCR and the channels are configured with a different Perceptive Content server, the installer populates the queue IDs from the PCR. You must validate the pre-populated data and modify accordingly. For details, see the Create and configure channels section.

> **Note** If the channels are not created during installation, you must collect the workflow Connect ASQ queue IDs from the Perceptive Content server and manually configure the channels in PCR.

12. In the **Ready to Install** page, click **Install**.
13. If the connectors are not properly configured, you need to open the **Perceptive Connect Runtime** UI to ensure that all the eAuthorize connectors are in Active state. If any of the connectors are not in Active state, restart the PCR server.
14. To continue with the post installation verification process, click **OK**. To skip the verification and continue, click **Cancel**.
15. In the **Installation Wizard Completed** page, optionally select the **Show the Windows Installer log** check box and then click **Finish**.

    Note If the installer fails to install certain components of eAuthorize, you need to install the components manually. To view the components that failed to install, check the Installer log. For additional information on how to install the components manually, see the Install eAuthorize manually section. You need to manually attach the **DocumentStoreAndForward.js** and **CreateTask.js** files. For details, see the Design workflow for sending documents for signature section. For ImageNow versions lower than 7.1.5, the installer creates an Envoy service named eAuthorize. Ensure that the Integration ASQ uses this Envoy service.

Install eAuthorize manually

Before you install eAuthorize manually, the following configurations must be installed and running.

- Perceptive Connect Runtime is installed and running.
- Content Connector is installed and running in Perceptive Connect Runtime.
- ImageNow Server and Integration Server are running.

To set up the eAuthorize connector, complete the following steps.

1. On the **Perceptive Connect Runtime** dashboard, select **Manage**>**Install a Connector**.
2. On the **Upload new bundles** page, complete one of the following steps.

- Drag the **eAuthorizeInstall-2.0.x.zip** file to the right side of the page
- Select **Manual Upload**. Under the **Open** dialog box, select the **eAuthorizeInstall-2.0.x.zip** file and select **Open**.

NotePerceptive Connect Runtime extracts and installs the bundles included in the ZIP file automatically and displays the number of installed bundles in the **Pending** box.

3. Select **Accept** to complete the installation. The installation summary appears in the **Completed** box.

4. Restart the PCR server.

Configure the app in Perceptive Connect Runtime

To configure the app in Perceptive Connect Runtime, complete the following steps.

1. In the **Perceptive Connect Runtime** dashboard, select **Manage**>**Configure**.
2. On the **Configuration** page, select **Configure eAuthorize**>**Configure AssureSign** and complete the following substeps to configure the AssureSign parameters.

   1. In the **WSDL URL** box, enter the AssureSign WSDL URL.
   2. In the **Local domain name** box, enter the name where AssureSign is installed locally. You need to populate this field for on premise AssureSign installation.
   3. In the **User name** box, enter the AssureSign account user name.
   4. In the **Context ID** box, enter the AssureSign Account Context ID.
   5. In the **Template tag** box, enter the AssureSign template tag.
   6. Click **Save**.

3. On the **Configuration** page, select **Configure eAuthorize**>**Configure Email** and perform the following substeps to configure theEmail parameters.
   1. In the **SMTP server name** box, enter the SMTP server name.
   2. In the **SMTP server port** box, enter the SMTP server port.
   3. In the **SMTP sender email ID** box, enter the SMTP server sender's email ID.

   NoteBy default, the **SMTP Authentication** check box is not selected. Select the check box if SMTP server authentication is required.

   4. In the **Authentication user name** box, enter the SMTP server authentication user name.
   5. In the **Authentication password** box, enter the SMTP server authentication password.
   6. Click **Save**.

Verify the connector JAR bundle status

To verify that the JAR bundle is correctly uploaded to Perceptive Connect Runtime, complete the following steps.

1. In the **Perceptive Connect Runtime** dashboard, select **Troubleshoot**>**List OSGi Bundles**.
2. On the **OSGI Bundles** page, under the **Name** column, search for the following bundle names.
   - eAuthorize Configurations
   - eAuthorizeAssureSignConnector
   - eAuthorizeCommon
   - eAuthorizeImageNowConnector
   - eAuthorizeSignatureEndpoint

Note Ensure that the status for all the bundles is Active. Active status indicates the bundle is started successfully.

3. Select **Troubleshoot**>**List OSGi Components**.
4. On the **OSGI Components** page, under the **Name** column, search for the following components.
   - eAuthorize AssureSign Connector
   - eAuthorize Download Signed Document Action
   - eAuthorize eForm Processor
   - eAuthorize ImageNow Connector

- eAuthorize REST Endpoint
- eAuthorize Send To AssureSign Action
- eAuthorize SignatureEndpoint
- eAuthorize Submit For Signature Action
- eAuthorizeASConfiguration
- eAuthorizeEmailConfiguration

Note Ensure that the status of all the components is Active. Active status indicates that the component is hosted successfully.

About Content Connector

Perceptive eAuthorize depends on the Content Connector to connect with the Perceptive Content Server. The credentials of the Department Manager are required. These credentials are stored in the configuration of the Content Connector.

Configure the Content Connector

To configure the Content Connector, complete the following steps.

1. In the **Perceptive Connect Runtime** dashboard, select **Manage**>**Configure**.
2. On the **Configuration** page, select **Perceptive Content Connector**>**Connection Manager**. To provide details for the Connection Manager, complete the following substeps.
    1. In the **Connection Provider Target** list, select **Integration Server 7.1**.

    Note For Perceptive Content 7.1.or above, select Integration Server 7.1. Similarly, for other versions select accordingly.

    2. In the **User Name** box, type the user name of the Department Manager of the view in **Perceptive Content Server**.
    3. In the **Password** box, type the password.
    4. Select **Save**.
3. Select **Perceptive Content Connector**>**Integration server 7.1 connection**, for Perceptive Content version 7.1.x.or higher. To provide details for Integration Server URL, complete the following substeps.
    1. In the **Integration Server URL** box, type the URL of the **Integration Server**.
    2. Select **Save**.
4. Verify the **PerceptiveConnect Extensions.js** script file that is copied to the <ImageNow Install Dir>/script folder.

Set up ImageNow Server

Configure ImageNow Server to submit documents for signature, to download the signed document, and to create a task to send notifications in the case of document failure.

Note If an older version of eAuthorize is already installed, you may skip the following steps, but it is recommended that you must verfiy the following steps.

To configure the ImageNow Server, complete the following steps.

1. Copy all script files from the **script** folder in e**Authorize_inserver.zip** file. The folder contains the following iScript files.
   - **CreateTask.js** – for creating a task in ImageNow if a document fails in workflow.
   - **DocumentStoreAndForward.js** – for storing and forwarding a document in workflow queue.
   - **RefreshAuditHistory.js** – for refreshing Audit History.
   - **eAuthorize** folder containing **IN_WorksheetManager.jsh**, **IN_XML.jsh**, **INBasePath.jsh**, and **Util_Misc.jsh**.
2. Paste these files to the <ImageNow Install Dir>/script folder.

Set up form for AssureSign Audit History

You can complete this procedure only if you are an owner or manager, or are assigned the Manage Forms privilege. A Forms license is required to use forms in eAuthorize. Without this license, the audit trail history will not be available in ImageNow but will be available from AssureSign. If you need a Forms license, contact your Perceptive Software representative.

Consider the following points when creating the Audit History eForm.

- Download and extract the **form** folder from **eAuthorize_inserver.zip** file in eAuthorize Installation Package. This folder contains the XSL files, supporting files, and the XML Data Definition file in **Audit_History** and **data_definition** folder, respectively.
- The data definition for AssureSign Audit History form is available in the **data_definition** folder.
- The XSL file and other supporting files required for the presentation of this form are available in the **Audit_History** folder.
- The name of the form must contain the words “AssureSign,” “Audit,” and “History.” This requirement is not case-sensitive.
- It is recommended that you create only one Audit History form, because data is populated in the form which appears first in the list of forms, alphabetically. If you erroneously create more forms, delete them.
- To create the AssureSign Audit History form, see the Create a form from your data definition file and presentations section
- To manually upload data definition file, see the Manually upload form definition files in ImageNow server section.

Manually upload form definition files in ImageNow server

To manually upload an XML data definition file, XSL files, supporting files, and organize your files into presentations, complete the following steps.

1. In the left pane of **Management Console**, under **Select Department**, select a department from the list.
2. In the left pane, click **Forms**.
3. In the right pane, click **Manage Components Manually**.
4. On the **Manage Form Components** dialog box, perform any of the following procedures, as described in the table below.

Situation	Steps
Upload an XML data definition file	1. In the **Data Definitions** pane, click **Add**. 2. In the **File Open** dialog box, navigate to the folder where your local form files are stored, select the XML file you created for this form and click **Open**.
Create a presentation	1. On the **Presentations** pane, click **Create**, type a name for your presentation and then press ENTER. 2. Select the presentation you just created and click **Modify**. 3. Optional. In the **Presentation** dialog box, in the **General** pane, type a description for your presentation.
Upload an XSL file for your presentation	1. In the presentation, in the **Files** pane, click **Add**, select the XSL file and any optional files you created for this presentation. 2. Click **Open**.

5. Click **OK**.

Create a form from your data definition file and presentations

To create a new form from your data definition file and presentations, complete the following steps.

1. In the left pane of **Management Console**, under **Select Department**, select a department from the list.
2. In the left pane, click **Forms**.
3. In the right pane, on the **Forms** tab, click **New**.
4. Type a unique name for your form and then press ENTER.
5. Select the form you just created and click **Modify**.
6. Optional. In the **Form** dialog box, in the **General** pane, in the **Description** box, type a description for your form.
7. In the left pane, click **Components**.

8. In the right pane, under **Data Definition**, in the **Data definition** list box, select the XML file you created for this form.
9. Click **Select** to choose presentations you want to be available for use with this form.
10. In the **Select Presentations** dialog box select the presentations and click **OK**.
11. Click **OK**.

Refresh time out for Audit History

To modify the refresh time for Audit History form, complete the following steps.

1. Copy the **eAuthorize** folder from **etc** directory available in the **inserver.zip** file and paste it to the <ImageNow Install Dir>\etc directory.
2. Open eAuthorize from the <ImageNow Install Dir>\etc directory, then open the **eAuthorize_config.xml** file, and edit the following configuration parameters.
    1. Provide the Envoy service name for eAuthorize within the **<envoyName>** tag.

    Note For Perceptive Content 7.1.5 or higher, you must leave the **<envoyName>** tag blank.

    2. Provide the time out in seconds within the **<refreshTimeout>** tag.

Set up form for AssureSign ImmediatePresentment

You can complete this procedure only if you are an owner or manager, or have the Manage Forms privilege. A Forms license is required to use forms in eAuthorize. If you need a Forms license, contact your Perceptive Software representative. If the form license is not activated, the AssureSign ImmediatePresentment form is not available in ImageNow.

To create the AssureSign ImmediatePresentment eForm, consider the following points.

- Download and extract the **eAuthorize_ImmediatePresentmentForm.zip** file from eAuthorize Installation Package. This archive contains the XSL files, supporting files, and the XML Data Definition file in **presentation** and **data_definition** folder, respectively.
- The data definition for AssureSign Audit History form is available in the **data_definition** folder.
- The XSL file and other supporting files required for the presentation of this form are available in the **Audit_History** folder.
- The name of the form must contain the words “AssureSign,” “Immediate,” and “Presentment.” This requirement is not case-sensitive.
- It is recommended that you create only one AssureSign ImmediatePresentment form, because data is populated in the form which appears first in the list of forms, alphabetically. If you have erroneously created more forms, delete them.

To set up AssureSign ImmediatePresentment form, you must manually load form components into ImageNow server and create a form from your data definition file and presentations. For details, see the following sections.

- Create a form from your data definition file and presentations
- Manually upload form definition files in ImageNow server

Design workflow for sending documents for signature

If you install eAuthorize manually, you must create a workflow process to send documents to AssureSign for signature and download the signed documents in ImageNow. These instructions may also be helpful if you install eAuthorize using the installer, but want to modify the workflow that is automatically created by the installer.

You can only complete this procedure if you are a user with the global privilege to manage workflow processes, a manager, or the owner. This procedure creates automated system queues (ASQs).

To create your workflow process, complete the following steps.

1. On the **ImageNow** toolbar, click **Manage**, and then click **Workflow**.
2. On the **Workflow** tab, click **New**.
3. Enter a name for the workflow process.
4. Optional. Enter a description for your workflow process.
5. Click **OK**.
6. Double-click the process to open it in the **Workflow Designer**.
7. Create your workflow process by performing the following substeps.
    1. In the **Workflow Designer** window, in the left pane, under **Queues**, select the **IntegrationASQ** or **Connect ASQ** icon and drag it to the right in your workflow diagram. Repeat this step to create two more ASQs.

       Note In this example, the ASQs are SubmitForSignature, DownloadSignedDocuments, and SendToAssureSign. You can supply other names for the ASQs. For ImageNow versions lower than 7.1.5, use **IntegrationASQ** and for Perceptive Content, versions 7.1.5 and higher use **Connect ASQ**. For details, see steps 14 and 15.
    2. In the left pane, under **Queues**, select the **Work** queue and then drag it to the right in your workflow diagram.
    3. Double-click the queue to modify its properties.
    4. In the **Queue Properties** dialog box, in the left pane, select **Properties**.
    5. In the right pane, in the **Name** box, enter **SignatureRequested**.
    6. Click **OK**.
    7. Repeat the substeps 2 to 6 to create the **DocumentStore**, **DocumentInProgress**, **SignatureComplete**, and **SignatureFailure** work queues.
    8. Double-click **DocumentStore**.
    9. In the left pane, click **Actions** and complete the following substeps.
        1. Under **Inbound**, in the **iScript** list, select **Edit iScripts** and click **Add**.
        2. Select **DocumentStoreAndForward.js** and click **OK**.
    10. Click **OK**.
    11. Double-click **SignatureFailure**.
    12. In the left pane, click **Actions** and complete the following substeps.
        1. Under **Inbound**, in the **iScript** list, select **Edit iScripts**, and click **Add**.

    2. Select **CreateTask.js** and click **OK**.

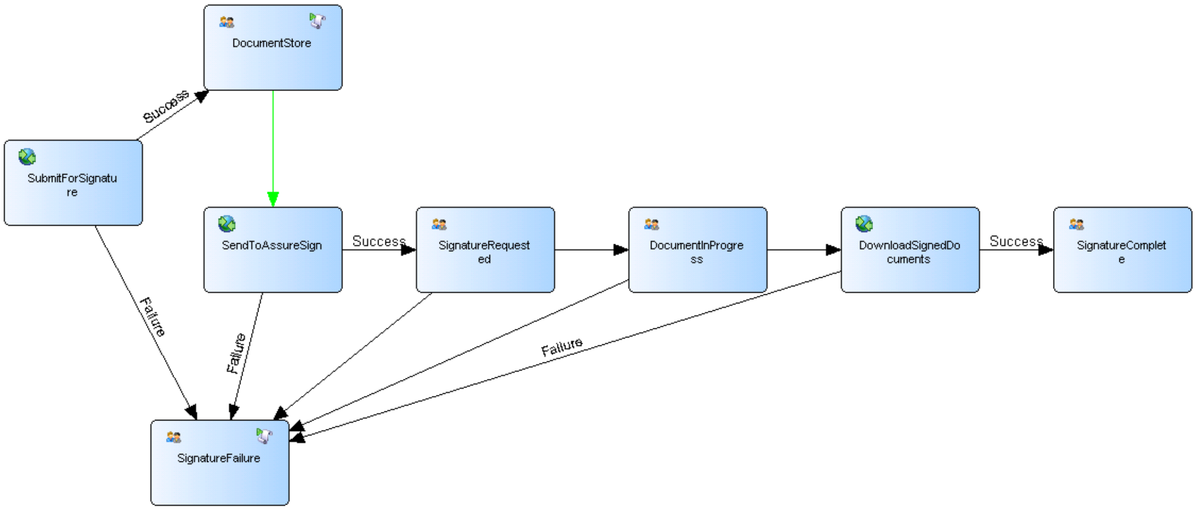
13. Click **OK.**

14. For Perceptive Content versions below 7.1.5, to configure **SubmitForSignature**,**DownloadSignedDocuments**, and **SendToAssureSign** ASQ, complete the followng steps.

    Note You must have an Envoy license to use Integration ASQs. Perform this procedure to create a queue that sends web service notifications to any business application. Before performing this procedure, you must create two queues: one queue for successfully processed items and another queue for processing unsuccessful items. In addition, you must define an Envoy service name and the number of days an item can remain in the Integration ASQ after your business application receives a successful call for that item. You have to create two ASQs, one for submitting document for signature and another for downloading signed documents.

    1. Double-click the queue to modify its properties.
    2. Under **Automated Action**, perform the following substeps.
        1. To designate the process and queue for items processed in the **SubmitForSignature** queue, in the **Success Action** list, select the workflow process in the **Process** list, and select **DocumentStore** queue in the **Queue** list.
        2. To designate the process and queue for items that do not successfully process in this queue, in the **Failure Action** list, select the workflow process created in the **Process** list, and select **SignatureFailure** queue in the **Queue** list.
        3. To set the number of days that items remain in this queue after the business application receives a successful call for those items, in the **Route After (Days)** box, type a number. The maximum number of days is 365. By default, ImageNow routes items to the failure queue after one day.

           Note If your business application does not place a web service call for an item, that item remains in the Integration ASQ for the number of days you specify in the **Route After (Days)** box.
        4. To designate the endpoint that receives web service notifications from this queue, only service operations that are available to use in workflow appear in the **Service Operation Name** list. You can perform this step after the Envoy service is created.
    3. Repeat the above substeps to configure **DownloadSignedDocuments** Integration ASQ with the following configurations.
        - For **Success Action**, select **SignatureComplete** from **Queue list**
        - For **FailureAction**, select **SignatureFailure** from the **Queue** list.
    4. Repeat the steps above to configure**SendToAssureSign** Integration ASQ with the following configurations.
        - For **Success Action**, select **SignatureRequested** from **Queue** list
        - For **Failure Action**, select **SignatureFailure** from the **Queue** list.
    5. To complete the workflow process, join the queues as shown in the following figure.



6. To create the routes between the queues, complete the following substeps.
   1. In **Workflow Designer**, in the **Task** pane, click **Routes**.
   2. On the **Grid** toolbar, verify that the **Normal Routes** button is selected.
   3. Under **Routes**, select **Sequential route**.
   4. To create a route from one queue to another queue, click on the queue where you want the route to begin and drag your cursor to the queue where you want the route to end.

   Note Ensure that the route from **DocumentStore** to **SendToAssureSign** is a **Seq-Auto route**.

   5. After completing the workflow process creation, close the **Workflow Designer**.

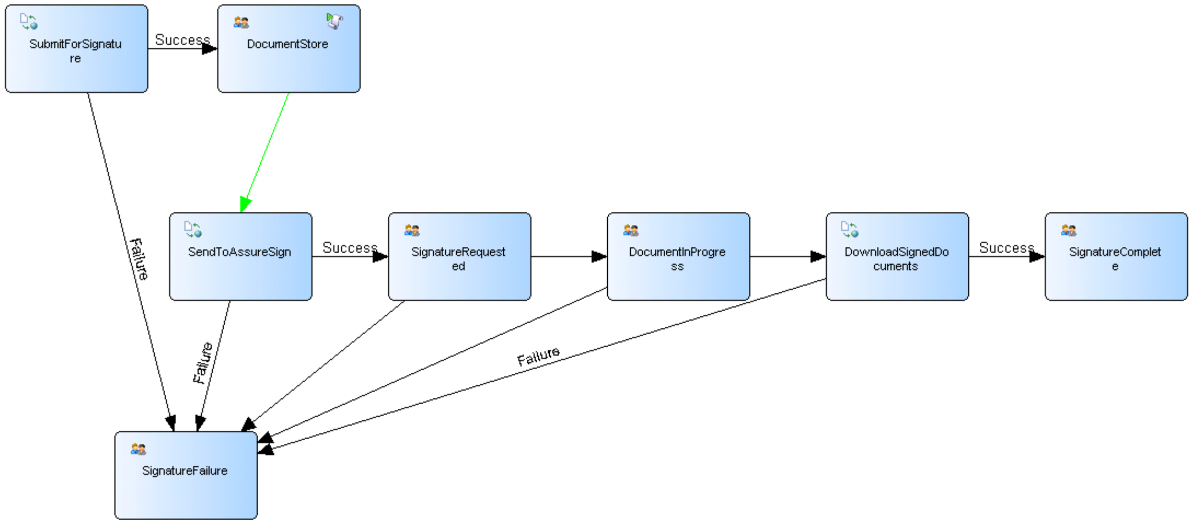
15. ForPerceptive Content version 7.1.5 or higher, you must use Connect ASQ instead of Integration ASQ in order to configure **SubmitForSignature**, **DownloadSignedDocuments**, and **SendToAssureSign** ASQ, complete the followng steps.

    Note If an older version of eAuthorize is already installed, delete the **SubmitToSignature**, **SendToAssureSign** and **DownlaodSigned Documents** Integration ASQs from the workflow. Currently, Integration ASQ is replaced with Connect ASQ.

    1. Double-click the **SubmitForSignature** queue to modify its properties.
    2. Under **Automated Action**, perform the following substeps.
       1. To designate the process and queue for items processed in **SubmitForSignature** queue, in the **Success Action** list, select the workflow process in the **Process** list, and select **DocumentStore** queue in the **Queue** list.
       2. To designate the process and queue for items that do not successfully process in this queue, in the **Failure Action** list, select the workflow process created in the **Process** list, and select **SignatureFailure** queue in the **Queue** list.
       3. To set the number of days that items remain in this queue after the business application receives a successful call for those items, in the **Route After (Days)** box, type a number. The maximum number of days is 365. By default, ImageNow routes items to the failure queue after one day.

Note If your business application does not place a web service call for an item, that item remains in the Connect ASQ for the number of days you specify in the **Route After (Days)** box.

3. Repeat the steps above to configure**DownloadSignedDocuments** Connect ASQ with the following configurations.
    - For **SuccessAction**, select **SignatureComplete** from **Queue** list, and for **FailureAction**, select **SignatureFailure** from the **Queue** list.
4. Repeat the steps above to configure**SendToAssureSign** Connect ASQ with the following configurations.
    - For **Success Action**, select **SignatureRequested** from **Queue** list, and for **Failure Action**, select **SignatureFailure** from the **Queue** list.
5. To create a complete workflow, join the queues as shown in the following figure.



6. To create the routes between the queues, complete the following substeps.

    1. In **Workflow Designer**, in the **Task** pane, click **Routes**.
    2. On the **Grid** toolbar, verify that the **Normal Routes** button is selected.
    3. Under **Routes**, select **Sequential route**.
    4. To create a route from one queue to another queue, click on the queue where you want the route to begin and drag your cursor to the queue where you want the route to end.

    Note Ensure that the route from **DocumentStore** to **SendToAssureSign** is a **Seq-Auto route**.

    5. After completing the workflow process creation, close the **Workflow Designer**.

Note If the flow of documents is interrupted anywhere in this workflow it redirects to the **Failed** queue. To route the documents manually to the queue from where it was interrupted, you can open the document in **Workflow** and click **RouteBack**.

Configure the Content Connect service

For Perceptive Content 7.1.5 or higher, a new queue type called Connect ASQ is available, which can be configured to use a single instance of the Connect Runtime.

To configure the Content Connect service, complete the following steps.

1. Navigate to the location the **[*drive*:]\inserver\etc** directory where Content Server is installed.
2. Open the **inserverWorkflow.ini** file and perform the following substeps.
    1. Configure the `connect.uri` setting and set it to your Connect Runtime instance with the followingformat.
        - http://{Connect Runtime host name}:{port}/rs/workflowTrigger
    2. Configure the `connect.timeout` to your desired expiration time.
3. Save the file.
4. Optional. The setting will be automatically loaded after a short period. To reload the configuration immediately, you can restart the Content Server service.

Set up the Envoy services

For ImageNow versions lower than 7.1.5, to configure the Envoy services, complete the following steps.

1. Log into ImageNow, and on the **ImageNow** toolbar, click **Manage**, and then click **Envoy Services**.
    1. Click **New** in the right pane.
    2. In the **Envoy Services** page, complete the following steps.
        1. In the **Name** box, type **eAuthorize**.
        2. In the **Description** box, type a description.
        3. In the **URI** box, type `http://<Connect Runtime host name>:<port>/ws/SignatureEndpoint?wsdl`, replacing `<Connect Runtime host name>`and <`port>` with your specific information.
        4. In the **Authentication** list, select **None** and verify that the **Enable interceptor logging** check box is cleared.
        5. Click **Next**.
        6. Ensure that all of the items under **ESignatureService** are selected.
        7. Click **Finish**.
2. In **Management Console,** in the left pane, click **Workflow**.
    1. On the **Workflow** tab, click **eAuthorize**, click **Modify**and complete the following step.
        - Complete the following substeps to configure the **SubmitForSignature** Integration ASQ.
            1. In **Workflow Designer**, double-click **SubmitForSignature**.
            2. For **Envoy Service**, in the **Service Operation Name** list, select the **eAuthorize:: SubmitForSignature** Envoy service.

               Note You do not need to map Envoy Service Parameters.
            3. Click **OK**.

2. Complete the following substeps to configure the **SendToAssureSign** Integration ASQ.
    1. In **Workflow Designer**, double-click **SendToAssureSign**.
    2. For **Envoy Service**, in the **ServiceOperationName** list, select the **eAuthorize::SendToAssureSign** Envoy service.

        NoteYou do not need to map Envoy Service Parameters.
    3. Click **OK**.
3. Complete the following substeps to configure the **DownloadSignedDocuments** Integration ASQ.
    1. In **WorkflowDesigner**, double-click **DownloadSignedDocuments**.
    2. For **EnvoyService**, in the **ServiceOperationName** list, select the **eAuthorize::DownloadSignedDocument** Envoy service.

        Note You do not need to map Envoy Service Parameters.
    3. Click **OK**.

Create and configure channels

For Perceptive Content version 7.1.5 and higher you need to configure the Connect ASQ channels. To create and configure channels using Perceptive Connect Runtime, complete the following steps.

1. In the **Perceptive Connect Runtime** dashboard, select **Manage**>**Create a channel**.
2. In the **Name** box, provide a channel name.
3. In the **Trigger** list, select `Integration ASQ Trigger`.

Note If Content Connector is not installed, Integration ASQ Trigger will not appear in the **Trigger** list.

4. In the **Workflow Queue ID** box, type the Integration queue ID of the SubmitForSignature queue that was created previously.
5. Click **Continue**.
6. In the **Actions** list, select `SubmitForSignatureAction`available in the **EAuthorizeSignatureEndpoint** section.
7. Click **Save Inputs**.
8. Click **Enable Channel**.
9. Click **Create a channel** and provide a channel name for SendToAssureSign queue.
10. In the **Trigger** list, select `Integration ASQ Trigger`.
11. In the **Workflow Queue ID** box, type the Integration queue ID of the SendToAssureSign queue that was created previously.
12. In the **Actions** list, select `SendToAssureSignAction`available in the **EAuthorizeSignatureEndpoint** section.
13. Click **Save Inputs**.
14. Click **Enable Channel**.
15. Click **Create a channel** and provide a channel name for the DownloadSignedDocumentChannel queue.

16. In the **Trigger** list, select `Integration ASQ Trigger`.
17. In the **Workflow Queue ID** box, type the Integration queue ID of the DownloadSignedDocumentChannel queue that was created previously.
18. In the **Actions** list, select `DownloadSignedDocumentsAction` available in the **EAuthorizeSignatureEndpoint** section.
19. Click **Save Inputs**.
20. Click **Enable Channel**.

Create new custom properties

To create new custom properties, complete the following steps.

1. On the **ImageNow** toolbar, click **Manage**.
2. To create a custom property for **Signatory 1 Full Name**, perform the following substeps.
    1. In **Management Console**, in the left pane, click **Custom Properties**. In the right pane, point to **New** and click **String**.
    2. In the **Name** box, type **Signatory 1 Full Name.**
    3. Click **OK**.
3. Repeat the previous step to create each of the custom properties: Signatory 1 Email Address, AS_ID, AS_SIGNATURE_STATUS, and AS_AUTH_TOKEN.
4. To create a flag that enables you to keep the original unsigned document, perform the following substeps.
    1. Click **New** and select **Flag**.
    2. In the **Name** box, type `AS_KEEP_ORIGINAL_DOCUMENT`.
    3. Click **OK**. For more information about using this flag, see the *Perceptive eAuthorize Getting Started Guide*.
5. To create a list of failure notifications, perform the following substeps.
    1. Click **New** and select **List**.
    2. In the **Name** box, type `AS_FAILURE_NOTIFICATION_TYPE`.
    3. Click **Add**, type `Email`, and press ENTER. Repeat this step to add **Task** and **Both**.
    4. In the **Default value** list, select **Email** as the default value**.**
    5. Click **OK**.

Notes

- Signatory 1 Full Name and Signatory 1 Email Address are the input parameters for AssureSign Connector that you must provide. AS_ ID, AS_AUTH_TOKEN, and AS_SIGNATURE_STATUS are the output parameters for AssureSign Connector that automatically populate.
- Various actions occur depending on the value you set for **AS_FAILURE_NOTIFICATION_TYPE**.
    - **Email**. If the document fails in the workflow, an email is sent to the email ID that you configured in ImageNow while creating user profiles. You must provide the SMTP server name, port, email ID in the **Configuration** page of **Perceptive Connect Runtime** dashboard, and the authentication if needed.

- **Task**. You receive a task in **My Assigned** view in ImageNow that shows that the document failed in workflow.
- **Both**. You receive an email in your email account and a task in ImageNow.

Set up ImageNow for signing

You can complete the procedures in the following sections if you are a user with global privileges, a manager, or the owner.

The eAuthorize installation wizard sets up several aspects of ImageNow to get you started. These automatic configurations are detailed in Appendix A: About the eAuthorize ImageNow configuration. However, before you can send a document to AssureSign for signing, there are some ImageNow configurations you need to complete using the Management Console. The following list is an overview of these procedures.

1. Create document types and assign custom properties
2. Configure task templates for document notification
3. Create a folder type to send multiple documents for signing
4. Design workflow for sending documents for signature

Create document types and assign custom properties

To create document types and assign custom properties, complete the following steps.

1. On the **ImageNow** toolbar, click **Manage**.
2. In **Management Console**, in the left pane, click **DocumentTypes**.
3. In the right pane, click **New**, and then type a name for the document type that matches the name of the corresponding template in AssureSign. For details, see the AssureSign Quick Reference Guide for instructions on creating a template.
4. To assign custom properties to the document type, complete the following substeps.
    1. Select the document type from the previous step and click **Modify**.
    2. In the **CustomProperties** tab, in the **By Type** list, select **All**.
    3. Select the appropriate custom properties in the list and then click **Add**. The following properties are required.
        - AS_AUTH_TOKEN
        - AS_FAILURE_NOTIFICATION_TYPE
        - AS_ID
        - AS_KEEP_ORIGINAL_DOCUMENT
        - AS_SIGNATURE_STATUS
        - Signatory 1 Email Address
        - Signatory 1 Full Name

        Note To add more custom properties, see the About custom properties for multiple signatures section.

4. To mark these properties as required, click the column in front of the custom property until the **Required**⊕ icon displays.
5. Click **OK**.

Configure task templates for document notification

You receive a task in the My Assigned view in ImageNow when a submitted document fails in workflow. You can also opt to receive email notifications when submitting the document for signature.

The eAuthorize installation wizard automatically creates task templates, reasons, and a reasons list. The installation wizard also populates the reason lists with the corresponding reason list member and associates the appropriate action reasons and return reasons with each task template. For a table showing these correlations, see the Task templates section.

To configure the task templates, complete the following steps.

1. On the **ImageNow** toolbar, click **Manage**.
2. In **Management Console**, in the left pane, click **Tasks**.
3. In the right pane, on the **Templates** tab, in the **Select a task type** box, click **Pointer**.
4. On the **Templates**tab, select **FailureNotification_Cancelled** and click**Modify**.
5. In the **Pointer Task** dialog box, complete the following steps.
    1. In the left pane, select **Properties**.
        1. In the **Description** box, type a template description.
        2. Under **Options**, check the **Is active** check box to make the task template available to task creators assigning tasks from the **Tasks** toolbar.
    2. In the left pane, click **Components**.
        1. In the right pane, under **General**, in the **Task instructions** box, type the instructions you want your task assignees to see. These instructions are the content for the email notifications that the system sends to the task assignee. You can base your instructions on the **Action Reason List** column in the table in the Task templates section.
        2. If you want to allow a task creator to modify the instructions on the **Options** tab in the **NewTask** dialog box, ensure that the **Modifiable during task creation** check box is selected.
        3. In the **Task location** section, select the following locations to determine where tasks created with this template are assigned.
            - **Folder.** Create a task for a folder.
            - **Document.** Create a task for a document.
            - **Page without a visual representation.** Create a task for a page in a document with no visual representation.
            - **Page with a visual representation.** Create a task, along with a visual representation, for a page in a document.
        4. In the **Completion** box, select **Manual**.
        5. Optional. On **WorkflowAssignment**, in the **Send to queue** list, select **(None)**.
    3. In the left pane, click **Assignment**.

        1. In the right pane, click **Add**.
        2. In the **Select Users and Groups** dialog box, assign the users and groups you want to have access to this task.
    4. Optional. In the left pane, click **Reasons** and then select the **Assignee must specify a reason during task completion** check box to require task assignees to select a reason after completing a task.
6. Repeat this procedure four more times to configure the remaining eAuthorize pointer task templates.
    - FailureNotification_Declined
    - FailureNotification_DownloadFailed
    - FailureNotification_Expired
    - FailureNotification_SubmissionFailed
7. In the **Pointer Task** dialog box, complete the following steps.
    1. In the left pane, select **Properties**.
        1. In the **Description** box, type a template description.
        2. Under **Options**, check the **Is active** check box to make the task template available to task creators assigning tasks from the **Tasks** toolbar.
    2. In the left pane, click **Components**.
        1. In the right pane, under **General**, in the **Task instructions** box, type the instructions you want your task assignees to see. These instructions are the content for the email notifications that the system sends to the task assignee. You can base your instructions on the **Action Reason List** column in the table in the Task templates section.
        2. If you want to allow a task creator to modify the instructions on the **Options** tab in the **NewTask** dialog box, ensure that the **Modifiable during task creation** check box is selected.
        3. In the **Task location** section, select the following locations to determine where tasks created with this template are assigned.
            - **Folder.** Create a task for a folder.
            - **Document.** Create a task for a document.
            - **Page without a visual representation.** Create a task for a page in a document with no visual representation.
            - **Page with a visual representation.** Create a task, along with a visual representation, for a page in a document.
        4. In the **Completion** box, select **Manual**.
        5. Optional. On **WorkflowAssignment**, in the **Send to queue** list, select **(None)**.
    3. In the left pane, click **Assignment**.
        1. In the right pane, click **Add**.
        2. In the **Select Users and Groups** dialog box, assign the users and groups you want to have access to this task.

4. Optional. In the left pane, click **Reasons** and then select the **Assignee must specify a reason during task completion** check box to require task assignees to select a reason after completing a task.

8. Repeat this procedure four more times to configure the remaining eAuthorize pointer task templates.
   - FailureNotification_Declined
   - FailureNotification_DownloadFailed
   - FailureNotification_Expired
   - FailureNotification_SubmissionFailed

Create a folder type to send multiple documents for signing

You can send multiple documents for signature at the same time by sending a folder of documents to be signed through an AssureSign envelope. To create a folder type to send multiple documents for signing, complete the following steps.

1. On the **ImageNow** toolbar, click **Manage**.
2. In **Management Console**, in the left pane, click **Folder Types**.
3. In the right pane, under **Folder Types**, click **New** and specify a name that matches the name of the corresponding envelope type name in AssureSign. For details, see the AssureSign Quick Reference Guide for instructions on creating an envelope.
4. Select the new folder type and click **Modify**.
   1. On the **Document Types** tab, select the document type you created in the Create document types and assign custom properties section of this document and click **Add**.
   2. On the **Custom Properties** tab, in the **By Type** list, select **(All)**.
   3. Select **AS_ID, AS_AUTH_TOKEN**,**AS_SIGNATURE_STATUS**, and **AS_FAILURE_NOTIFICATION_TYPE** and then click **Add**.

      Note AS_ID, AS_AUTH_TOKEN and AS_SIGNATURE_STATUS represent corresponding values of an AssureSign envelope.
   4. Click **OK**.

Set up the AssureSign environment

Set up AssureSign DocumentTRAKfor status notifications

Log into AssureSign to configure the following DocumentTRAK web notifications. If you are using a local instance of the AssureSign environment, see the Appendix C: Copy web notification templates for information on copying AssureSign web notification templates from the sandbox environment.

eAuthorizeDocumentStatus

1. On the **Administration** tab, on the left, click **DocumentTRAK**.
2. In the **Web Notifications** section, copy the **eAuthorizeDocumentStatus** web notification template.
   1. Select **Edit** for the **General Information** section.
   2. In the **Design Name** box, enter a name for the web notification.

3. In the **Service Endpoint (URL)** box, replace **[Server IP]** with the `http://<Connect Runtime host name>:<port>/ws/SignatureEndpoint`and click **Next**.
4. Select **Edit Raw XML**and click **Next**.
5. Verify that the content of the XML file is similar to the following example and click **Next**.

```
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope
    xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:esig="http://www.perceptivesoftware.com/asq/esignature">
<soapenv:Header/>
<soapenv:Body>
<esig:UpdateStatusDocument>
<DOC_ORDER_ID>[Order ID]</DOC_ORDER_ID>
<DOC_STATUS>[Document Status]</DOC_STATUS>
</esig:UpdateStatusDocument>
</soapenv:Body>
</soapenv:Envelope>
```

6. Select **Compare response to expected XML string** and click **Next**.
7. Select **Edit Raw XML** and click **Next**.
8. Verify that the XML is similar to the following example, click **Next**, and then click **Finish**.

```
<soap:Envelope
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body>
<ns2:UpdateStatusDocumentResponse
            xmlns:ns2="http://www.perceptivesoftware.com/asq/esignature">
<Return>true</Return>
</ns2:UpdateStatusDocumentResponse>
</soap:Body>
</soap:Envelope>
```

eAuthorizeStepStart

1. On the **Administration** tab, open **Notifications,** and click **DocumentTRAK**.
2. In the **Web Notifications** section, copy the **eAuthorizeStepStart** web notification template.
    1. Select **Edit** for the **General Information** section.
    2. In the **Design Name** box, enter a name for the web notification.
    3. In the **Service Endpoint (URL)** box, replace **[Server IP]** with the `http://<Connect Runtime host name>:<port>/ws/SignatureEndpoint`and click **Next**.
    4. Select **Edit Raw XML** and click **Next**.
    5. Verify that the XML is similar to the following example and click **Next**.

```
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope
    xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:esig="http://www.perceptivesoftware.com/asq/esignature">
<soapenv:Header/>
<soapenv:Body>
<esig:UpdateStatusStepStarted>
<DOC_ORDER_ID>[Order ID]</DOC_ORDER_ID>
<DOC_SIGNING_STEP>[Signing Step]</DOC_SIGNING_STEP>
</esig:UpdateStatusStepStarted>
```

```
</soapenv:Body>
</soapenv:Envelope>
```

6. Select **Compare response to expected XML string** and click **Next**.
7. Select **Edit Raw XML** and click **Next**.
8. Verify that the XML is similar to the following example, click **Next**, and then click **Finish**.

```
<soap:Envelope
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body>
<ns2:UpdateStatusStepStartedResponse
            xmlns:ns2="http://www.perceptivesoftware.com/asq/esignature">
<Return>true</Return>
</ns2:UpdateStatusStepStartedResponse>
</soap:Body>
</soap:Envelope>
```

eAuthorizeStepComplete

1. On the **Administration** tab, open **Notifications** and click **DocumentTRAK**.
2. In the **Web Notifications** section, copy the **eAuthorizeStepStart** web notification template.
    1. Select **Edit** for the **General Information** section.
    2. In the **Design Name** box, enter a name for the web notification.
    3. In the **Service Endpoint (URL)** box, replace **[Server IP]** with the `http://<Connect Runtime host name>:<port>/ws/SignatureEndpoint`and click **Next**.
    4. Select **Edit Raw XML** and click **Next**.
    5. Verify that the XML is similar to the following example and then click **Next**.

```
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope
    xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:esig="http://www.perceptivesoftware.com/asq/esignature">
<soapenv:Header/>
<soapenv:Body>
<esig:UpdateStatusStepCompleted>
<DOC_ORDER_ID>[Order ID]</DOC_ORDER_ID>
<DOC_SIGNING_STEP>[Signing Step]</DOC_SIGNING_STEP>
</esig:UpdateStatusStepCompleted>
</soapenv:Body>
</soapenv:Envelope>
```

6. Select **Compare response to expected XML string** and click **Next**.
7. Select **Edit Raw XML** and click **Next**.
8. Verify that the XML is similar to the following example, click **Next**, and then click **Finish**.

```
<soap:Envelope
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body>
<ns2:UpdateStatusStepCompletedResponse
            xmlns:ns2="http://www.perceptivesoftware.com/asq/esignature">
<Return>true</Return>
</ns2:UpdateStatusStepCompletedResponse>
</soap:Body>
```

```
</soap:Envelope>
```

eAuthorizeStepUserVisit

1. On the **Administration** tab, open **Notifications** and click **DocumentTRAK**.
2. In the **Web Notifications** section, copy the **eAuthorizeStepStart** web notification template.
    1. Select **Edit** for the **General Information** section.
    2. In the **Design Name** box, enter a name for the web notification.
    3. In the **Service Endpoint (URL)** box, replace **[Server IP]** with the `http://<Connect Runtime host name>:<port>/ws/SignatureEndpoint` and click **Next**.
    4. Select **Edit Raw XML** and click **Next**.
    5. Verify the XML looks like the following example and then click **Next**.

    ```
    <?xml version="1.0" encoding="utf-8"?>
    <soapenv:Envelope
        xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:esig="http://www.perceptivesoftware.com/asq/esignature">
    <soapenv:Header/>
    <soapenv:Body>
    <esig:UpdateStatusStepLandingPageVisited>
    <DOC_ORDER_ID>[Order ID]</DOC_ORDER_ID>
    <DOC_SIGNING_STEP>[Signing Step]</DOC_SIGNING_STEP>
    </esig:UpdateStatusStepLandingPageVisited>
    </soapenv:Body>
    </soapenv:Envelope>
    ```

    6. Select **Compare response to expected XML string** and click **Next**.
    7. Select **Edit Raw XML** and click **Next**.
    8. Verify that the XML is similar to the following example, click **Next**,and then click **Finish**.

    ```
    <soap:Envelope
        xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Body>
    <ns2:UpdateStatusStepLandingPageVisitedResponse
                xmlns:ns2="http://www.perceptivesoftware.com/asq/esignature">
    <Return>true</Return>
    </ns2:UpdateStatusStepLandingPageVisitedResponse>
    </soap:Body>
    </soap:Envelope>
    ```

eAuthorizeDocumentCompleted

1. On the **Administration** tab, open **Notifications** and click **DocumentTRAK**.
2. In the **Web Notifications** section, copy the **eAuthorizeDocumentCompleted** web notification template and complete the following substeps to edit the XML data.
    1. Select **Edit** for the **General Information** section.
    2. In the **Design Name** box, enter a descriptive name for the web notification**.**
    3. In the **ServiceEndpoint (URL)** box, replace **[Server IP]** with the `http://<Connect Runtime host name>:<port>/ws/SignatureEndpoint` and click **Next**.
    4. Select **Edit** in the **RequestXML** section.

5. Select **EditRawXML** and click **Next**.
6. Replace the original text in the XML with the following highlighted text. Note that this is for indexing a signed document within ImageNow. If the document originated within ImageNow and you want to maintain the original document index values, leave the field values blank.

   To do this, complete the following substep.

   - Select the existing text in the code in place of the highlighted text and click the exact parameter name enclosed in brackets in the **RequestXMLEditing** box.

   Note The values for `<field1>` through `<field5>` can be static text (no brackets) or can contain the name of an AssureSign jotblock within brackets ([JotblockName]) so the jotblock value can be populated as the index field. For any empty field in AssureSign, the corresponding field in ImageNow remains unchanged.

```
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope
    xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:esig="http://www.perceptivesoftware.com/asq/esignature">
<soapenv:Header/>
<soapenv:Body>
<esig:UpdateStatusDocumentCompleted>
<DOC_AUTH_TOKEN>[Document AuthToken]</DOC_AUTH_TOKEN>
<DOC_ID>[Document ID]</DOC_ID>
<DOC_ORDER_ID>[Order ID]</DOC_ORDER_ID>
<field1>(Field 1 value)</field1>
<field2>(Field 2 value)</field2>
<field3>(Field 3 value)</field3>
<field4>(Field 4 value)</field4>
<field5>(Field 5 value)</field5>
</esig:UpdateStatusDocumentCompleted>
</soapenv:Body>
</soapenv:Envelope>
```

7. Select **Compare response to expected XML string** and click **Next**.
8. Select **Paste Raw XML** and click **Next**.
9. Type the following code in the **Expected Response XML Editing** box and click **Finish**.

```
<soap:Envelope
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body>
<ns2:UpdateStatusDocumentCompletedResponse
            xmlns:ns2="http://www.perceptivesoftware.com/asq/esignature">
<Return>true</Return>
</ns2:UpdateStatusDocumentCompletedResponse>
</soap:Body>
</soap:Envelope>
```

eAuthorizeDocumentStatusKBA

1. On the **Administration** tab, on the left, click **DocumentTRAK**.
2. In the **Web Notifications** section, copy the **eAuthorizeDocumentStatusKBA** web notification template and complete the following substeps.
    1. Select **Edit** for the **General Information** section.
    2. In the **Design Name** box, enter a name for the web notification.
    3. In the **Service Endpoint (URL)** box, replace **[Server IP]** with the `http://<Connect Runtime host name>:<port>/ws/SignatureEndpoint` and click **Next**.
    4. Select **Edit Raw XML**and click **Next**.
    5. Verify that the XML is similar to the following example and click **Next**.

        ```
        <?xml version="1.0" encoding="utf-8"?>
        <soapenv:Envelope
            xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
            xmlns:esig="http://www.perceptivesoftware.com/asq/esignature">
        <soapenv:Header/>
        <soapenv:Body>
        <esig:UpdateStatusDocumentKBA>
        <DOC_ORDER_ID>[Order ID]</DOC_ORDER_ID>
        <DOC_SIGNING_STEP>[Signing Step]</DOC_SIGNING_STEP>
        <DOC_STATUS>[Document Status]</DOC_STATUS>
        <SIGNER_AUTH_FAIL_DET>[Signatory Authentication Failure
        Details]</SIGNER_AUTH_FAIL_DET>
        <SIGNER_KBA_DET>[Signatory KBA Result Details]</SIGNER_KBA_DET>
        <SIGNER_KBA_RES>[Signatory KBA Result]</SIGNER_KBA_RES>
        </esig:UpdateStatusDocumentKBA>
        </soapenv:Body>
        </soapenv:Envelope>
        ```

    6. Select **Compare response to expected XML string** and click **Next**.
    7. Select **Edit Raw XML** and click **Next**.
    8. Verify that the XML is similar to the following example, click **Next**, and then click **Finish**.

        ```
        <soap:Envelope
            xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
        <soap:Body>
        <ns2:UpdateStatusDocumentKBAResponse
                    xmlns:ns2="http://www.perceptivesoftware.com/asq/esignature">
        <Return>true</Return>
        </ns2:UpdateStatusDocumentKBAResponse>
        </soap:Body>
        </soap:Envelope>
        ```

Set up an AssureSign template for signature

For details, see the AssureSign Quick Reference Guide for instructions to create a template. However, consider the following points when creating a template.

- Make sure the template name matches the name of the corresponding document type in ImageNow.
- Make sure the Template Tag in AssureSign is same as the value that you provided in the **Configuration** page of **Perceptive Connect Runtime** dashboard.

Add web notifications

In the **Workflow Template**, for **Web Notifications**, add the notifications as shown in the following table.

Note If there are multiple steps (signatories) defined in the template, then each step (Step 1, Step 2, and so on) should have the following assigned design names.

Stage	Timing	Design Name
Document Started	Before Document Started	eAuthorize Document Status
Step 1	Before Step	eAuthorize Step Start
	After Step	eAuthorize Step Complete
	Landing Page Visited	eAuthorize Step User Visit
Document Completed	After Document Completed	eAuthorize Document Completed
Expiration Warning	No notification selected	
Document Expired	After Document Expiration	eAuthorize Document Status
Document Cancelled	Document Cancelled	eAuthorize Document Status
Document Declined	Document Declined	eAuthorize Document Status
Feedback Submitted	No notification selected	
Authentication Failed	Authentication Failed	eAuthorize Document StatusKBA
KBA Started	KBA Started	eAuthorize Document StatusKBA
KBA Completed	KBA Completed	eAuthorize Document StatusKBA

Add dynamic JotBlock in PDF documents

To add dynamic JotBlocks in a PDF document, you have to change the following setting in the AssureSign environment.

1. In **AssureSign**, on the **Administration** tab, on the left pane, click **Settings**.
2. In **Document Preferences**, point to **Flatten PDF Documents Prior to Processing** and click **Edit**.

   Note If you cannot find this setting in **Document Preferences**, contact your administrator to set this preference to **No**.
3. Select the **No** button and click **Save**.

Set up the ability to download signed documents from a third party

Signed documents submitted by a third party automatically upload into ImageNow after the signatory signs them. These documents do not originate in ImageNow. A third party sends them for signature manually or from another application. The system then uploads the documents directly into ImageNow after signing.

You have to create document types and configure templates within the AssureSign environment for document transmission. To complete the following steps, you must have administrative rights to your AssureSign environment.

Create document types to download signed documents submitted by third party applications

To download signed documents in ImageNow, submitted by third-party applications, you have to create a document type that contains AS_AUTH_TOKEN and AS_ID as custom properties. These custom properties are automatically populated when a signed document is downloaded in ImageNow.

1. On the **ImageNow** toolbar, click **Manage**.
2. In **Management Console**, in the left pane, click **Document Types**.
3. In the right pane, click **New** and specify a name for the document type.

   Note The name of the document type must contain the words “AssureSign” and “External”. This is the default document type for document transmission.
4. Select the added document type and click **Modify**.
   1. Under **Custom Properties**, in the **By Type** list, select **String**.
   2. In the **Available** box, select **AS_AUTH_TOKEN** and **AS_ID**,and then click **Add**.
   3. Click **OK**.

Set up AssureSign for document transmission

The steps given below are for the transmission of third-party documents in ImageNow 6.7 or higher.

Complete the following steps to set up the AssureSign environment for document transmission.

1. In **AssureSign**, on the **Administration** tab, open **Notifications** and click **DocumentTRAK**.
2. In **Completed Document Transmission** section, copy the **eAuthorizeExternalDocUpload** document transmission template.
   1. Select **Edit** for the **General Information** section.
   2. In the **Design Name** box, enter a name for the web notification.
   3. In the **Service Endpoint (URL)** box, replace**[Server IP]** with the `http://<Connect Runtime host name>:<port>/ws/SignatureEndpoint` and click **Next.**
   4. Select **EditRawXML** and click **Next**.
   5. Replace the original text in the XML with the following highlighted text by performing the following substeps.
      1. Select the existing text in the code in place of the highlighted text and click the exact parameter name enclosed in brackets in the **Request XML Editing** box.
      2. In the `<field1>`, `<field2>`, `<field3>`, `<field4>`**,** and `<field5>` tags, enter the appropriate index values for the signed document when it comes into ImageNow.

         Note Value for `<field1>` through `<field5>` can be static text (no brackets) or could contain the name of an AssureSign jotblock within brackets ([JotBlockName]). If any field value is empty, the corresponding field in ImageNow appears empty.

3. In the `<documentType>` tag, enter the document type value that you want the signed document to contain.

    ```
    <?xml version="1.0" encoding="utf-8"?>
    <soapenv:Envelope
        xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:esig="http://www.perceptivesoftware.com/asq/esignature">
    <soapenv:Header/>
    <soapenv:Body>
    <esig:UploadSignedDocument>
    <DOC_ID>[Document ID]</DOC_ID>
    <DOC_AUTH_TOKEN>[Document AuthToken]</DOC_AUTH_TOKEN>
    <DOC_ORDER_ID>[Order ID]</DOC_ORDER_ID>
    <drawer>default</drawer>
    <name>[Document Name]</name>
    <field1>[Document Name] Field 1</field1>
    <field2>[Document Name] Field 2</field2>
    <field3>[Document Name] Field 3</field3>
    <field4>[Document Name] Field 4</field4>
    <field5>[Document Name] Field 5</field5>
    <documentType>AssureSign_External_Abhirup</documentType>
    <DOCUMENT>[Completed Document]</DOCUMENT>
    <EXTERNAL_DOCUMENT_QUEUE>SignatureComplete</EXTERNAL_DOCUMENT_QUEUE>
    </esig:UploadSignedDocument>
    </soapenv:Body>
    </soapenv:Envelope>
    ```

    Notes

    - Ensure that the document keys contain unique values for signed documents. This restricts ImageNow from appending a signed third-party document.
    - Provide the queue name for the **EXTERNAL_DOCUMENT_QUEUE** parameter to download the signed document in that queue in ImageNow. The previous example shows the **SignatureComplete** queue.
    - If you do not provide a document name for the name parameter, ImageNow uses the document ID as the default document name.
    - If you do not provide a type for the documentType parameter, the default document type for document transmission is used. For details, see the Create document types to download signed documents submitted by third party applications section of this document.
    - When you use an eForm from ImageNow Forms Server, ensure that document type is not specified as "is a form" for document storage in ImageNow.
    - If you provide a document type, ensure the document type contains **AS_AUTH_TOKEN**and **AS_ID**as the custom properties.

6. Select **Compare response to expected XML string** and click **Next**.
7. Select **Edit Raw XML** and click **Next**.
8. Verify the XML looks like the following example.

```
<soap:Envelope
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body>
<ns2:UploadSignedDocumentResponse
            xmlns:ns2="http://www.perceptivesoftware.com/asq/esignature">
```

```
<Return>true</Return>
</ns2:UploadSignedDocumentResponse>
</soap:Body>
</soap:Envelope>
```

3. Create a template for document transmission. For details,see the AssureSign Quick Reference Guide for instructions to create a template.

   Note Consider the following points when creating the template.

   - In **Workflow Template**, for **Web Notifications**, ensure that no notifications are selected for any of the stages.
   - For **Document Transmission**, select the design name added in this section.

Set up the AssureSign environment for envelopes

This section outlines the steps to set up the AssureSign environment for sending multiple documents in a folder for signature. To see the steps to send multiple documents see the *Perceptive eAuthorize Getting Started Guide*.

Configure DocumentTRAK for the AssureSign envelope template

1. In **AssureSign**, on the **Administration** tab, open **Notifications** and click **DocumentTRAK**.
2. In the **Web Notifications** section, copy the **eAuthorizeEnvelopeAll** web notification template.
   1. Select **Edit** for the **General Information** section.
   2. In the **DesignName** box, enter a name for the web notification.
   3. In the **Service Endpoint (URL)** box, replace **[Server IP]** with the `http://<Connect Runtime host name>:<port>/ws/SignatureEndpoint` and click **Next**.
   4. Select **Edit Raw XML** and click **Next**.
   5. Verify that the XML is similar to the following example and click **Next**.

      ```
      <?xml version="1.0" encoding="utf-8"?>
      <soapenv:Envelope
          xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
          xmlns:esig="http://www.perceptivesoftware.com/asq/esignature">
      <soapenv:Header/>
      <soapenv:Body>
      <esig:UpdateStatusEnvelope>
      <ENVELOPE_AUTH_TOKEN>[Envelope AuthToken]</ENVELOPE_AUTH_TOKEN>
      <ENVELOPE_ID>[Envelope ID]</ENVELOPE_ID>
      </esig:UpdateStatusEnvelope>
      </soapenv:Body>
      </soapenv:Envelope>
      ```

   6. Select **Compare response to expected XML string** and click **Next**.
   7. Select **Edit Raw XML** and click **Next**.
   8. Verify that the XML is similar to the following example, click **Next**,and then click **Finish**.

      ```
      <soap:Envelope
          xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
      <soap:Body>
      <ns2:UpdateStatusEnvelopeResponse
                  xmlns:ns2="http://www.perceptivesoftware.com/asq/esignature">
      ```

```
<Return>true</Return>
</ns2:UpdateStatusEnvelopeResponse>
</soap:Body>
</soap:Envelope>
```

Create an envelope template

Email notifications is assigned within the Envelope Template and disabled within the individual Document Templates that are included as part of the Envelope. Otherwise, instead of receiving one notification for all documents in the envelope, the signatories receive multiple email notifications for the same document.

1. In the **Envelope Templates** section, click **New**.
2. In the **Name** box, enter a name for the envelope template. Ensure that the template name matches the name of the corresponding folder type in ImageNow.
3. In the Tag box in AssureSign, enter a value that matches the value that you provided in the Configuration.xml file. For additional information on the Configuration.xml file, see the Appendix B: Configuration.
4. Select an email design set from the **Email Design Set** list and an **Account** from the **Accessibility** list.
5. Click **Save**.

Edit notifications

1. Click **Edit** in front of the new envelope template.
2. Click **Edit Notifications** and add the notifications as shown in the following table.

Stage	Timing	Design Name
Envelope Started	Envelope Started	eAuthorizeEnvelopeAll
Envelope Completed	Envelope Completed	eAuthorizeEnvelopeAll
Envelope Expired	Envelope Expired	eAuthorizeEnvelopeAll
Envelope Cancelled	Envelope Cancelled	eAuthorizeEnvelopeAll
Envelope Declined	Envelope Declined	eAuthorizeEnvelopeAll

Set up an eForm for Signature from server download location

If you are using an eForm, you do not have to capture the document in ImageNow. The signatory receives the form with a Submit button. After the signatory completes the form and clicks the Submit button, a Begin signing link displays directly within the eForm. When the signatory clicks the Begin signing link within the eForm, the document appears for signing. The eForm data dynamically populates the data on the document. After signing, you can configure the document within the AssureSign template and then automatically upload it into ImageNow.

1. Log into ImageNow with managerial privileges and click **Manage**.
    1. In **Management Console**, in the left pane, click **Forms**.
    2. On the **Forms** tab, click **Open Form Designer** and create a form.

   Note For more information on creating forms using Form Designer, see the *Perceptive Software ImageNow Form Designer Help*.

   3. On the **Forms** tab, click **Manage Form Components**.
   4. On **Presentations**, select the newly created presentation and click **Modify**.
      1. In the left pane, click **Files**.
      2. In the right pane, click **Add**, browse to select **CallAssureSign.js**, and click **OK**.

2. Open the XSL file from the newly created form folder in the **[*drive*:]:\inserver6\form\** directory and complete the following substeps.
   1. Add `<script language="JavaScript" src="CallAssureSign.js"></script>` within the head tag to call AssureSign, as shown in the following example.

      ```
      <?xml version="1.0" encoding="windows-1252"?>
      <xsl:stylesheet version="1.0"
      xmlns:xhtml="http://www.w3.org/1999/xhtml"
      xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
      <xsl:template match="/form">
      <html>
      <head xmlns="http://www.w3.org/1999/xhtml">
             <script language="JavaScript" src="CallAssureSign.js"></script>
      <meta name="generator"
              content="HTML Tidy for Windows (vers 14 February 2006), see
      www.w3.org">
      </meta>
      <title>ImageNow Forms</title>
      <meta name="GENERATOR" content="MSHTML 9.00.8112.16455">
      </meta>
      <meta name="GENERATOR" content="MSHTML 9.00.8112.16455">
      </meta>
      <meta name="GENERATOR" content="MSHTML 9.00.8112.16455">
      </meta>
      <meta content="text/html; charset=us-ascii"
              http-equiv="Content-Type"></meta>
      <meta name="GENERATOR" content="MSHTML 9.00.8112.16455">
      </meta>
      </head>
      ```

   2. Add `<input type="button" value="Submit" onclick="getImmediatePresentmentLink()" />` and `<p id="SigningLink"></p>` within a body tag to place the **Submit** button and the **Begin signing** link in the form body, as shown in the following example.

      ```
      <input type="button" value="Submit" onclick="getImmediatePresentmentLink()" />
      <p id="SigningLink"></p>
      </body>
      </html>
      </xsl:template>
      </xsl:stylesheet>
      ```

3. In the installed PCR directory, navigate to **conf** directory and open **config.properties** file.
4. Make the following entries in the **config.properties** file under the section **Cross Origin Resource Sharing**.

```
##############################
# Cross Origin Resource Sharing
##############################
connect.rs.cors.enabled=true
```

```
connect.rs.cors.allow.all.origins=true
connect.rs.cors.allow.credentials=false
connect.rs.cors.allowed.origins=*
```

5. You must modify the CallAssureSign.js file. The following URL in the CallAssureSign.js must point to the eForm service running as an eAuthorize component on PCR.
   - xmlHTTP.open("POST", "http://<Connect Runtime host>:<port>/rs/SignatureEndpoint/SubmitToAssureSign", true)

Configure CallAssureSign.js to work with manually designed eForms

Manually designed eForms are eForms that are created using utilities other than the eForm designer utility of ImageNow. If you design the eForm manually, you need to make some changes in the CallAssureSign.js script so that it can recognize the inputs and associated value to construct the URL encoded request parameters.The following example displays the Java script template that you must modify to work with a manually created eForm.

```
function getImmediatePresentmentLink() {
    var allElements = document.all;
    for (var i = 0; i < allElements.length; i++) {
        allElements[i].setAttribute("disabled", true);
    }
    var winLoc = window.location.href;
    var tempStr = winLoc.substring(winLoc.lastIndexOf("/"), winLoc.lastIndexOf("."));
    var formName = tempStr.substring(tempStr.indexOf("_") + 1);

    document.getElementById("SigningLink").innerHTML = 'Please wait....The document
isbeing submitted....Your signing link will appear here shortly';
    var strRequest = "ImageNowFormName=" + formName;
    var row = document.getElementsByTagName("tr");
    for (i = 0; i < row.length; i++) {
        var currentItem = row.item(i);
        if (currentItem.childNodes.length < 2) {
            continue;
        }
        var field = currentItem.childNodes.item(0).innerText;
        var dataItem = currentItem.childNodes.item(1).childNodes.item(0);
        var value;
        if (dataItem.nodeName.toUpperCase() == "INPUT") {
            value = dataItem.value;
        }
        if (dataItem.nodeName.toUpperCase() == "SELECT") {
            var selectedIndex = dataItem.selectedIndex;
            value = dataItem.getElementsByTagName("option")[selectedIndex].innerText;
        }
        strRequest = strRequest + "&" + field + "=" + value;
    }

    var xmlHTTP;
    if (window.XMLHttpRequest) {
        xmlHTTP = new window.XMLHttpRequest;
    }
    else {
        try {
            xmlHTTP = new ActiveXObject("MSXML2.XMLHTTP.3.0");
        }
        catch (ex) {
        }
    }
    xmlHTTP.open("POST", "http://<Connect Runtime
host>:<port>/rs/SignatureEndpoint/SubmitToAssureSign", true);
    xmlHTTP.setRequestHeader("Content-Type", "application/x-www-form-
urlencoded;charset=utf-8");
    xmlHTTP.onreadystatechange = function () {
        if (xmlHTTP.readyState == 4 && xmlHTTP.status == 200) {
            document.getElementById("SigningLink").innerHTML = '<a href="' +
xmlHTTP.responseText + '" target="_blank">' + 'Begin Signing' + '</a>';
            /* window.open(xmlHTTP.responseText);*/
        }
    }
    xmlHTTP.send(strRequest);
}
```

You can make the following changes in the CallAssureSign.js script to make it work with your manually designed eform.

- In the line `for (i = 0; i < row.length; i++)`, establish the iteration mechanism to implement proper traversal for your eForm.
- In the `var field = currentItem.childNodes.item(0).innerText;` line, under the `field` variable, assign the variable name of AssureSign parameter.
- In `the var dataItem = currentItem.childNodes.item(1).childNodes.item(0);` line, under the `dataItem` variable, assign the value of the AssureSign parameter that is identified in the `field` variable.

The strRequest = strRequest + "&" + field + "=" + value; line is eForm specific. This line denotes the relationship between AssureSign parameter names and associated values. The strRequest variable must be of the format ImageNowFormName=<Name of the ImageNow form>&parameter1=value1&parameter2 =value2 and so on, where parameter1 and parameter2 are AssureSign parameters and value1 and value2 are associated values.

The following URL in the above code snippet must point to the eForm service running as an eAuthorize component on PCR.

```
xmlHTTP.open("POST", "http://<Connect Runtime
host>:<port>/rs/SignatureEndpoint/SubmitToAssureSign", true)
```

Disable the Begin signing link

To disable the immediate presentment link, complete the following steps.

1. In the XSL file, delete `<p id="SigningLink"></p>`in the body tag.
2. In the **CallAssureSign.js**, delete the following lines.

```
document.getElementById("SigningLink").innerHTML = 'Please wait....The document is
being submitted....Your signing link will appear here shortly';
and
   xmlHTTP.onreadystatechange = function () {
        if (xmlHTTP.readyState == 4 && xmlHTTP.status == 200) {
            document.getElementById("SigningLink").innerHTML = '<a href="' +
xmlHTTP.responseText + '" target="_blank">' + 'Begin Signing' + '</a>';
            /* window.open(xmlHTTP.responseText);*/
        }
    }
```

3. Restart **Tomcat** containing the forms server.

Disable buttons on eForms

ImageNow Forms Server provides the option to disable the save, print, reset, and attachments buttons.

1. Access the **[*drive*:]\inserver\etc** directory and open the imagenowforms.xml file.
2. Go to the section where the `<FormName>` tag value is the name of the form you are using to sign.
3. Within `<ConfigParams>`, add the configuration parameters and set the values as FALSE for the buttons which you want to disable, as shown in the following example.

```
<DocumentForm>
    <FormName>eAuthorize_eForm</FormName>
    <QueueName></QueueName>
    <Drawer>Accounts Payable</Drawer>
    <Field1 isUnique="true"/>
    <Field2 isTimeStamp="true"/>
    <Field3/>
    <Field4/>
    <Field5/>
<ConfigParams>
<ConfigParam name=”saveVisible” value=”FALSE”/>
<ConfigParam name=”printVisible” value=”FALSE”/>
<ConfigParam name=”resetVisible” value=”FALSE”/>
   <ConfigParam name=”attachmetnsVisible” value=”FALSE”/>
</ConfigParams>
</DocumentForm>
```

4. Stop the **Engine** service and then restart **Tomcat**. Now all the buttons are invisible.

   Note If you save the attachments in ImageNow, you cannot submit them along with the signed document. As in this case, where you are not saving the form to ImageNow and are only collecting values from the eForm, you cannot submit attachments.

Map eForm fields to JotBlocks in AssureSign

To map the fields in forms with the parameters in JotBlock, consider the following points while creating eForms for submitting documents for signature.

- Create a document template in AssureSign matching the name of the form used for signature.
- JotBlocks should have **Type** as **Text**, **Input** as **Parameter** and the parameter name should match the field names in the form.
- **Workflow** template in AssureSign should contain the **Signatory Name** and **Email Address** matching those in the form.
- AssureSign treats the documents submitted for signature though eForm as third party documents. Hence, while creating **Workflow** template, on **Document Transmission**, select **eAuthorizeExternalDocUpload** as the **Design Name**.

Note The sample CallAssureSign.js provided with the installer is not an universal one. You may need to modify it in accordance with the form inputs.

Issues and workaround

Troubleshoot if bundles and components are not in Active state

Issue: All Bundles and Components mentioned in Verify the connector JAR bundle status section are not active.

Solution: This situation can occur if the connectors or related dependencies are either not installed or configured correctly in the Perceptive Connect Runtime. To solve this issue, perform the following steps.

1. Navigate to **Perceptive Connect Runtime** dashboard.
2. Configure and check that the configuration mentioned in the **Configure the Content Connector** section is correct and the bundles or components related to the Content Connector are in Active state.
3. In the **Perceptive Connect Runtime** dashboard, configure and check that the configuration mentioned in the **Configure the app inPerceptive Connect Runtime** is correct.
4. Restart the **Perceptive Connect Runtime** service.

Troubleshoot if the WSDL does not show the operations during Envoy creation

Issue: While configuring Envoy, the WSDL at `http://<Connect Runtime host>:<port>/ws/SignatureEndpoint?wsdl` does not show the relevant operations in the XML that appears.

Solution: This situation occurs if the connectors are not installed or configured correctly in Perceptive Connect Runtime. To solve this issue, perform the following steps.

1. Navigate to **Perceptive Connect Runtime** dashboard.
2. Configure and check that the configuration mentioned in the **Configure the app inPerceptive Connect Runtime** is correct.
3. In **Perceptive Connect Runtime** dashboard, check that all the bundles and components mentioned in the Verify the connector JAR bundle status section are in Active status.
4. Restart the **Perceptive Connect Runtime** service.

Troubleshoot if AssureSign is unable to send notifications to eAuthorize

Issue: AssureSign is unable to send notifications to eAuthorize

Solution: This situation occurs if the notifications configured in AssureSign are incorrect. To solve this issue, perform the following steps.

1. Navigate to **AssureSign** administration page and check the following
    - If the notifications point to the correct Perceptive Connect Runtime service
    - If the Request XML and Response XML of the notifications are correct as per **Set up the AssureSign environment** section.

Troubleshoot if there is Perceptive Connect Runtime startup failure

Issue: If Integration Server and ImageNow Forms Server are installed on the same Tomcat server, and one of the servers may fail to start causing Perceptive Connect Runtime startup failure.

Solution:

1. Cut **encryption.jar** from the **Tomcat\webapps\integrationserver\WEB-INF\lib** directory and paste to the **tomcat\webapps\shared** folder. Create the directory if it does not exist.
2. Open the **Tomcat\conf\catalina.properties** file and edit the shared.loader setting to **catalina_home\webapps\shared**.

Troubleshoot if Template ID is missing during eAuthorize document submission

Issue: The eAuthorize document submission fails and error logs display a message.

Solution: This error occurs if the AssureSign template is not properly configured. When you submit a document in ImageNow, the Document Type name in ImageNow must match with an AssureSign template name. The name match is case-sensitive. To know how to set up an AssureSign template, see the Set up an AssureSign template for signature section.

Troubleshoot if there is an installation issue after running the installer

Issue: After running the installer, installation issue may arise due to some reason.

Solution: If there is an installation problem, it is recommended that you must verify all the manual installation steps. For details, see the Install eAuthorize manually section.

Troubleshoot eForm

Issue: There may be an issue with the eForm.

Solution: If there is an issue with the eForm, complete the following steps.

1. Open the browser debug console and ensure that the **CallAsssureSign.js** file is properly loaded.

Note If there is an error during loading the script file, ensure that the script file **.js** is included in the Presentation files list.

2. Restart the application server where the Forms server is hosted.
3. Add `console.log(strRequest)`in the script file after the entire request string is generated.
4. Save the script and refresh the browser to reload the form.
5. Enter the values in the input fields and click **Submit**.
6. Open the browser debug console and check the value of the strRequest variable appearing in the console which must be in the format `ImageNowFormName=<Name of the ImageNow form>&parameter1=value1&parameter2=value2.`

Note Ensure that there is no unnecessary space or unwanted charactersin the query parameter names. You must have a template with the same name as the eForm name configured in the AssureSign server and associated with a correct document transmission that points to the appropriate PCR server.

Appendix A: About the eAuthorize ImageNow configuration

The eAuthorize solution uses various products for the signing and storage of documents. This section of the installation guide describes the ImageNow configuration provided with the installer. After you run the installation wizard using the Complete setup type or the Workflow Configuration option in the Custom setup type, the installer creates the storage and workflow needed by eAuthorize on your ImageNow system.

This appendix provides details about the ImageNow configuration that is automatically set up by the installation wizard.

Custom properties

The following table provides the list of custom properties that the installation wizard creates during installation.

Custom Property Name	Description	Parameter Type	Data Type
AS_AUTH_TOKEN	Unique security token from AssureSign	Output parameter	String
AS_FAILURE_NOTIFICATION_TYPE	Type of notification sent to the user when a document fails in workflow	Input parameter	List
AS_ID	Unique ID from AssureSign	Output parameter	String
AS_KEEP_ORIGINAL_DOCUMENT	If this is set as TRUE, the original document remains as is in the DocumentStore work queue in ImageNow workflow and a copy of it is created.	Input parameter	Flag
AS_SIGNATURE_STATUS	Status of the signature in workflow	Output parameter	String
Signatory 1 Full Name	Name of the person who needs to sign the document	Input parameter	String
Signatory 1 Email Address	Email address of the person who needs to sign the document	Input parameter	String
Signatory 2 Full Name	Name of the person who needs to sign the document	Input parameter	String
Signatory 2 Email Address	Email address of the person who needs to sign the document	Input parameter	String
Signatory 3 Full Name	Name of the person who needs to sign the document	Input parameter	String

Custom Property Name	Description	Parameter Type	Data Type
Signatory 3 Email Address	Email address of the person who needs to sign the document	Input parameter	String

It is important to understand how these custom properties function.

- Signatory 1 Full Name and Signatory 1 Email Address are the input parameters for AssureSign Connector that you must provide.
- AS_ ID, AS_AUTH_TOKEN, and AS_SIGNATURE_STATUS are the output parameters for AssureSign Connector that populate automatically.
- Various actions occur, depending on the value you set for AS_FAILURE_NOTIFICATION_TYPE:
  - **Email**. If the document fails in the workflow, an email is sent to the email ID that you configured in ImageNow while creating user profiles. You must provide the SMTP server name, port, email ID in the **Configuration** page of **Perceptive Connect Runtime** dashboard, and the authentication if needed.
  - **Task**. You receive a task in the My Assigned view in ImageNow that shows that the document failed in workflow.
  - **Both**. You receive an email in your email account and a task in ImageNow.

About custom properties for extended features

To send a document to multiple signatories, you need the signatory full name and signatory email address custom properties corresponding to each signatory. During installation, the following custom properties are automatically created for sending a document to additional signatories.

- Signatory 2 Full Name
- Signatory 2 Email Address
- Signatory 3 Full Name
- Signatory 3 Email Address

When you create the multiple signatories, you must understand how the information correlates to the AssureSign template and ImageNow custom properties.

- You specify the signatory names and email addresses while creating a template in AssureSign.
- You must make sure that the custom properties for signatory full name and signatory email address in ImageNow match the AssureSign template. For example, if you use Signatory 1 Full Name and Signatory 1 Email Address in a particular template, make sure that ImageNow uses the same Signatory 1 Full Name and Signatory 1 Email Address custom properties.

Note Additional custom properties can be used to prefill information on an AssureSign document if the name of AssureSign template parameter and the names of custom property are same.

For details, see the AssureSign Quick Reference Guide for instructions on creating a template. Ensure that each name and email address corresponds to custom properties in ImageNow.

Task templates

The eAuthorize installation wizard automatically creates pointer task templates, reasons, and reason lists. The installation wizard also populates the reason lists with the corresponding reason member and associates the appropriate action reasons and return reasons with each task template. The following table shows these correlations.

Task Name	Action Reason List	Action Reason List Members	Return Reason List	Return Reason List Members
FailureNotification_Cancelled	Cancelled	Document/Envelope is cancelled by signatory.	Task Return List	Additional information requested. Not my document. Not my folder. Not completed as required. See comments for more information.
FailureNotification_Declined	Declined	Document/Envelope is declined by signatory.	Task Return List	Additional information requested. Not my document. Not my folder. Not completed as required. See comments for more information.
FailureNotification_DownloadFailed	DownloadFailed	Document/Envelope download failed.	Task Return List	Additional information requested. Not my document. Not my folder. Not completed as required. See comments for more information.
FailureNotification_Expired	Expired	Document/Envelope is expired.	Task Return List	Additional information requested. Not my document. Not my folder. Not completed as required. See comments for more information.
FailureNotification_SubmissionFailed	Submission Failed	Document/Envelope submission failed.	Task Return List	Additional information requested. Not my document. Not my folder. Not completed as required. See comments for more information.

eAuthorize iScripts

The installation wizard places the following iScripts in the [*drive*:]\inserver6\script directory during installation.

Script	Function
CreateTask.js	For creating a task in ImageNow if a document fails in workflow.
DocumentStoreAndForward.js	For storing and forwarding a document in a workflow queue.
RefreshAuditHistory.js	For refreshing Audit History.

The installation wizard places the following files in the [*drive*:]\inserver6\script\eAuthorize directory during installation.

- IN_WorksheetManager.jsh
- IN_XML.jsh
- INBasePath.jsh
- Util_Misc.jsh

AssureSign forms

A Forms license is required to use forms in eAuthorize. If you need a Forms license, contact your Perceptive Software representative.

AssureSign Audit History form

This form displays the audit trail of each document processed in eAuthorize. If the form license is not activated, the audit trail history will not be available in ImageNow but will be available in AssureSign.

About the AssureSign Audit History form files and components

The eAuthorize installation wizard automatically creates the AssureSign Audit History form for you. You create a form by first uploading the data definition file and then the XSL style sheet and supporting files. The eAuthorize installation wizard automatically loads these files to the [*drive*:]\inserver6\forms directory and configures the corresponding ImageNow components. To create it manually, see the Set up eForm for AssureSign Audit History section.

File name	Purpose
AssureSign_AuditHistory.xml	The data definition XML file contains the schema used to save data instances in data content record files.
AssureSign_Audit_History_Presentation.xsl	The presentation XSL file describes how to present the XML data in the form.

File name	Purpose
Supporting files	The supporting files for the presentation. • AssureSign_AuditHistory.xls • Asynch.js • Forms.css • Refresh_16.png • Section_header_bg.gif

AssureSign ImmediatePresentment form

This form provides you the link to sign the associated documents from within ImageNow client. If the form license is not activated, the AssureSign ImmediatePresentment form is not available in ImageNow.

About AssureSign ImmediatePresentment form files and components

The eAuthorize installation wizard automatically creates the AssureSign ImmediatePresentment form for you. You create a form by first uploading the data definition file and then the XSL style sheet and supporting files. The eAuthorize installation wizard automatically loads these files to the [*drive:*]\inserver6\forms directory and configures the corresponding ImageNow components. To create this manually, see the Set up eForm for AssureSign ImmediatePresentment.

File name	**Purpose**
AssureSign_ImmediatePresentment.xml	The data definition XML file contains the schema used to save data instances in data content record files.
AssureSign_ImmediatePresentment.xsl	The presentation XSL file describes how to present the XML data in the form.
Supporting files	The supporting files for the presentation. • Forms.css • Forms.js • section_header_bg.gif

About the workflow for sending documents for signature

A workflow process is required to send documents to AssureSign for signature and download the signed documents in ImageNow. The installer automatically configures workflow configurations.

The eAuthorize installation wizard creates a workflow process and the queues described in the following table.

Queue Name	Description
SubmitForSignature	ASQ for submitting a document for signature. This is the first queue in the workflow process.
DocumentStore	When AS_KEEP_ORIGINAL_DOCUMENT is TRUE, the original document remains as is in this work queue, a copy of it is created in ImageNow, and through sequential auto-routing it is forwarded to the SendToAssureSign ASQ.
SendToAssureSign	When the document is submitted to AssureSign for signature.
SignatureRequested	When the email notification from AssureSign is sent to signatory.
DocumentProgress	When the signing process is in progress.
DownloadSignedDocuments	ASQ where the signed document is routed for downloading in ImageNow.
SignatureComplete	Work queue where the document is routed when the required signature is obtained.
SignatureFailure	Cancelled, expired, declined, or format mismatched documents are routed to this queue.

Appendix B: Configuration

The following table provides definitions and instructions for setting the parameter values in the Configuration page of Perceptive Connect Runtime dashboard.

Section	Parameter	Guideline
AssureSign parameters configuration	WSDL_URL	A URL that defines the location of the sandbox or production instance in the AssureSign cloud, or a URL to the local AssureSign web application you are using.
	Local domain name	Keep the field blank if you are using an instance of the AssureSign cloud, for example: <parameter name= "AS_LOCAL_INSTANCE_DOMAIN_NAME"value=""/ > If you are using a local AssureSign web application, provide the machine name as the value. You can also find the machine name in self-signed certificate issued during AssureSign installation.
	User name	An AssureSign administrative account that is used to authenticate into AssureSign and submit documents for signature.
	Context ID	AssureSign's DocumentNOW Account Context Identifier specifies a unique identifier needed in order to validate the request. You can find this identifier in the **Settings** section of the Administrative tab within your AssureSign environment, if you have administrative access.
	Template tag	This value needs to match the Template tag value in the AssureSign template. Use the value that you have already entered in AssureSign, or note this value so that you can enter it in AssureSign as the Template Tag. For details, see the AssureSign Quick Reference Guide for instructions to create a template.
Email parameters configuration	SMTP server name	The name of the SMTP server that sends email notifications.
	SMTP server port	The port of the SMTP server that sends email notifications.
	SMTP sender email ID	The email ID configured on the SMTP server that sends email notifications.
	SMTP Authentication	If your SMTP email server requires authentication, provide the value as 'true'; otherwise, use "false".

Section	Parameter	Guideline
	Authentication user name	If your SMTP email server requires authentication, provide a username for the email server.
	Authentication password	If your SMTP email server requires authentication, provide the password corresponding to above-mentioned username for the email server.

Appendix C: Copy web notification templates

If you are using a local instance of the AssureSign environment, complete the following steps to copy the web notification templates from the sandbox environment.

1. In a browser window, sign into the **AssureSign sandbox environment**.
2. In another browser window, sign into your **AssureSign local environment**.
3. In the **sandbox** environment, on the **Administration** tab, click **DocumentTRAK**.
4. In your **local** environment, on the **Administration** tab, click **DocumentTRAK**.
5. In the **sandbox** environment, in the **Web Notifications** table, locate the design you want to copy and click **Copy**.
6. In your **local** environment, in the heading row of the **Web Notifications** table, click **New**.
7. In the **sandbox** environment, copy the values from the **Design Summary** page to the **General Information** window in your local environment.
8. In your **local** environment, in the **General Information** page, click **Next**.
9. Copy the request XML from the sandbox environment.
    1. In the **sandbox** environment, in the **Design Summary** page, in the **Request XML** section, click **Edit**.
    2. In the **Request Message XML** page, ensure **Edit Raw XML** is selected and click **Next**.
    3. In the **Request XML Editing** page, copy the XML.
    4. Click **Next**.
    5. In your **local** environment, in the **Request Message XML** page, ensure **Paste Raw XML** is selected and click **Next**.
    6. In the **Request XML Editing** page, paste the XML.
    7. Click **Next**.
10. Copy the response validation method from the sandbox environment.
    1. In the **sandbox** environment, in the **Design Summary** page, in the **Response Validation** section, click **Edit**, and note the response validation method.
    2. In your **local** environment, in the **Response Validation Method** page, select the same value from the sandbox environment.
    3. Click **Next** and then click **Finish**.
11. Repeat the above steps for each required template.

Index