opentext™

OpenText™ Electronic Signatures

Installation and Administration Guide

OpenText Electronic Signatures is an optional module that adds electronic signature capabilities and secure access control to Content Server.

LLESESN210100-IGD-EN-01

OpenText™ Electronic Signatures
Installation and Administration Guide
LLESESN210100-IGD-EN-01
Rev.: 2021-Jan-12

This documentation has been created for OpenText™ Electronic Signatures CE 21.1.
It is also valid for subsequent software releases unless OpenText has made newer documentation available with the product, on an OpenText website, or by any other means.

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111
Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440
Fax: +1-519-888-0677
Support: https://support.opentext.com
For more information, visit https://www.opentext.com

Table of Contents

Chapter 1

Installing and uninstalling OpenText Electronic Signatures

The OpenText Electronic Signatures module extends the OpenText Workflow capabilities to provide a secure way of managing Document review and approval processes. Electronic Signatures allows you to initiate signing Workflows in which Documents or Forms circulate and are either approved and signed or rejected by authorized users, called Signing Authorities. Information associated with each signing event, such as who approved a Document and when, is recorded and displayed through audit trails.

Electronic Signatures is supplemented with the *OpenText Electronic Signatures Extended Features* module, which provides new attribute types for Document numbering. The Electronic Signatures Extended Features module is dependent on Electronic Signatures and is added to the staging directory when you unpack the installation files. For more information about installing a module, see *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)*

After you install Electronic Signatures, you must administer its features. For example, you must set up some Signing Authority administrators, set the appropriate Electronic Signatures passwords, administer Electronic Signatures security features, and configure the properties associated with the Signatory and Electronic Signatures Robot Workflow steps. For more information, see the following: *OpenText Electronic Signatures - OpenText Content Server Admin Online Help (LLESESN-H-AGD)*.

This chapter covers the following topics:

1.1 Verifying system requirements

You must install the following software before you can install the OpenText Electronic Signatures module:

- OpenText™ Content Server
- Third-party renditioning engine

To make full use of all Electronic Signatures features, you can also install the optional Content Server module, Content Server PDF Forms. You install the PDF Forms module if you want to allow users to sign PDF Forms and manipulate form views. These modules allow you to attach Content Server Forms and PDF Forms to signing Workflows. For more information about PDF Forms, see *OpenText Electronic Signatures - OpenText Content Server User Online Help (LLESESN-H-UGD)*.

You install a renditioning engine if you want to convert documents to PDF using the Electronic Signatures Robot step in signing Workflows. For more information about converting documents to PDF format, see *OpenText Electronic Signatures - OpenText Content Server User Online Help (LLESESN-H-UGD)*.

Note: Although you can install any third-party renditioning engine, OpenText recommends that you use OpenText™ Blazon™ for Content Suite, which you can purchase from Open Text Corporation. For more information about installing and using Blazon for Content Suite, see the documentation that accompanies the product.

1.2 Installing Electronic Signatures

Electronic Signatures is compatible with Content Server and relies on server-side PDF manipulation tools from Appligent. to securely sign and watermark documents within a Workflow. These command-line tools perform specific functions to extract or map particular information to and from PDF files. They run as a process on the primary admin server installed with Content Server. The Appligent tools are included with the Electronic Signatures module.

You can obtain the Electronic Signatures files from the OpenText My Support (https://knowledge.opentext.com/). You must download these files to a temporary folder on the server before you can begin the installation process.

You install the Electronic Signatures module and the Electronic Signatures Extended Features module the same way that you install most other optional Content Server modules. For more information about installing Content Server modules on Windows and UNIX-like systems, see *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)*.

1.2.1 Installing the Appligent products

You must install Appligent products for both Windows and UNIX-like environments.

To install Appligent products on Windows:

1. Uninstall any previously installed Appligent products.
2. Access the *<Content Server_home>* directory, and create a new directory called `fonts`.
3. Change directory to the *<Content Server_home>*`\module\esign_`*<x>*`_`*<y>*`_`*<z>*`\dropin\stamppdfbatch` directory, and run `StampPDFBatch`, entering the serial number contained in the `key.txt` file.
   a. During the StampPDFBatch installation process, for **Installation Path**, enter *<Content Server_home>*`\module\esign_`*<x>*`_`*<y>*`_`*<z>*`\dropin\stamppdfbatch`.
   b. For the **Font Path**, enter *<Content Server_home>*`\fonts`.
4. If you have any font files that you want to use for the stamping signature, store those font files in the *<Content Server_home>*`\fonts` folder.
5. Access the *<Content Server_home>*`\module\esign_`*<x>*`_`*<y>*`_`*<z>*`\dropin\fdfmerge` directory, and run `FDFMerge`, entering the serial number contained in the `key.txt` file.
   a. During the FDFMerge installation process, for **Installation Path**, enter *<Content Server_home>*`\module\esign_`*<x>*`_`*<y>*`_`*<z>*`\dropin\fdfmerge`.
   b. For the **Font Path**, enter *<Content Server_home>*`\fonts`.
6. Access the *<Content Server_home>*`\module\esign_`*<x>*`_`*<y>*`_`*<z>*`\dropin\secursign` directory, and run `SecurSign`, entering the serial number contained in the `key.txt` file.
   - During the SecurSign installation process, for **Installation Path**, enter *<Content Server_home>*`\module\esign_`*<x>*`_`*<y>*`_`*<z>*`\dropin\secursign`.
7. Access to the *<Content Server_home>*`\module\esign_`*<x>*`_`*<y>*`_`*<z>*`\dropin\appendpdf` directory, and run `AppendPDF`, entering the serial number contained in the `key.txt` file.
   a. During the AppendPDF installation process, for **Installation Path**, enter *<Content Server_home>*`\module\esign_`*<x>*`_`*<y>*`_`*<z>*`\dropin\appendpdf`.
   b. For the **Font Path**, enter *<Content Server_home>*`\fonts`.

To install Appligent products on UNIX-like systems:

1. On a UNIX-like system, sign in to the system as the `superuser`.
2. Change directory to *<Content Server_home>* and create a new directory called `fonts`.
3. Navigate to the *<Content Server_home>*`/module/esign_`*<x>*`_`*<y>*`_`*<z>*`/dropin` folder. Ensure that the following Appligent files are present:

   - `apgetinfo.tar.gz`
   - `appendpdf.tar.gz`
   - `fdfmerge.tar.gz`
   - `securesign.tar.gz`
   - `stamppdfbatch.tar.gz`

   In the *<Content Server_home>*`/module/esign_`*<x>*`_`*<y>*`_`*<z>*`/dropin` folder, extract the Appligent files.
4. In the *<Content Server_home>*`/module/esign_`*<x>*`_`*<y>*`_`*<z>*`/dropin` folder, extract the contents from each of the Appligent files.

   Important
   Do not change the names of any of the extracted directories.
5. Navigate to the `apgetinfo` folder, and then run the `./install.sh` command.

   Tip: Optionally, to check that the install has run correctly, run the `./apgetinfo -h` command after you run the `./install.sh` command.
6. Navigate to the `appendpdf` folder, then run the `./install.sh` command.

   Tip: Optionally, to check that the install has run correctly, run the `./appendpdf -h` command after you run the`./install.sh` command.
7. Navigate to the `fdfmerge` folder, then run the `./install.sh` command.

   Tip: Optionally, to check that the install has run correctly, run the `./fdfmerge -h` command after you run the `./install.sh` command.
8. Navigate to the `securesign` folder, then run the `./install.sh` command.

   Tip: Optionally, to check that the install has run correctly, run the `./securesign -h` command after you run the `./install.sh` command.
9. Navigate to the `stamppdfbatch` folder, then run the `./install.sh` command.

   Tip: Optionally, to check that the install has run correctly, run the `./stamppdfbatch -h` command, after you have run the `./install.sh` command.

10. If you have any font files that you want to use for the stamping signature, store the font files in the *<Content Server_home>*/fonts folder.

1.2.2 Configuring the Electronic Signatures agents

Electronic Signatures uses agents to perform tasks on a schedule. You must enable only one instance of each Electronic Signatures agent must be enabled in a Content Server cluster.

The following table lists and describes the tasks performed by Electronic Signatures agents.

Table 1-1: Electronic Signatures agents

Name	AgentID	Function
SignatoryAgent	2501	Completes Electronic Signatures Robot Workflow steps, if the steps require conversion of Workflow attachments to PDF documents. This agent runs every 5 minutes.
GenerationAgent	2502	Completes Electronic Signatures Generation Workflow tasks. This agent runs every 5 minutes.
Signing Password Expired	2503	Sends email notifications about the expiration of signing passwords. These settings are controlled in the **Configure Signing Password Settings** Electronic Signatures administration page, and the Content Server administration pages for Notification Administration. For more information about these settings, see *OpenText Electronic Signatures - OpenText Content Server Admin Online Help (LLESESN-H-AGD)*. This agent runs once a day.

Name	AgentID	Function
Clear undolabelinfo Table	2504	Removes records that are no longer needed. • For completed and archived Workflows, it removes their records in the `undolabelinfo` table. • For completed and archived Workflows, it removes their records in the `fieldinfo` table. • For completed Workflows, it removes their records in the `itemrefinfo` and `itemrefdata` tables. This agent runs once a week.

1.2.3 Adding an admin server

Electronic Signatures requires that an admin server is present, started, and local on each Content Server front-end computer in a cluster, in order to run the Electronic Signatures agents tasks.

To add an admin server to each Content Server in the cluster:

1. In the **Search Administration** section of the **Content Server Administration** page, click the **Open the System Object Volume** link.
2. On the **Content Server System** page, on the **Add Item** menu, select **Admin Server**.
3. On the **Add: Admin Server** page, in the **Admin Server** area, do the following:
   a. In the **Alias Name** box, enter a unique name for this admin server.

      Tip: OpenText recommends that you choose a naming convention for all admin servers in the cluster. For example, name the first admin server *eSignAdminServer1*, and the second admin server *eSignAdminServer2*. Keep increasing the number for each new admin server until you have added one admin server to each Content Server instance in the cluster.

   b. Clear the **Set as Default Admin Server** check box.
   c. In the **Host Name** box, enter the host name of this particular computer.
   d. In the **Port Number** box, use the value assigned to **port**. You find this value in the **[OTAdmin]** section of the `opentext.ini` file on this particular instance.

e. In the **Password** box, type your Content Server administrator password.

f. In the **Verify Password** box, retype your Content Server administrator password.

4. Click **Add**.

5. On the **Content Server System** page, ensure that your new admin server is *Active* in the **Status** box.

Tip: If it is not active, click the **Functions** menu for the new admin server, and then click **Ping Server**.

6. Repeat these steps for all Content Server instances in the cluster.

1.3 Upgrading Electronic Signatures

When upgrading Electronic Signatures, the process for upgrading is similar to other Content Server modules. However, consider the following before proceeding with the upgrade:

- Any previously installed Appligent products (`ApGetInfo`, `AppendPDF`, `FDFMerge`, `SecurSign`, and `StampPDFBatch`) must be uninstalled. You can only have one copy each of the Appligent products installed on your Content Server machine.
- A change in how Electronic Signatures handles signature settings means that settings will revert to default values when an upgrade is performed. Make a record of your settings, and apply the changes after the upgrade on the **Configure Electronic Signatures Settings** page. For more information, see "Administering Electronic Signatures passwords" on page 22.

For more information about upgrading Content Server modules, see *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)*.

1.4 Uninstalling Electronic Signatures

Before you uninstall Electronic Signatures, ensure that all initiated signing Workflows have been completed. Otherwise, the Workflow information contained in Content Server may be lost and the signing Workflow may not complete correctly. Then, you can uninstall the Electronic Signatures module the same way that you uninstall other optional Content Server modules.

When you uninstall the Electronic Signatures module, the following Electronic Signatures administrator settings and audit information are deleted:

- Settings on the **Configure Electronic Signatures Settings** page.
- Signing Authority administrators.
- Signing passwords.
- Information on the **Signatory** tab.

- Stamping and undo watermark information in the Robot step.
- All existing Electronic Signatures tables.
- All signature trails.

Note: This information will not be recovered when Electronic Signatures is reinstalled.

For information on uninstalling the Electronic Signatures module, see *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)*.

Chapter 2

Overview

Using the OpenText Electronic Signatures module, Document and Form signing processes take place under the control of a Workflow. When the Electronic Signatures module is installed, the following Workflow steps, specific to electronic signing, are added:

- **Signatory Step**

  Creates a user assignment requesting the user to reauthenticate with their user name and password. A signature manifestation is stamped onto the Document or Form and an audit trail record is created.

- **Robot Step**

  Converts a Document into PDF format so that it can be stamped with electronic signing information. Sets PDF security options, and can place watermarks on a Document to ensure Document protection.

- **Generation Step**

  Creates a secure Generation of the Document and places it in a specified Workflow location.

The Electronic Signatures module enhances Content Server functionality and features to provide compliance with electronic signatures regulations, such as the FDA ruling found in *21 CFR Part 11* and the *1999/93/EC* directive on electronic signatures of the European parliament.

Electronic Signatures uses content from Appligent. For additional information on Appligent content, see the Appligent documentation (docs.appligent.com).

2.1 OpenText Electronic Signatures features

This section describes the main features of OpenText Electronic Signatures.

Security

The following security features are available for Electronic Signatures:

- User privileges can be applied for Signing Authority administrators and Signing Authority Users to restrict signing rights to selected preauthorized individuals.
- Authentication can be required to view or modify the PDF Document secure password.
- Security can be applied to a PDF Document to control the ability to edit, print, or access text. Electronic Signatures can encrypt a PDF Document using either 40-bit or 128-bit encryption levels.

Audit

The following audit features are available for Electronic Signatures:

- An audit event entry can be created when sign-in is disabled due to lock out.
- Signing step reauthentication can be audited.
- A signing event can be recorded in the signing audit trail.
- A signing audit trail can be created for the Document used to initiate a Workflow.
- A signature manifestation can be applied to the signed Document.
- An audit trail of changes to the user profile and group membership can be displayed.

Document management

The following document management features are available for Electronic Signatures:

- Documents can be rendered as PDF for signing purposes.
- A signing page can be attached to PDF Documents at the front or back of the Document.
- Defined templates can be used for the signing page.
- A Document reference, or Generation, of the approved and signed Document version can be created.
- Watermarks can be applied to a PDF Document.

Workflow

The following Workflow features are available for Electronic Signatures:

- The Workflow designer can choose the Generation Document storage location within Content Server.
- The Workflow initiator can sign a Document.
- Watermarks can contain Document and Workflow system and custom attributes.
- Content Server Web Forms can be converted into HTML Documents as Workflow attachments to allow for conversion to PDF and subsequent signing.
- The list of Workflows displayed for the **Initiate Workflow** from Document function can be filtered by Category attribute values.
- Categories and attributes can be passed to the Workflow attachment and the Document Generation.

Signing

The following signing features are available for Electronic Signatures:

- The Signatory step provides Document approval or rejection as one of the specific sequence of steps in a review and approval Workflow design.
- Signing can be performed on either the Document used to start the Workflow, or the first attachment added to the Workflow.
- A PDF Form can be signed.
- The components required for reauthentication on a signing step can be configured. Examples of the components include user name, system password, and alternate signing password.
- An optional digitized signature image can be included with the signature manifestation.
- The time zone description on the signature manifestation can be derived from the system time zone, the client time zone, or the user's personal profile.
- A Signing Authority can accept a signing assignment on behalf of a group.
- Reauthentication on delegation of a signing assignment can be suppressed.

Electronic Signatures Extended Features module

You can install this additional module separately, and it provides the following features:

- Display of Category attribute changes showing both old and new values.
- Special attribute types for Document ID and Document release numbering are available for the Regulated Document Category.

2.2 Understanding Electronic Signatures with Workflows and Forms

OpenText Electronic Signatures is an optional module that relies heavily upon the combined features of both Workflows and Forms. This guide explains how to use Electronic Signatures, and offers a brief overview of Workflows and Forms. This guide does not explain, in detail, the functionality of implementing Workflows or Forms within Content Server.

For more information about using Workflows, see *OpenText Workflow - Workflow Designer's Guide (LLESWFP-CWM)* and *OpenText Content Server - Workflow Maps (LLESWFP-H-UGD)*.

For more information about using the Forms module, see *OpenText Content Server - Workflow Forms (LLESFWF-H-UGD)* and *OpenText Content Server - Workflow Maps (LLESWFP-H-UGD)*.

You can use Workflows and Workflow Maps to implement and run business processes in Content Server. A Workflow is a predefined implementation of a business process that usually involves multiple users and tasks. For example, a simple Workflow Map can provide a way for an employee to request and receive

permission to take a vacation day, and may consist of a few tasks that involve the employee, a manager, and a human resources representative. A complex Workflow Map can contain numerous steps and require the participation of dozens of users. A Workflow Map is a graphical representation of the both business process and the information used in the business process.

A Workflow Map contains the following:

- A series of linked steps that define tasks, users, milestones, evaluations, and other functions that are performed sequentially or in parallel.
- A work package, which consists of attachments, comments, attributes, and other information related to the work process.
- General settings, which consist of management permissions, due date calculations, the type of information included in the work package, and other settings that affect the entire Workflow Map.

Content Server Forms is an optional module that enables you to create electronic documents used to organize and collect data. For example, you can implement a survey as a Form. When Forms are available, you can make them available in Workflow Maps.

When you enable and add Forms to the Workflow Map‘s work package, you can use them in the following ways:

- Make them available on Start, User, Initiator, and Item Handler steps.
- Define Form Task steps to users or groups that present a Form and no other task as an assignment.

The Form data gathered during the Workflow process is stored and can be viewed in the Workflow. Also, you can define an Evaluate step that determines how to route a Workflow based on a Form field value.

Electronic Signatures adds electronic signature capabilities to Content Server. It allows Content Server users to initiate Workflows to manage processes that require other authorized users to review and approve Documents. Audit trails capture the details of each signing event, including each signing authority's full name, job title, the meaning associated with the signing, and the time and date. An example of a meaning associated with the signing is the approval of an expense report. The information can be applied to the original Document as a signature manifestation, and then the Generation is an alias of that original document that is more widely distributed outside the Workflow.

2.3 Understanding multilingual Electronic Signatures

The administrator must download, install, and enable the required language packs from the OpenText My Support (https://knowledge.opentext.com/knowledge). Once installed and enabled, the administrator can assign that language as the system default language.

For more information about installing and enabling language packs, see *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)* and *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)*.

If your system has multiple languages installed and enabled, you can input values to multilingual metadata boxes. When items are created in Electronic Signatures, the

Click to edit multilingual values button  will appear next to certain boxes, such as **Name** and **Description**. Clicking this button will bring up the **Edit Additional Languages** dialog box. Users can type text for these boxes in any language installed and enabled on their system.

For general information about using multilingual in Content Server, see *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)*, *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)*, and *OpenText Content Server - Get Started (LLESRT-H-UGD)*.

Language rules in Electronic Signatures

Electronic Signatures follows a specific order to display the contents of boxes which allow multilingual values. This order applies to the display of all multilingual content in Electronic Signatures, including signing and watermarking:

- The system default language, if it has been set.
- If the system default language has not been set, Electronic Signatures will display the contents of multilingual boxes in English.
- If the system default language has not been set, and no entry for English is found for that box, then Electronic Signatures will display the contents of the multilingual text boxes in the first language found, searching alphabetically by language code.

Important

For every Electronic Signatures box which allows you to input multilingual values:

1. OpenText recommends that you enter all Electronic Signatures metadata values in the system default language.
2. OpenText recommends that you enter all Electronic Signatures metadata values in English.

Note: Electronic Signatures does not display languages using the same priority order used for multilingual user interface in Content Server. The user's preferred language, either browser-specific or user-specified, is not used.

2.3.1 To edit multilingual values boxes

To edit multilingual values boxes:

1. Click the **Click to edit multilingual values** button  next to any box where it is available. The **Edit Additional Languages** dialog box opens. This dialog box can have multiple tabs, one for each box that can be edited.
2. In the dialog box, enter a value in the system default language box.
3. Optional Enter values in any multilingual box available. Only those languages which have been installed and enabled will have a multilingual box.
4. Optional If you are going to enter values for any other multilingual-available box, first type the value in the system default language, then enter values for any of the other languages.
5. Click **OK**.

Chapter 3

Administering Electronic Signatures

When you add the Electronic Signatures module to Content Server, users can initiate Workflows that require specific authorized users to review and approve Documents.

For more information about initiating and signing Documents with Electronic Signatures, see *OpenText Electronic Signatures - OpenText Content Server User Online Help (LLESESN-H-UGD)*.

Audit trails capture the details of each signing event, including the following:

- Each signing authority's full name, job title, and corporate position.
- The meaning associated with the signing, for example, the approval of an expense report.
- The time and date of signing.

This information can be applied to the original Document as a signing manifestation. A duplicate of the original Document, or a Generation, can be created and circulated without altering the original Document.

Before users begin using Electronic Signatures, you must administer some of its features. For example, you must do the following:

- Set up Signing Authority administrators.
- Set the Electronic Signatures passwords.
- Administer the security features of Electronic Signatures.
- Configure the settings associated with the Signatory and Electronic Signatures Robot Workflow steps.
- Configure the secure sign in features of Electronic Signatures to strengthen Content Server access control.
- Specify the user or group to whom an error email will be delivered.

You can administer these features from the **Content Server Administration** page, in the **Electronic Signatures Administration** section.

Important

To see how many users are currently permitted to use Electronic Signatures, run a Content Server System Lite Report. For more information about Content Server System reports, see *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)*.

3.1 Administering Electronic Signatures features

The following sections describe the features of Electronic Signatures that you must set up before users can begin using the OpenText Electronic Signatures module.

Electronic Signatures passwords

You can apply security controls at a signing event by enabling Electronic Signatures signing passwords, which users must enter when they sign documents. Also, to ensure that the signed documents are not altered, you can set a Document password, which is used to secure PDF Documents after they are signed. For more information about Electronic Signatures passwords, see "Administering Electronic Signatures passwords" on page 22.

Signatory properties

Electronic Signatures extends Content Server's standard Workflow capabilities to control the signing or approval of Documents as part of business processes. For more information, see "Administering signatory properties" on page 24.

Electronic Signatures Robot properties

The Electronic Signatures Robot step adds the ability to convert Documents, which are attached to a Workflow, into PDF format. Administering the Electronic Signatures Robot step includes setting up the directories necessary to perform the document conversion. You can also use the Robot step to add watermarks and improved security to PDF Documents. For more information, see "Administering Robot properties" on page 30.

Content Server access control

You configure the Electronic Signatures secure sign-in features to strengthen Content Server access control and reduce the threat of unauthorized Content Server access and use. You can maintain audit trails of events, such as signing in, signing out, and providing signatures, to track user behavior in Content Server For more information, see "Setting Electronic Signatures audit data" on page 33.

Electronic Signatures error email recipients

Workflows sometimes experience errors, and it is important to specify the user or group that an error email will be delivered to if such an event occurs. Error emails can be sent to either an administrator, or to the Master Manager user or group specified in the Workflow. For more information see "Setting Electronic Signatures error email recipients" on page 35.

3.2 Administering Signing Authority administrators

Users with system administration rights have the option of being members of signing groups. By default this option is disabled, but you can enable it.

Note: The Administrator user cannot be a member of signing groups.

3.2.1 Working with Signing Authority administrators

Signing Authority administrators are Content Server users who are responsible for setting up and administering Signing Authorities. Signing Authorities are Content Server users who can sign Documents that circulate as part of signing Workflows. An administrator user can set up and remove Signing Authority administrators, but cannot be a Signing Authority administrator or Signing Authority.

You can create a Signing Authority administrator when you create a new user or when you edit an existing user. Signing Authority administrators are automatically given rights to create and modify groups in Content Server. You remove a Signing Authority administrator's rights when you want to revoke that user's ability to set up and administer Signing Authorities.

To set up a Signing Authority administrator

To set up a Signing Authority administrator:

1. On the Global Menu Bar, click **Users & Groups** on the **Enterprise** menu.
2. On the **Users & Groups** page, find the user that you want to set up as a Signing Authority administrator.
3. In the **Actions** column, click the **Edit** link for that user.
4. On the **General Info** page for that user, select the **Signing Authority Administrator** check box.
5. Click **Update**.

To remove a Signing Authority administrator

To remove a Signing Authority administrator:

1. On the Global Menu Bar, click **Users & Groups** on the **Enterprise** menu.
2. On the **Users & Groups** page, find the user that you want to remove as a Signing Authority administrator.
3. In the **Actions** column, click the **Edit** link for that user.
4. Clear the **Signing Authority Administrator** check box.
5. Click **Update**.

3.3 Administering Electronic Signatures passwords

You can configure Electronic Signatures passwords in the Content Server Electronic Signatures administration section. You can configure the Electronic Signatures signing password settings for all users. For example, you can specify the minimum number of characters that passwords must contain, whether passwords must contain digits, and if and when passwords expire. For more information about configuring password settings, see "Configuring signing password settings" on page 28.

3.3.1 Enabling and resetting signing passwords

By default, Signing Authorities must provide their Content Server system password before they can sign a Document in a signing Workflow. If you want Signing Authorities to provide a different password before signing a Document, you enable signing passwords. You can then specify whether you want Signing Authorities to provide their signing passwords in addition to, or instead of, their Content Server system passwords. After you enable signing passwords, each Signing Authority must set up their particular password. For more information, see *OpenText Electronic Signatures - OpenText Content Server User Online Help (LLESESN-H-UGD)*.

If you have enabled signing passwords, and a Signing Authority forgets the password that they set up, only a Signing Authority administrator who does not have user administration rights can reset that Signing Authority's signing password. When a password is reset, it is reset to a user's Content Server user name. For more information, see *OpenText Electronic Signatures - OpenText Content Server User Online Help (LLESESN-H-UGD)*. For more information about editing a Content Server user's profile, see *OpenText Content Server - Users and Groups (LLESWBU-H-UGD)*.

To enable Signing Authority passwords

To enable Signing Authority passwords:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Settings** link.
2. In the **Password Settings** section of the **Configure Electronic Signatures Settings** page, in the **Signing Password Required** area, select the **Enable** check box.
3. Click one of the following options:
   - **Additional Password**, which requires Signing Authorities to provide a signing password and a Content Server system password when signing documents in a signing Workflow.
   - **Alternate Password**, which requires Signing Authorities to provide a signing password instead of a Content Server system password when signing documents in a signing Workflow. This is the default setting.

4. Click **Save Changes**.

3.3.2 Setting the secure Document password

To prevent users from performing unauthorized actions to a PDF Document, a secure Document password is required. This password is used by the Electronic Signatures Robot Workflow step to restrict PDF features such as printing, editing, or selecting text and graphics. For more information, see "To view the secure Document password archive" on page 23.

Whenever the secure Document password is changed, the event is recorded and archived. Viewing the secure Document password archive displays the current and previously applied passwords, as well as the date the password was changed.

Important

A temporary password is supplied when you first install the OpenText Electronic Signatures module. OpenText recommends that you change this password immediately after installation.

To view the temporary password, view the secure password archive and look at the **Document Password** column. For more information, see "To set the secure Document password" on page 24.

Notes

- To prevent unauthorized access to secure PDF Documents, ensure that no other user knows this password.
- When setting the secure Document password, use ASCII characters only.

To view the secure Document password archive

To view the secure Document password archive:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Settings** link.
2. In the **Password Settings** section of the **Configure Electronic Signatures Settings** page, in the **Secure Document Password** area, click **View Secure Password Archive**.
3. On the **Content Server Administrator User Log-in** page, enter your administrator credentials in the **Username** and **Password** boxes, and then click **Log-in**.
4. On the **View Secure Document Password Archive** page, view the password archive. The current password is the first password listed in the **Document Password** column.
5. When you have finished, click **Close**.

To set the secure Document password

To set the secure Document password:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Settings** link.

   Note: If you are setting the password for the first time, the current secure password is the default password, and it can be found by accessing the secure document password archive. For more information, see "To view the secure Document password archive" on page 23.

2. On the **Configure Electronic Signatures Settings** page, in the **Password Settings** section, in the **Secure Document Password** box, click **Set Secure Password**.

3. On the **Content Server Administrator User Log-in** page, type your administrator credentials in the **Username** and **Password** boxes, and then click **Log-in**.

4. On the **Set Secure Document Password** page, in the **Current Password** box, type the current secure password.

5. In the **New** box, type the new secure password.

   Note: Your password must contain ASCII characters and must be at least six characters.

6. In the **Verify Password** box, retype the new secure password.

7. Click **Save Changes** > **OK**.

3.4 Administering signatory properties

Administering signatory properties allows you to set up the parameters associated with the Signatory step of a Workflow. When Workflows are created, Signatory steps are defined and assigned to Signing Authorities. When a Signing Authority completes each Signatory step, their signature manifestation is added to a signing page, which is generated from the corresponding Signing PDF Template file. When you set signatory properties, you are specifying parameters for the PDF Template file, determining if the Workflow Initiator is a Signing Authority, allowing administrators to sign documents, and setting date and time options.

3.4.1 Adding Signing PDF Templates

Signing PDF Template files are PDF files that Workflow creators associate with Signatory steps in signing Workflows. When a Signing Authority completes each Signatory step, their signature manifestation is added to a signing page that is generated from the corresponding Signing Template file. When the first user signs the Document, the signature page is appended to either the front or the back of the Document, and the user's signing manifestation is stamped onto the page. Subsequent user signature manifestations are added when additional pages are appended. The administrator can specify the number of signatures to a maximum of five signature manifestations per page.

To view a sample Signing Template file, go to the *<Content Server_home>*/`module/esign_16_2_8/documentation` directory, and open the `esigntemplatefile.pdf` file. For more information about creating Signing Template files and defining Signatory steps, see *OpenText Electronic Signatures - OpenText Content Server User Online Help (LLESESN-H-UGD)*.

Before a Signing PDF Template file can be used in a Signing Workflow, you must add it to the Electronic Signatures Signing PDF Template folder in Content Server. If a Signing PDF Template file is not used by existing Workflows, and you no longer want it to be available to Workflow creators, you remove it. For information about adding documents to Content Server, see *OpenText Content Server - Documents and Text Documents (LLESWBD-H-UGD)*. For information about deleting items from Content Server, see *OpenText Content Server - Get Started (LLESRT-H-UGD)*.

To add a Signing PDF Template file

To add a Signing PDF Template file:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Open the Electronic Signatures Signing PDF Templates Volume** link.
2. On the **eSign Signing PDF Templates** page, on the **Add Item** menu, select **Document**.
3. On the **Add: Document** page, in the **Document** box, click **Existing**.
4. Click **Choose**, navigate to the file, and click **Open**.
5. In the **Name** box, type a name for the document.

   Tip: If your system has multiple languages installed and enabled, click the **Click to edit multilingual values** button  to edit the names in the other enabled languages.
6. Optional In the **Description** box, type a description for your document.
7. In the **Version Control** box, click either **Standard**, which is the default, or **Advanced**.

8. Optional In the **Categories** box, click **Edit** to either select or add a Category to apply to this document.
9. Optional If you want to place the document in a location other than that in the **Create In** box, click **Browse Content Server**, navigate to the container where you want to place the document, then click its **Select** link.
10. Click **Add**.

3.4.2 Determining if the Workflow Initiator is a Signing Authority

When a Signing Workflow is initiated, you can configure the system to determine whether any Signatory Steps are assigned to the Initiator, and whether the user initiating the process is a Signing Authority.

Note: If you use the **Check if Workflow Initiator is a Signing Authority** option, all signing Workflows may experience a minimal delay in the initiation of the Workflow. The length of the delay depends on your system, but should not last more than a few minutes.

To determine if the Workflow Initiator is a Signing Authority

To determine if the Workflow Initiator is a Signing Authority:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Settings** link.
2. In the **Signing Settings** section of the **Configure Electronic Signatures Settings** page, select the **Check if Workflow Initiator is a Signing Authority** check box.
3. Click **Save Changes**.

3.4.3 Specifying authentication properties

You can also administer the authentication properties associated with a Signatory step. When Signing Authorities complete Signatory steps, Electronic Signatures prompts them to provide their user name and each required password. Electronic Signatures uses this information to verify that the current user has signing authority and to apply the user's signature manifestation to the Signing PDF template associated with the step. To simplify the authentication process, you can configure Electronic Signatures to automatically provide the Signing Authority's user name, so that the Signing Authority only provides each required password. For more information about signing passwords, see "Administering Electronic Signatures passwords" on page 22.

To set the maximum number of signatures per signing page

To set the maximum number of signatures per signing page:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Settings** link.
2. In the **Signing Settings** section, in the **Signatures Per Signing Page** area, enter a number in the **Number of Signatures Per Page** box, or use the slider.
3. Click **Save Changes**.

To allow system administrators to sign documents

To allow system administrators to sign documents:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Settings** link.
2. In the **Signing Settings** section, select the **Enable** check box for **Enable System Administrators to be Members of Signing Groups**.
3. Click **Save Changes**.

To pre-populate the user name on signing

To pre-populate the user name on Signing:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Settings** link.
2. In the **Signing Settings** section, select the **Enable** check box for **Enable Pre-population of User Name on Signing**.
3. Click **Save Changes**.

3.4.4 Setting date and time parameters

When applying the date and time format to the signature manifestation, you can choose either the server or the client computer. If you select the client date and time, you can apply the time zone description from either the client computer or the client's Content Server user profile. If you are going to apply the time zone description from the user profile, ensure that Signing Authorities have the time zone included in their user profile. For more information about setting up the user profile, see *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)*.

Note: OpenText recommends that you use the server setting for the date and time format. If the client setting is selected, the time and date of the client system is used. This could cause problems with the Workflow, because the client time and date for one participant may be different from others who are participating in the Workflow.

To set signature manifestation date and time

To set signature manifestation date and time:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Settings** link.
2. In the **Signing Settings** section, in the **Select Signing Manifestation Date/Time** area, click one of the following options:
   - **Server**, to apply the server date and time.
   - **Client**, to apply the client date and time.
3. Optional In the **Apply User Profile Time Zone Description on Signing Manifestation** area, select the **User Profile** check box to apply the time zone set in the user profile to the Client.
4. Optional In the **Set Content Server Time Zone Description** area, click **Select Server Time Zone Description** to change the time zone setting for the server.
5. Click **Save Changes**.

3.5 Configuring signing password settings

You can configure password settings for Electronic Signatures in the **Electronic Signatures Administration** section of the **Content Server Administration** page. When upgrading to Electronic Signatures 16, these settings are created with default values. You will have to change them here, if desired.

Tip: If you want to retain all settings for signing passwords, copy the settings on the **Configure Password Settings** page before performing the upgrade to Electronic Signatures 16.

You can configure the following options for signing passwords:

- **Minimum Number of Characters**, determines the minimal number of characters required in a password.
- **Password Must Contain a Digit**, determines if a password requires a number.
- **Password Cannot Begin with a Digit**, determines if a password can begin with a number.
- **Password Cannot End with a Digit**, determines if a password can end with a number.
- **Changed Passwords Must Be Different**, determines if a changed password must differ from previously used passwords.
- **Password Expiration**, determines if signing passwords will expire. If this setting is disabled, signing passwords will never expire.
- **Days to Prevent Password Reuse**, determines how many days must pass before a password can be reused.

- **Days Required Between Password Changes**, determines the number of days between required password changes.

Note: All settings for this feature apply to all instance on a cluster installation of Electronic Signatures.

3.5.1 To configure the signing password settings

To configure the signing password settings:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Signing Password Settings** link.
2. On the **Configure Signing Password Settings** page, do the following:
    1. Enter the **Minimum Number of Characters** for a password.
    2. In the **Password Must Contain a Digit** area, select the **Enable** check box to require a number in a password.
    3. In the **Password Cannot Begin with a Digit** area, select the **Enable** check box to specify that passwords cannot begin with a number.
    4. In the **Password Cannot End with a Digit** area, select the **Enable** check box to specify that passwords cannot end with a number.
    5. In the **Password Expiration** area, click **On** to set an expiry date for signing passwords, and enter the number of **Days Before Expiration**. The default setting is 30 days. Click **Off** to specify that signing passwords do not expire.
    6. In the **Days to Prevent Password Reuse** area, enter the number of days that must pass before a user can reuse a signing password.
    7. In the **Days Required Between Password Changes** area, enter the number of days that must pass before a user can change a signing password again.
3. Click **Save Changes**.

Tip: Click**Reset** to return to the settings specified when you first opened the page.

3.6 Configuring notifications for expiring signing passwords

The Electronic Signatures signing password expiration notification settings are located on the **Configure Scheduled Activities** page found on the **Content Server Administration** page. When enabled, this functionality will run once a day, scanning all signing passwords to check how soon they will expire, and will send an email to users that meet the notification criteria. The settings are as follows:

- **Status**, set to **Enable** to perform the scan, or **Disable** to not perform the scan.
- **E-Mail Notifications**, specifies when users will receive the first email notification about the expiration of their signing password, and when they will to begin receiving daily notifications about the expiry of their signing password.

3.6.1 To configure the signing password expiration email notifications:

To configure the signing password expiration email notifications:

1. In the **Notification Administration** section of the **Content Server Administration** page, click the **Configure Scheduled Activities** link.
2. In the **Signing Password Expiration** section, do the following:
   a. In the **Status** area, click **Enable** or **Disable**.
   b. In the **E-mail Notifications** area, enter a number for the **Send first e-mail day(s)** and **Send daily e-mails starting day(s)** boxes.
3. Click **Submit**.

3.7 Administering Robot properties

Workflow creators add Electronic Signatures Robot steps to signing Workflows when they want to convert a Workflow Document to PDF format. Electronic Signatures Robot steps are powered by a renditioning engine, such as Blazon for Content Suite, which converts the Document and makes a PDF version available within the Workflow. For more information about Electronic Signatures Robot steps, see *OpenText Electronic Signatures - OpenText Content Server User Online Help (LLESESN-H-UGD)*.

3.7.1 Configuring the renditioning engine

Before Workflow creators can add Electronic Signatures Robot steps to Workflows, you must create the directories that the renditioning engine uses to render Documents to PDF format. A renditioning engine uses a watched (input) directory and a PDF (output) directory. It monitors the watched directory for new files, automatically converts those files to PDF format, and then places the PDF versions in the PDF directory.

Notes

- File names greater than 253 characters in length may cause problems for creating renditions, watermarking, and securing Documents. For long file names, you should configure an alternate processing directory on the **Electronic Signatures Settings** page.
- The Electronic Signatures Robot step will not complete when converting a web form to an HTML form if the Form Template and View names are 248 characters or longer. If the Form name is too long, the Workflow might not initiate.

You must create the watched and PDF directories on the system where your Content Server instance is installed. After you create the directories, you can share and map them on the server where the renditioning engine runs. You then configure the renditioning engine's input and output settings to point to the corresponding directories. For information about how to configure the renditioning engine's input and output settings, see the documentation that accompanies the renditioning engine.

After you point the renditioning engine to the watched and PDF directories, you configure Electronic Signatures to recognize the watched and PDF directories. You must also specify the MIME type of the Documents that you want the renditioning engine to convert and the number of attempts to pick up the rendered version of the Document.

Note: Although it is not mandatory, you may want to install Blazon for Content Suite on a remote server to reduce the load on the computer where Content Server runs.

To configure the renditioning engine

To configure the renditioning engine:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Robot** link.
2. In the **Watched Folder** section, do the following:
   a. In the **Directory Path** box, type the absolute path of the directory where the renditioning engine retrieves documents for conversion to PDF format.
   b. In the **Available** and **Selected** columns:
      i. In the **Available** column, select the MIME types that you want the renditioning engine to retrieve for conversion to PDF format.

      Tip: You can select multiple MIME types by holding **CTRL** while clicking your selections.
      ii. Click **Add** to add those selected MIME types to the **Selected** column.

      Tip: To remove MIME types, select them in the **Selected** column, and then click **Remove**.
   c. Optional Repeat the configuration process for any additional MIME types.

      To add a new watched folder, click **Add Watched Set**. If a watched folder can be deleted, **Delete** will appear in the next to that watched folder.
3. In the **PDF Folder** section, in the **Directory Path** box, type the absolute path of the directory where the renditioning engine deposits converted PDF files.
4. In the **Maximum Number of Attempts** section, use the **Number of Attempts** slider or enter a numerical value for conversion attempts.
5. Click **Save Changes**.

3.7.2 Working directory

Electronic Signatures uses a working directory to store temporary process files. This working directory will be used during signing, watermarking, and when securing documents. The temporary process files will be deleted when the process is complete. Electronic Signatures uses a default working directory: *<Content Server_home>*`/temp/esign`.

3.7.3 Watermark files

All watermark files need to be saved as `TYPE (UTF8)`. You must add a new line, `Encoding (UTF8)`, after the `TYPE (UTF8)` line in the watermark files.

Note: You must ensure that all watermark files include the lines:

```
Type (UTF8)
Encoding (UTF8)
```

3.8 Setting Electronic Signatures audit data

You will need to administer certain event types. Once you have set up the event types, you can query the information in the audit log, or selectively purge information from the audit log. For more information, see *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)*.

The following audit features are available for Electronic Signatures:

Setting up event type auditing

You can audit Electronic Signatures data in the same way you audit other Content Server items. Administering Electronic Signatures event types involves setting the types of events you want to audit, and then performing event type queries. For more information about administering event types, see *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)*.

When auditing Workflows, you have the option to display the user name in the audit trail. To ensure that the user name is displayed, you will need to configure the Workflow parameters. For more information about displaying the user name in the Workflow audit trail, see *OpenText Content Server Admin Online Help - Workflow Administration (LLESWFW-H-AGD)*. If the user name is set to be displayed, you can view the audit trail from the Workflow Map properties **Audit** tab. For more information about viewing Workflow properties, see *OpenText Content Server - Get Started (LLESRT-H-UGD)*.

The following table outlines which event types need to be set up before you can query Electronic Signatures event types.

Table 3-1: Electronic Signatures event audit data

Event type	Events to select	Description
Electronic Signatures Login Audit Data	Electronic Signatures - Failed Signing Login Attempt Electronic Signatures - Signing Login	Allows you to query successful and failed attempts for signing sign-in.

Event type	Events to select	Description
Log-in Audit Data	Failed Log-in Attempt Log-in	Allows you to query successful and failed attempts for Content Server system sign-in.
Electronic Signatures Settings	Electronic Signatures - Signed Electronic Signatures - Signed Version Electronic Signatures - Signing Rejected	Allows you to query successful and failed attempts for signing.
Electronic Signatures Configuration Settings	Configuration Changed	Allows you to display the user name and date of any changes made to the **Configure Electronic Signatures Settings** page.
Electronic Signatures Rendition Settings	Rendition Created Rendition Deleted	Allows you to query successful and failed attempts for creating renditions.
User Audit Data	Attributes Changed Membership Changed Permissions Changed	Allows you to query changes made to users, including Signing Authorities.
Group Audit Data	Members Changed Owner Changed	Allows you to query changes made to standard and signing groups.
Category Attribute Audit Data	Attributes Changed Category Added Category Removed	Allows you to query Category attribute changes made to Documents and Compound Documents.

3.8.1 To set audit event types

To set audit event types:

1. In the **Core System - Feature Configuration** section of the **Content Server Administration** page, click the **Event Auditing** link.
2. On the **Administer Event Auditing** page, click the **Set Auditing Interests** link.
3. On the **Set Auditing Interests** page, select the Electronic Signatures event types you want to record in the **Available** column, and click **Add** to move them into the **Selected** column. You can find the event types listed in "Electronic Signatures event audit data" on page 33.

4. Click **Save Changes**.

3.9 Setting Electronic Signatures error email recipients

Workflows sometimes experience errors, and it is important to specify the user or group to whom an error email will be delivered if such an event occurs. Error emails can be sent to any one or all of the following:

- An administrator
- The Master Manager user
- A group specified in the Workflow

3.9.1 To set recipient for Workflow error emails

To set recipient for Workflow error emails:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Settings** link.
2. In the **Miscellaneous** section, in the **Set Recipient for Workflow Error E-mails** area, click one of the following options:
   - **Administrator**
   - **Master Manager**

   Note: If the Master Manager user or group has not been defined in the Workflow, error emails will be sent to the administrator.
3. Click **Save Changes**.

3.10 Changing the signing font in Electronic Signatures

To display all fonts available for this Content Server instance, do one of the following:

- In Windows, open a command prompt, change directory to *<Content Server_home>*`\module\esign_16_2_8\dropin\stamppdfbatch` and then run the command: `stamppdfapp.exe -listfonts`
- In Solaris, open a command prompt, change directory to *<Content Server_home>*`/module/esign_16_2_8/dropin/stamppdfbatch` and then run the command: `./stamppdf -listfonts`

Tip: In the *<Content Server_home>*`\module\esign_16_2_8\dropin\stamppdfbatch` directory, you will find the `stamppdf.log` file that contains all fonts.

3.10.1 To change the signing font

To change the signing font:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Settings** link.
2. In the **Signing Settings** area, in the **Signing Font** box, enter the name of the font you want displayed.

   Notes

   - The default is `ArialMT`.
   - If an unavailable font is entered into the **Signing Font** box, no warning of an invalid font choice will display and signings will fail. Ensure that the font you enter is available.

3. Click **Save Changes**.

3.11 Electronic Signatures log files

When errors occur, you can access the Electronic Signatures log files to determine the source of the error. The Electronic Signatures log files are written to a directory named `esignlogs`, in the Content Server logs directory. To get the configured log path of the log folder, open the `opentext.ini` file, and look in the `[general] section` of the file. For example, `Logpath=C:\opentext\alpha\logs` in the`opentext.ini` file means that your Electronic Signatures logs will be available at `C:\opentext\alpha\logs\esignlogs`.

Table 3-2: Electronic Signatures log files

File name	Description
`AdminProcLog.txt`	Logs any errors that occur while running Appligent executables on the admin server. If log level is set to 2 or higher, Appligent commands will be logged.
`AgentErrorLog.txt`	Logs any errors that occur while running Electronic Signatures Agents.
`Applog.txt`	Logs any errors that occur while running `AppendPDFApp`. `AppendPDFApp` is from Appligent.
`EmailErrorLog.txt`	Logs any errors that occur while sending email to administrators or Workflow Managers detailing errors that occurred on a Robot step.
`FdfLog.txt`	Logs any errors that occur while running `FDFMergeApp`. `FDFMergeApp` is from Appligent.
`Generationlog.txt`	Logs any errors that occur during a Generation step.

File name	Description
`Getinfolog.txt`	Logs any errors that occur while running `APGetIinfoApp`. `APGetIinfoApp` is from Appligent.
`RenditionLog.txt`	Logs any errors that occur during a Robot step.
`SecLog.txt`	Logs any errors that occur while running `SecurSignApp`. `SecurSignApp` is from Appligent.
`SignLog.txt`	Logs any errors that occur during a signing step. It will log the name of the user performing the step and the reason for the error. Depending on the reason for the error, the user may have to look into different log files created. For example, `appLog.txt`, `fdfLog.txt`, or `StampLog.txt`.
`StampLog.txt`	Logs any errors that occur while running `StampPDFApp`. `StampPDFApp` is from Appligent.
`TimeLog.txt`	Logs any errors that occur if the `TmZoneApp.dll` does not find a valid value for the server's time zone.

3.12 Administering signing Workflow deletion

Users cannot delete signing Workflows by default, but this can be changed in the **Electronic Signatures Administration** area of the **Content Server Administration** page. If enabled, any Workflow with signatory steps can be deleted.

Caution

This feature may put you into non-compliance with your regulatory rules. Consult any regulatory rules that apply before enabling signing Workflow deletion.

Whenever this setting is changed, an entry is made in the audit log. The auditing event type is called *Electronic Signatures – Deletion of Signing Workflows Setting Changed*.

3.12.1 To enable deletion of signing Workflows

To enable deletion of signing Workflows:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Settings** link.
2. In the **Signing Settings** section, in the **Deletion of Signing Workflows** area, select the **Enable** check box.
3. Click **Save Changes**.

Note: Ensure you have reviewed the risks with performing this action before completing this procedure. For more information, see "Administering signing Workflow deletion" on page 37.

3.12.2 To disable deletion of Signing Workflows

To disable deletion of Signing Workflows:

1. In the **Electronic Signatures Administration** section of the **Content Server Administration** page, click the **Configure Electronic Signatures Settings** link.
2. In the **Signing Settings** area, in the **Deletion of Signing Workflows** area, clear the **Enable** check box.
3. Click **OK** and then click **Save Changes**.