Perceptive eAuthorize

Installation and Setup Guide

Version 1.1
Compatible with ImageNow versions 6.5.x to 6.7.x

perceptivesoftware

Written by: Product Documentation, R&D
Date: September 2016

Table of Contents

About Perceptive eAuthorize **5**

Requirements **5**

Software prerequisites 5

License 6

Configure eAuthorize for ImageNow 6.5.1 or 6.6 .... **6**

Set up DocumentTRAK for document transmission 6

Set up ImageNow access *6*

Set up ImageNow upload *7*

Set up ImageNow workflow *7*

Install and configure eAuthorize for ImageNow 6.7 or higher **8**

Install Perceptive Platform Integration Engine 8

Install eAuthorize 8

Download the eAuthorize files *9*

Run the eAuthorize installer *9*

Set up the Envoy services *12*

Set up ImageNow for signing 13

Create document types and assign custom properties *14*

Configure task templates for document notification *14*

Create a folder type to send multiple documents for signing *16*

Set up the AssureSign environment **16**

Set up AssureSign DocumentTRAK for status notifications 16

eAuthorizeDocumentStatus *16*

eAuthorizeStepStart *17*

eAuthorizeStepComplete *18*

eAuthorizeStepUserVisit *19*

eAuthorizeDocumentCompleted *19*

Set up an AssureSign template for signature 21

Add web notifications 21

Add dynamic JotBlock in PDF documents 22

Set up the ability to download signed documents from a third party **22**

Create document types to download signed documents submitted by third party applications 22

Set up AssureSign for document transmission 22

Set up the AssureSign environment for envelopes **24**

Configure DocumentTRAK for the AssureSign envelope template 24
Create an envelope template 25
Edit notifications 25
Set up an eForm for Signature 26
Disable the Begin signing link 28
Disable buttons on eForms 28
Map eForm fields to JotBlocks in AssureSign 29
Troubleshooting 29
Appendix A: About the eAuthorize ImageNow configuration 30
Custom properties 30
About custom properties for multiple signatories 31
Task templates 32
eAuthorize iScripts 33
AssureSign Audit History form 33
Set the refresh time for the Audit History form 34
About the workflow for sending documents for signature 34
Appendix B: Configuration.xml file table 36
Appendix C: Copy web notification templates 38
Index 39

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 who's signature is 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 (for ImageNow, version 6.7 or higher).

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, refer to the *Perceptive eAuthorize Getting Started Guide*.

Requirements

Software prerequisites

For ImageNow, version 6.6 or lower, before you run the eAuthorize solution, ensure that your system meets the following prerequisites.

- ImageNow Client and ImageNow Server are installed and running properly.
- You can log into an ImageNow user account with managerial privileges.
- Message Agent is installed and running properly.
- Download Microsoft .NET Framework 4.0 from http://www.microsoft.com/en-us/download/details.aspx?id=17851.
- 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

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

- ImageNow Client and ImageNow Server are installed and running properly.
- You can log into an ImageNow user account with manager privileges.
- Tomcat, version 7.0 or higher, is installed with host manager and apps manager.

  Note Tomcat must be installed on an HTTP server, not an HTTPS server.
- Perceptive Integration Server is installed and running properly.
- 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
- Platform Integration Engine is installed and running on a system that has public Internet Protocol address (IP).

License

If you are using ImageNow, version 6.7 or higher, you are required to have the ImageNow eAuthorize license.

Configure eAuthorize for ImageNow 6.5.1 or 6.6

If you are using ImageNow, version 6.5.1 or 6.6, complete the steps in this section to configure eAuthorize for post-signature integration. Note that this functionality provides a subset of the eAuthorize features and functionality that are available with ImageNow, version 6.7.

Set up DocumentTRAK for document transmission

Use the following built-in web notifications in AssureSign to set up DocumentTRAK for document submission using third-party applications. If you are using a local instance of the AssureSign environment, refer to Appendix C: Copy web notification templates for information on copying AssureSign web notification templates from the sandbox environment.

Perform the procedures in this section to set up the following items.

- **ImageNow access**. Authenticate with Message Agent to establish a session.
- **ImageNow upload**. Upload a signed document to ImageNow.
- **ImageNow workflow**. Route the stored document to an ImageNow workflow queue.

Set up ImageNow access

1. In AssureSign, under **Administration**, expand **Notifications** and click **DocumentTRAK**.

2. Under **Web Notifications**, click **Copy** in front of **ImageNow Access** in the **Name** column.
    1. On the **Design Summary** page, in the **General Information** section, click **Edit**.
    2. In the **Service Endpoint (URL)** box, replace **[TODO: Server IP]** with the IP of the server on which Message Agent is running, and click **Next** until the **Finish** button displays.

        Note The port provided is 6070, which is the default port for Message Agent. If you change your Message Agent port, change 6070 accordingly.
    3. Click **Finish**.

Set up ImageNow upload

1. Under **Web Notifications**, click **Copy** in front of **ImageNow Upload** in the **Name** column.
    1. On the **Design Summary** page, in the **General Information** section, click **Edit**.
    2. In the **Service Endpoint (URL)** box, replace **[TODO: Server IP]** with the IP of the server on which Message Agent is running.

        Note The port provided is 6070, which is the default port for Message Agent. If you change your Message Agent port, change 6070 accordingly.
    3. In the **Design Used for Authentication** list, select **ImageNow Access** and click **Next**.
    4. Select **Edit Raw XML** and click **Next**.
    5. Edit the values for the parameters in the XML to set the index values for the signed documents as required and click **Next** until the **Finish** button displays.
    6. Click **Finish**.

Set up ImageNow workflow

1. Under **Web Notifications**, click copy in front of **ImageNow Workflow** in the **Name** column.
    1. On the **Design Summary** page, in the click **General Information** section, click **Edit**.
    2. In the **Service Endpoint (URL)** box, replace **[TODO: Server IP]** with the IP address of the server on which Message Agent is running.

        Note The port provided is 6070, which is the default port for Message Agent. If you change your Message Agent port, change 6070 accordingly.
    3. In the **Design Used for Authentication** list, select **ImageNow Upload** and click **Next**.
    4. Select **Edit Raw XML** and click **Next**.
    5. Edit the values for the parameters in the XML as required and click **Next** until the **Finish** button displays.

        Note The index values for this notification must be the same as those defined in the **ImageNow Upload** web notification in order for the same document to be routed to a workflow queue. You define the workflow queue name within the WORKFLOW_Q_NAME text tags for the signed document to route to this queue.
    6. Click **Finish**.
2. In **AssureSign**, under **Administration**, click **Settings**.
    1. Under **Notification Preferences**, click **Edit** in front of **DocumentTRAK Credential**.

2. Enter the username and password of an ImageNow account to communicate with ImageNow Server using Message Agent.

3. In **AssureSign**, under **Templates**, click **New** and create a template for document submission using third-party applications. Refer to the AssureSign Quick Reference Guide for instructions to create a template.

   Note Consider the following points when creating the template.

   - In **Workflow Template**, under **Web Notifications**, for **Document Completed** stage, select either **ImageNow Upload** or **ImageNow Workflow**.
   - Use this template to submit a document for signature using a third-party application or when manually uploading them directly to AssureSign.

Install and configure eAuthorize for ImageNow 6.7 or higher

If you are using ImageNow, version 6.7 or higher, install Perceptive Platform Integration Engine and then install eAuthorize using the installation wizard. During this installation, you perform the following procedures.

1. Install Perceptive Platform Integration Engine
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

Install Perceptive Platform Integration Engine

Perceptive Platform Integration Engine is required to install eAuthorize. To install Platform Integration Engine, complete the following steps.

Before you start, verify that Apache Tomcat is already installed and running on the target machine. You can change the server configuration to match your environment.

1. Extract the **Engine.war** file from **PIE+ImageNowServices.zip**.
2. Open a browser, go to **http://<tomcatservername>:<tomcatserverport>/**, and click **Manager App**.
3. Log in with your credentials.
4. In the **Tomcat Web Application Manager** page, scroll to the **Deploy** section.
5. Under **WAR file to deploy**, click **Browse** to locate the **Engine.war** file, and then click **Deploy**.
6. Under the **Applications** section, verify that the **Engine** service is running, and in the **[*drive*:]\IntegrationEngine** directory, that the **etc**, **lib**, **log**, and **Modules** subdirectories exist.

Install eAuthorize

When you run the eAuthorize installation wizard, you can choose from two installation options: complete and custom. For a complete installation, the wizard installs all of the required components on the same computer. For a custom installation, ensure that you have already installed the required software for each installation option according to the following table. Regardless of the option, all components are required for eAuthorize to function correctly.

Typically, you select the custom installation to set up this installation on two machines:

- On the machine running Tomcat and Platform Integration Engine, you can install the Framework Configuration option.
- On a separate machine running ImageNow Server, you can install the other options (Perceptive Configuration and Workflow Configuration).

Note Install the Framework Configuration option first, and then the Perceptive Configuration and Workflow Configuration options. You must specify the IP address of your web application server during the installation steps of the Perceptive Configuration and Workflow Configuration options.

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
Workflow Configuration	Creates a sample workflow and document types. Install Workflow Configuration on the same machine as ImageNow Server.	• ImageNow Server
Framework Configuration	Installs all files required for Perceptive Integration Engine. Install Perceptive Framework on the same machine as Perceptive Integration Engine.	• Tomcat • Platform Integration Engine

Download the eAuthorize files

1. Go to the Perceptive Software website at www.perceptivesoftware.com and log into the Customer Portal.
2. In the **Product Downloads** page, search for all downloadable items for the specific product and version you want to use, including 32-bit or 64-bit.
3. Download the relevant files to a temporary directory on your computer and then unzip the files as needed.

Run the eAuthorize installer

1. Log out of ImageNow.
2. Stop the Apache Tomcat web service.
3. Run the eAuthorize setup executable.
4. In the **Welcome** page, click **Next**.
5. 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**.

6. In the **Setup Type** page, select one of the following installation options.
   - **Complete**. Select **Complete** if Tomcat with Platform Integration Engine and ImageNow Server are installed on the same machine. Click **Next** and continue to the next step.
   - **Custom**. Select **Custom** if Tomcat with Platform Integration Engine and ImageNow Server are installed on different machines. This allows you to define the location. For further details, refer to the Install eAuthorize section. Click **Next** and perform the following substeps.

     1. Select from the following features to make the corresponding configuration changes. Note that you can install Perceptive Configuration independently, but Workflow Configuration requires Perceptive Configuration to already be installed or to be installed at the same time.
        - **Perceptive Configuration** creates a customized Perceptive environment on ImageNow Server, including an Envoy service, custom properties, a reason list, reasons, tasks, and the audit history form required for eAuthorize.
        - **Workflow Configuration** creates the signature workflow and document types on ImageNow Server.
        - **Framework Configuration** deploys the required JAR files and connector for Platform Integration Engine.
     2. Click **Next**.
7. In the **Destination Folder** page, select the root Tomcat folder: **[*drive:*]\Program Files\Apache\Tomcat 7.0** or click **Change** to select a different directory, and click **Next**. If you select a different directory, it must be a valid Tomcat directory.
8. 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 example.

     ```
     [Site Root]/Documents/Services/DocumentNow/v2/DocumentNow.svc?wsdl
     ```

     where **[Site Root]** is one of the following values:
     - AssureSign sandbox: `https://sb.assuresign.net`
     - AssureSign production: `https://na1.assuresign.net`
     - AssureSign local: The machine name 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 creating a template in AssureSign. Refer to the AssureSign Quick Reference Guide for instructions to create a template and the template tag.

  Important The installer assigns the value you enter to the AS_TEMPLATE_TAG parameter in the configuration.xml file located in the [*drive*:]\IntegrationEngine\etc directory. If the template tag value in the configuration.xml file doesn't match the template tag value in the AssureSign template, documents fail when they are submitted for signature.

9. Click **Next**.
10. In the **SMTP Information** page, provide the following information if you want to notify an email address if a document fails. Otherwise, you can leave the information on this page blank.
    - 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, then in the **User ID** box, provide a user name for the email server.
      - If your SMTP email server requires authentication, then in the **Password** box, provide the password corresponding to the user name you entered for the email server.
11. Click **Next**.
12. In the **Integration Server Information** page, provide the following information to properly configure ImageNow Server.
    - In the **Integration Server URL** box, type the URL of Perceptive Integration Server. For example:

      ```
      http://<tomcatservername>:<tomcatportnumber>/integrationserver
      ```
    - In the **Integration Server User ID** box, type the ImageNow user name that Integration Server uses to allow communication between the AssureSign service and ImageNow Server.
    - In the **Integration Server Password** box, type the password for the machine on which Perceptive Integration Server is installed.
13. Click **Next**.
14. In the **Tomcat Information** page, provide the information for your Tomcat web server.
    - In the **Tomcat IP** box, type the IP address or DNS name of the machine where Tomcat and Platform Integration Engine are located.
    - In the **Port** box, type the Tomcat port of the machine where Tomcat and Perceptive Platform Integration Engine are located.
15. In the **Ready to Install** page, click **Install**.
16. **Important** When the installer displays a message to ensure that your web application server is started, start your Apache Tomcat web service and then click **OK**.

17. **Important** When the installer displays a message to stop and start your web application server, stop and then restart your Apache Tomcat web service and then click **OK**.

    Note If the installation wizard displays the following message, complete the steps in the Set up the Envoy services after completing the installation wizard. If you do not receive this message, after completing the installation wizard, continue to the Set up ImageNow for signing section.

    > "The Engine service was unable to be initialized. Some ImageNow configurations will need to be created manually after installation is complete. Refer to the installation guide for more information."

    If the installer displays this message, you will also need to complete the `<AssureSignConnector>` section of the Configuration.xml file. Refer to Appendix B: Configuration.xml file table for more information.

18. In the **Installation Wizard Completed** page, you can optionally select the **Show the Windows Installer log** check box and then click **Finish**.

Set up the Envoy services

If you received the following message during the process of running the installation wizard, complete the steps in this section.

> "The Engine service was unable to be initialized. Some ImageNow configurations will need to be created manually after installation is complete. Refer to the installation guide for more information."

This message indicates that the installation wizard was unable to automatically configure the Envoy service and some of the ImageNow workflow routes. If you did not receive this message, continue to the Set up ImageNow for signing section.

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://<*tomcatservername*>:<*port*>/Engine/SignatureEndpoint**, replacing *tomcatservername* 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 then complete the following steps.
        1. In **Workflow Designer**, double-click **DocumentStore**.
            1. In the **Queue Properties** dialog box, in the left pane, click **Actions**.
            2. On the **Inbound** tab, in the **iScript** list, select **DocumentStoreAndForward.js** and click **OK**.

2. In **Workflow Designer**, double-click **SignatureFailure**.
    1. In the **Queue Properties** dialog box, in the left pane, click **Actions**.
    2. On the **Inbound** tab, in the **iScript** list, select **CreateTask.js** and click **OK**.
3. Complete the following substeps to configure the **SubmitForSignature** Integration ASQ.
    1. In **Workflow Designer**, double-click **SubmitForSignature**.
    2. For **Success Action**, select **DocumentStore** from the **Queue** list and for **Failure Action**, select **SignatureFailure** from the **Queue** list.
    3. 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.
    4. Click **OK**.
4. Complete the following substeps to configure the **SendToAssureSign** Integration ASQ.
    1. In **Workflow Designer**, double-click **SendToAssureSign**.
    2. For **Success Action**, select **SignatureRequested** from the **Queue** list, and for **Failure Action**, select **SignatureFailure** from the **Queue** list.
    3. For **Envoy Service**, in the **Service Operation Name** list, select the **eAuthorize::SendToAssureSign** Envoy service.

       Note You do not need to map Envoy Service Parameters.
    4. Click **OK**.
5. Complete the following substeps to configure the **DownloadSignedDocuments** Integration ASQ.
    1. In **Workflow Designer**, double-click **DownloadSignedDocuments**.
    2. For **Success Action**, select **SignatureComplete** from the **Queue** list and for **Failure Action**, select **SignatureFailure** from the **Queue** list.
    3. For **Envoy Service**, in the **Service Operation Name** list, select the **eAuthorize::DownloadSignedDocument** Envoy service.

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

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 Management Console. The following list is an overview of these procedures.

1. Create document types and assign the custom properties.
2. Configure task templates for document notification.

3. Create a folder type to send multiple documents for signing.

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 **Document Types**.
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. Refer to 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 **Custom Properties** 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
    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, refer to 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**.
2. In the right pane, on the **Templates** tab, in the **Select a task type** box, click **Pointer**.
3. Under **Templates**, select **FailureNotification_Cancelled** and click **Modify**.

4. 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 **New Task** 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. Under **Workflow Assignment**, 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.
5. 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. Refer to 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 DocumentTRAK for status notifications

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

eAuthorizeDocumentStatus

1. Under the **Administration** tab, click **DocumentTRAK** on the left side of the window.
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 **[TODO: Server IP]** with the IP address of the server running Tomcat and click **Next**.
    4. Select **Edit Raw XML** and click **Next**.

5. Verify that the XML looks like the following example and click **Next**.

```
<?xml version="1.0" encoding="utf-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <UpdateStatusDocument xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns="http://www.perceptivesoftware.com/asq/esignature">
      <DOC_ORDER_ID>[Order ID]</DOC_ORDER_ID>
      <DOC_STATUS>[Document Status]</DOC_STATUS>
    </UpdateStatusDocument>
  </s:Body>
</s:Envelope>
```

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, click **Next**, and then click **Finish**.

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <impl:Response xmlns:impl="http://www.perceptivesoftware.com/asq/esignature">
      <impl:Return>true</impl:Return>
    </impl:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

eAuthorizeStepStart

1. Under **Administration**, expand **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 **[TODO: Server IP]** with the IP address of the server running Tomcat and click **Next**.
    4. Select **Edit Raw XML** and click **Next**.
    5. Verify the XML looks like the following example and click **Next**.

```
<?xml version="1.0" encoding="utf-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <UpdateStatusStepStarted xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns="http://www.perceptivesoftware.com/asq/esignature">
      <DOC_ORDER_ID>[Order ID]</DOC_ORDER_ID>
      <DOC_SIGNING_STEP>[Signing Step]</DOC_SIGNING_STEP>
    </UpdateStatusStepStarted>
  </s:Body>
</s:Envelope>
```

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, click **Next**, and then click **Finish**.

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <impl:Response xmlns:impl="http://www.perceptivesoftware.com/asq/esignature">
      <impl:Return>true</impl:Return>
    </impl:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

eAuthorizeStepComplete

1. Under **Administration**, expand **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 **[TODO: Server IP]** with the IP address of the server running Tomcat 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"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <UpdateStatusStepCompleted xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns="http://www.perceptivesoftware.com/asq/esignature">
      <DOC_ORDER_ID>[Order ID]</DOC_ORDER_ID>
      <DOC_SIGNING_STEP>[Signing Step]</DOC_SIGNING_STEP>
    </UpdateStatusStepCompleted>
  </s:Body>
</s:Envelope>
```

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, click **Next**, and then click **Finish**.

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <impl:Response xmlns:impl="http://www.perceptivesoftware.com/asq/esignature">
      <impl:Return>true</impl:Return>
    </impl:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

eAuthorizeStepUserVisit

1. Under **Administration**, expand **Notifications** and click **DocumentTRAK**.
2. In the **Web Notifications** 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 **[TODO: Server IP]** with the IP address of the server running Tomcat 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"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <UpdateStatusStepLandingPageVisited xmlns:xsi="http://www.w3.org/2001/XMLSchema
-instance"xmlns="http://www.perceptivesoftware.com/asq/esignature">
      <DOC_ORDER_ID>[Order ID]</DOC_ORDER_ID>
      <DOC_SIGNING_STEP>[Signing Step]</DOC_SIGNING_STEP>
    </UpdateStatusStepLandingPageVisited>
  </s:Body>
</s:Envelope>
```

    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, click **Next**, and then click **Finish**.

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <impl:Response xmlns:impl="http://www.perceptivesoftware.com/asq/esignature">
      <impl:Return>true</impl:Return>
    </impl:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

eAuthorizeDocumentCompleted

1. Under **Administration**, expand **Notifications** and click **DocumentTRAK**.
2. In the **Web Notifications** section, copy the **eAuthorizeDocumentCompleted** web notification template.
    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 **Service Endpoint (URL)** box, replace **[TODO: Server IP]** with the IP address of the server running Tomcat and click **Next**.
    4. Select **Edit** in the **Request XML** section.
    5. Select **Edit Raw XML** 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, then 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 on the exact parameter name enclosed in brackets in the **Request XML Editing** box.

     Note The values for Field1 through Field5 can be static text (no brackets) or could contain the name of an AssureSign jotblock within brackets ([JotblockName]) in order for the jotblock value to 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"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <UpdateStatusDocumentCompleted xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns="http://www.perceptivesoftware.com/asq/esignature">
      <DOC_ORDER_ID>[Order ID]</DOC_ORDER_ID>
      <DOC_ID>[Document ID]</DOC_ID>
      <DOC_AUTH_TOKEN>[Document AuthToken]</DOC_AUTH_TOKEN>
      <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>
    </UpdateStatusDocumentCompleted>
  </s:Body>
</s: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-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <impl:Response xmlns:impl="http://www.perceptivesoftware.com/asq/esign
ature">
      <impl:Return>true</impl:Return>
    </impl:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Set up an AssureSign template for signature

Refer to 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 matches the value you provide in the Configuration.xml file, highlighted in the following section. Refer to Appendix B: Configuration.xml file table for more information on the Configuration.xml file.

```
<section name="connectors">
        <section name="AssureSignConnector">
            <parameter name="AS_USERNAME" value=""/>
            <parameter name="AS_CONTEXT_ID" value=""/>
            <parameter name="AS_TEMPLATE_TAG" value=""/>
        </section>
    </section>
```

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 below 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

Refer to the Set up AssureSign DocumentTRAK for status notifications section for instructions on creating these web notifications.

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** then 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 should 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. Refer to the Configure eAuthorize for ImageNow 6.5.1 or 6.6 section for transmitting third-party documents in ImageNow 6.5.1 and 6.6.

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

1. In **AssureSign**, under **Administration**, expand **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 **[TODO: Server IP]** with the IP address of the server running Tomcat and click **Next**.
    4. Select **Edit Raw XML** 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 on 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"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <UploadSignedDocument xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns="http://www.perceptivesoftware.com/asq/esignature">
      <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>field1 value</field1>
      <field2>field2 value</field2>
      <field3>field3 value</field3>
      <field4>field4 value</field4>
      <field5>field5 value</field5>
      <documentType>doctype value</documentType>
      <DOCUMENT>[Completed Document]</DOCUMENT>
      <EXTERNAL_DOCUMENT_QUEUE>SignatureComplete</EXTERNAL_DOCUMENT_QUEUE>
    </UploadSignedDocument>
  </s:Body>
</s:Envelope>
```

Notes

- 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, then ImageNow uses the document ID as the default document name.

- If you do not provide a type for the documentType parameter, then the default document type for document transmission is used. Refer to the Create document types to download signed documents submitted by third party applications section of this document.
- 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-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <impl:Response xmlns:impl="http://www.perceptivesoftware.com/asq/esignature">
      <impl:Return>true</impl:Return>
    </impl:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

3. Create a template for document transmission. Refer to 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 refer to the *Perceptive eAuthorize Getting Started Guide*.

Configure DocumentTRAK for the AssureSign envelope template

1. In **AssureSign**, under **Administration**, expand **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 **Design Name** box, enter a name for the web notification.
   3. In the **Service Endpoint (URL)** box, replace **[TODO: Server IP]** with the IP address of the server running Tomcat and click **Next**.
   4. Select **Edit Raw XML** and click **Next**.
   5. Verify the XML looks like the following example and click **Next**.

```
<?xml version="1.0" encoding="utf-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <UpdateStatusEnvelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xmlns="http://www.perceptivesoftware.com/asq/esignature">
```

```
      <ENVELOPE_ID>[Envelope ID]</ENVELOPE_ID>
      <ENVELOPE_AUTH_TOKEN>[Envelope AuthToken]</ENVELOPE_AUTH_TOKEN>
    </UpdateStatusEnvelope>
  </s:Body>
</s:Envelope>
```

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, click **Next**, and then click **Finish**.

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <impl:Response xmlns:impl="http://www.perceptivesoftware.com/asq/esignature">
      <impl:Return>true</impl:Return>
    </impl:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Create an envelope template

Email notifications should be 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.
3. Select an email design set from the **Email Design Set** list and an **Account** from the **Accessibility** list.
4. 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

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.

Before proceeding, make sure that eauthorize-eform-agent.war, the Tomcat server, and ImageNow Forms Server are deployed on the same machine.

1. Open an internet browser, and then go to http://<tomcatservername>:<tomcatserverport>/ and click **Manager App**.
2. Log in with your credentials.
3. In the **Tomcat Web Application Manager** page, scroll to the **Deploy** section, and under **WAR file to deploy**, click **Choose File** to locate the **eauthorize-eform-agent.war** file.
4. Click **Deploy**.
5. Under the **Applications** section, verify that the **eauthorize-eform-agent** service is running.
6. Go to the **[*drive*:]\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\eauthorize-eform-agent\WEB-INF\conf** directory and complete the following substeps.
    1. Open **config.properties** and provide Platform Integration Engine IP, Platform Integration Engine port, AssureSign URL, AssureSign local domain (if a local AssureSign web application is in use), AssureSign username, and context ID.
    2. Save the file.
    3. Open the **log4j.properties** file and specify the path for downloading log file. The default path is **[*drive*:]\EAuthorizeEFormAgent**.
7. 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, refer to *Perceptive Software ImageNow Form Designer Help*.
    3. On the **Forms** tab, click **Manage Form Components**.
    4. Under **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**.

8. 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>
```

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**.

Disable buttons on eForms

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

1. Access the **[*drive*:]\inserver6\etc** directory and open the **imagenowforms.xml** file.
2. Go to the section where the **<FormName>** tag value is **eAuthorize_eForm**.
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="attachmentsVisible" 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 then 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 can 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, under **Document Transmission**, select **eAuthorizeExternalDocUpload** as the **Design Name**.

Troubleshooting

Situation: Cannot restart Tomcat after installing Platform Integration Engine.

Solution: It is possible that Integration Server and Platform Integration Engine are on the same physical server and port, and since Platform Integration Engine attempts to start before Integration Server is running, it halts. To check this, comment the XML element in the configuration.xml file containing the Integration Server URL, save the configuration.xml file, and start Tomcat. Then, remove the comment and restore the original file.

Situation: The WSDL at http://<server>:<port>/Engine/SignatureEndpoint does not show the operations. Messages might display, such as “ImageNow endpoint cannot be created.”

Solution: This situation can occur if you restart the Engine service multiple times within a short period of time. Each time the Engine service restarts, it creates a new connection with Integration Server. To close these open connections, complete the following steps.

1. Go to **ImageNow Management Console**.
2. Click **Diagnostics** on the left pane and log off all of the Integration Server connections. The status changes from **Connected** to **Disconnected**.
3. Restart the **Engine** service (restart only the Engine service and not Tomcat, if both Integration Server and the Engine service are on the same server and port).
4. Access the WSDL and verify that it shows all operations.

Situation: If Integration Server and ImageNow Forms Server are installed on the same Tomcat server, then one of the servers may not start, which can result in a Platform Integration Engine startup failure. A message such as “Cannot connect with ImageNow” might display.

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**.

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, then the original document will remain 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
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.xml file, 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 multiple signatories

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, then make sure that ImageNow uses the same Signatory 1 Full Name and Signatory 1 Email Address custom properties.

Refer to 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 reasons 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	SubmissionFailed	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.
IntegrationServer_Page_Delete.js	For replacing the original document upon downloading the signed version.
IntegrationServer_User_Get.js	For fetching the user information from ImageNow.
IntegrationServer_VersionControl_Checkin.js	For version control.
IntegrationServer_VersionControl_Checkout.js	For version control.
IntegrationServer_VersionControl_UndoCheckout.js	For version control.
IntegrationServer_WorkflowQueue_GetByName.js	For document transmission.
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 Audit History form

A Forms license is required to use forms in eAuthorize. If you need a Forms license, contact your Perceptive Software representative. Without this license, 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 load 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\worksheet directory and configures the corresponding ImageNow components.

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

Set the refresh time for the Audit History form

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

1. Navigate to the **[*drive*:]\inserver6\etc\eAuthorize** directory.
2. Open the **eAuthorize_config.xml** file and edit the following configuration parameters.
    1. In the **<envoyName>** tag, provide the Envoy service name for eAuthorize.
    2. In the **<refreshTime>** tag, provide the time, in seconds, for the refresh to occur.

About the workflow for sending documents for signature

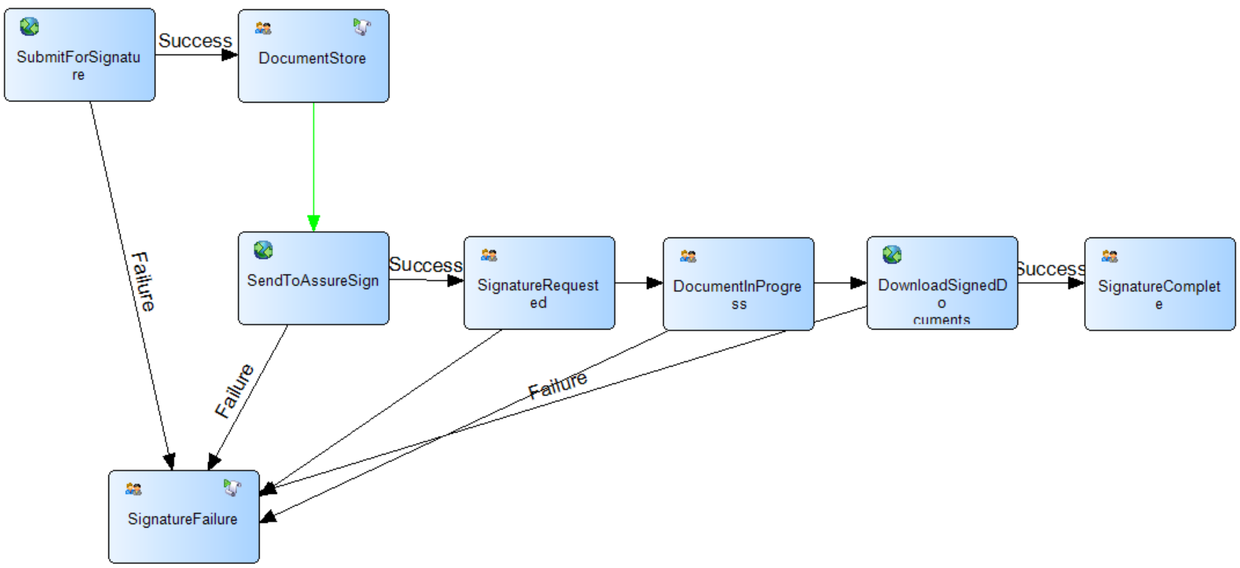
A workflow process is required to send documents to AssureSign for signature and to download the signed documents in ImageNow. Workflow configurations are automatically configured by the installer.

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.

Queue Name	Description
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.

You can verify the workflow setup in Workflow Designer, as shown in the workflow diagram below. You can use Workflow Designer if you are a user with the global privilege to manage workflow processes, a manager, or the owner.



When you use this process, if the flow of documents is interrupted anywhere in this workflow it redirects to the **SignatureFailed** queue. If that occurs, you can open the document in Workflow and click **Route Back** to return it.

Appendix B: Configuration.xml file table

The following table provides definitions and instructions for setting the parameter values in the configuration.xml file, located in the [*drive*:]\IntegrationEngine\etc directory. This table displays the settings under group headings, for example, `<AssureSignConnector>`, in the order the groups appear in the file. Use this table as a guide if you need to customize the file.

Section	Parameter	Guideline
AssureSignConnector	AS_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.
	AS_LOCAL_INSTANCE_DOMAIN_NAME	Set the value to null 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 will also find the machine name in self-signed certificate issued during AssureSign installation.
	AS_USERNAME	An AssureSign administrative account that is used to authenticate into AssureSign and submit documents for signature.
	AS_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.
	AS_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. Refer to the AssureSign Quick Reference Guide for instructions to create a template. To specify template tag, complete the following steps. 1. In **AssureSign** under the **Templates** tab, click **New**. 2. Select **Start from Scratch** and click **Next**. 3. Optional. Expand **Show Advanced Options** and type the template tag in **Template Tag**. 4. Enter this template tag value for the parameter in the **Configuration.xml** file and restart Platform Integration Engine.

Section	Parameter	Guideline
EMAIL **Note** This section is required for sending email notifications if a document fails, such as sending a document to AssureSign and there is an error.	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_SERVER_EMAIL_ID	The email ID configured on the SMTP server that sends email notifications.
	SMTP_AUTH_REQUIRED	If your SMTP email server requires authentication, then provide the value as 'true'; otherwise, use "false".
	SMTP_AUTH_USERNAME	If your SMTP email server requires authentication, then provide a username for the email server.
	SMTP_AUTH_PASSWORD	If your SMTP email server requires authentication, then provide the password corresponding to above-mentioned username for the email server.
IntegrationServer	IntegrationServerURL	The URL of Perceptive Integration Server. http://<tomcatservername>:<tomcatportnumber>/integrationserver/
	Username	A valid Perceptive Integration Server username.
	Password	The password for the abovementioned Perceptive Integration Server username.

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, click the **Administration** tab, and in the left pane, click **DocumentTRAK**.
4. In your **local** environment, click the **Administration** tab, and in the left pane, 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

AS_ ID, 31

AS_AUTH_TOKEN, 31

AS_SIGNATORY_MAIL, 31

AS_SIGNATURE_STATUS, 30, 31, 32, 34

AS_TEMPLATE_ID, 14

AS_TEMPLATE_TAG, 21, 36

Configuration.xml, 21, 31, 36

Connector, 31

Document Types, 14, 22

DocumentTRAK, 6

eAuthorize, 5

Flatten PDF Documents Prior to Processing, 22

Management Console, 13