OPENTEXT

MARCH 2013

OpenText Regulated Documents for the Life Sciences Industry:

21 CFR Part 11 Compliance

OpenText Regulated Documents helps organizations in the Life Sciences industry achieve compliance with the requirements of Rule 21, Code of Federal Regulations, Part 11, which is abbreviated as "21 CFR Part 11" or simply "Part 11." This paper discusses the requirements of rule 21 CFR Part 11 and describes how OpenText Regulated Documents, built on OpenText Content Server - the leading collaborative knowledge management software from OpenText, enables Life Sciences companies to comply with 21 CFR Part 11.

Contents

1.0 Introduction

All companies that develop new products are interested in reducing the time that it takes to get their products to market. For Life Sciences companies, the challenge of reducing time-to-market for new products is even greater than for other industries due to the strict regulatory environment in which they must operate.

Historically, Life Sciences companies have managed and tracked documents in paper format. The methods and practices for ensuring that the paper records included in submissions or maintained for possible inspection were authentic and unaltered were well established and well understood. Substituting electronic documents and signatures for paper required new procedures to insure authenticity, integrity and confidentiality.

The FDA requirements for certifying that electronic records and electronic signatures are trustworthy, reliable, and essentially equivalent to paper records and handwritten signatures are described in 21 CFR Part 11.

21 CFR Part 11 contains two major sections that contain requirements for:

- **Electronic Records**—defined as "any combination of text, graphics, data, audio, pictorial, or other information in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system."[1] (The rules apply to any records covered by FDA regulations that exist in an electronic form, including records that are required to be maintained whether they are submitted to the FDA or not.)
- **Electronic Signatures**—defined as "a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature."[2]

The determination of whether to use an electronic signature is up to an individual organization.

Clarifications:

- **Federal Register/Vol. 62, No 54/Rules & Regulations/Part 11, Section 11.3 (6) Electronic Record 21 CFR Part 11** applies to those records and signatures required by an FDA predicate rule, as well as to signatures that are not required, but that appear in required records.
- **Even though 21 CFR Part 11** applies to all FDA program areas, it does not mandate electronic record keeping. Rather, it describes the technical and procedural requirements that must be met if a submitting entity chooses to maintain records electronically and use electronic signatures.

[1] Federal Register/Vol. 62, No 54/Rules & Regulations/Part 11, Section 11.3 (6) Electronic Record
[2] Federal Register/Vol. 62, No 54/Rules & Regulations/Part 11, Section 11.3 (7) Electronic Signature

2.0 OpenText Enterprise Information Management Overview

OpenText is the leader in Enterprise Information Management (EIM). EIM enables organizations to grow the business, lower costs of operations, and reduce information governance and security related risks. OpenText focuses on the key drivers of business success to improve business insight, strengthen business impact, accelerate process velocity, address information governance and provide security.

OpenText Enterprise Content Management (ECM), an EIM offering, helps you manage information through its lifecycle, improve business productivity, mitigate risk, and control costs of growing volumes of content.

OpenText ECM software unites records management, archiving, search and eDiscovery to minimize organizational risk and cost, and maximize business insight and efficiency.

From information capture, to classification, management, storage, distribution, archiving, and disposition, ECM software manages the flow of information across the organization. Fast and seamless access from multiple environments—web, desktop, mobile, within business processes and applications—improves user productivity and organizational efficiency.

2.1 Enterprise Content Management Software Products

CONTENT MANAGEMENT	Manage and archive corporate content in a consistent and compliant manner with fully integrated records, metadata, archiving, and storage management services.
ARCHIVING	Meet compliance requirements, reduce storage and eDiscovery risks and costs, and maintain seamless access to content for business users.
RECORDS MANAGEMENT	Control risks and costs by managing the retention and disposition of content according to internal policies and external regulations.
EMAIL MANAGEMENT	Reduce costs and mitigate the risks of compliance and litigation concerning email content.
DATA AND CONTENT INTEGRATION	Intelligently consolidate and transform data and content throughout the entire information ecosystem to increase the business impact of your information and unify information channels across application boundaries.
LEGAL CONTENT MANAGEMENT (EDOCS)	Support business practices, proactive compliance and information governance needs throughout the matter lifecycle from client intake through to final disposition.
LEARNING MANAGEMENT	Successfully manage the learning process, reduce training costs and improve user satisfaction through support of independent learning styles.
CONTENT-CENTRIC APPLICATIONS	Provide the right task and resource support in your enterprise value chain while leveraging your secure ECM repository and other foundational infrastructure investments.

2.2 **OpenText Solutions for Pharmaceutical & Life Sciences**

Helping achieve compliant management of all electronic records and documents

Pharmaceutical and Life Sciences companies operate in a highly regulated environment with long product lifecycles. The operations are both data and document-intensive. Pharmaceutical product development can take up to 15 years and over $2 billion for a product to reach the market. Recent demands for increased public accountability against a trend of fewer new products and expiring patents are threatening traditional profitability and revenue growth. Life sciences departments must share key information with team members and make the best decisions possible based on all relevant information, while complying with government regulations including the US's 21 CFR Part 11 and conforming to industry standards such as GxP.

OpenText solutions for the Pharmaceutical and Life Sciences industries support critical processes where compliant management of all paper and electronic records and documents is essential. We recognize that these processes range from informal research collaborations to formal procedures like Standard Operating Procedure (SOP) review and approval, and that these processes may be limited to single departments, span your enterprise or even include alliance partners, contractors and consultants. Users can access a variety of interfaces ranging from email clients, Web browsers, as well as office and specialty applications, allowing them to work in the environment that is most natural to them.

OpenText solutions for Pharmaceutical and Life Sciences are based on a framework providing the right task and resource support for the processes in the industry's value chain.

3.0 Complying with 21 CFR Part 11

For Life Sciences companies that have chosen to maintain records and make submissions electronically, the challenge is to comply with 21 CFR Part 11 by ensuring that:

- The software products that they use function in a way that enables them to comply with the many requirements of 21 CFR Part 11
- They develop and follow SOPs that describe how to use software functionality in a way that is compliant with 21 CFR Part 11

The requirements of 21 CFR Part 11 are described in detail in the **"Appendix A: How OpenText Content Server Addresses 21 CFR Part 11,"** but the requirements of 21 CFR Part 11 for Life Sciences companies can be summarized as follows:

- Ensure the authenticity, integrity, and confidentiality of electronic records
- Generate accurate and complete copies of records for the FDA to inspect and review
- Ensure the security and easy retrieval of electronic records
- Ensure that only authorized individuals can access, manipulate, and electronically sign records
- Maintain a log of all changes made to electronic records throughout their lifecycle

- Record and store electronic signatures with the electronic records to which they have been applied
- Ensure that record processing steps are performed in the proper order
- Ensure that persons who develop maintain, or use the electronic record/electronic signing system are properly trained
- Ensure that individuals are accountable for actions initiated under their electronic signatures
- Maintain control over system documentation
- Establish and maintain SOPs regarding all of the above and other requirements

3.1 The OpenText Solution

OpenText Regulated Documents offering helps Life Sciences companies manage electronic records and signatures in compliance with 21 CFR Part 11 in the following ways:

- Through the capabilities of its OpenText Content Server, OpenText Electronic Signatures and other software products, which enable compliance with 21 CFR Part 11 requirements
- Through consulting services that help Life Sciences companies develop the policies, procedures, and best practices to ensure that OpenText software products are used in a 21 CFR Part 11- compliant manner

Regulated Documents enables Life Sciences companies to address not only their need for software that can be used in a Part 11-compliant way, but also to manage the SOPs that describe the procedures and best practices that must be followed to ensure 21 CFR Part 11 compliance. Electronic Signatures is a module specifically designed to address the access control and electronic signature requirements of 21 CFR Part 11.

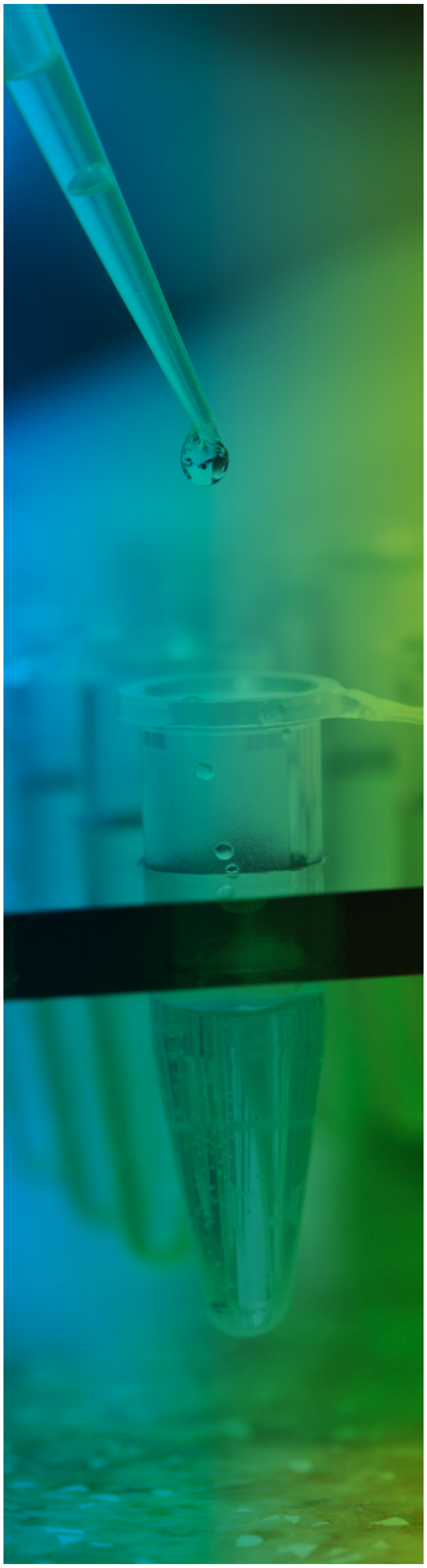
3.2 OpenText Content Server

Serving as the foundation of Regulated Documents, Content Server is a highly scalable, collaborative knowledge management application that allows organizations to store and manage a wide range of digital objects—from simple and compound documents, data records, molecular models, image and video files, to search queries and URLs—and provides controlled user access to these objects. All of the electronic records maintained by Life Sciences companies can be stored and managed in Content Server.

Content Server is ideal for managing unstructured electronic records in regulated industries, such as the pharmaceutical sector. The key features of Content Server for 21 CFR Part 11 compliance are:

- Secure repository for storing and distributing electronic records with full version control
- Web-based interface for team collaboration that is easy to access and deploy
- Security features such as password authentication and eight levels of permissions on document objects
- Ability to store custom metadata (such as signature information) with electronic records
- Ability to track the complete version and event history of electronic records, as well as to audit and report on all actions
- Workflow for automating and ensuring the integrity of electronic record review, approval, and signing processes

Content Server provides the ability to perform lifecycle management of all electronic content including Microsoft® Office files, XML files, emails, PDFs, CADs, multi-media, UTF-8 content, etc. This content is stored in the ECM repository, tracked, retained for its lifecycle and disposed of once the end of life is reached for that content. The electronic content can have metadata (data elements) associated with the content providing information about the content. For instance, is the content a Microsoft Word document or an email or an HR record, or an official record of the corporation, or an SOP document? Each of these items has a different lifespan and can be involved in very different business processes during their lifecycles. The access permissions on each of these items vary significantly as well. The ability to classify electronic content, control its access, manage it with defined processes (workflows), retain it for the appropriate length of time and then dispose of it in a legally defensible manner is a cornerstone of the content lifecycle management (CLM) solution. But CLM is not just about controlling and managing business content and the repositories where it resides. It is about understanding the relationship between people, processes and content in a corporation. It is also about documenting how content flows within and across departments, what systems it touches and what processes with which it is associated.



Content can be created from a variety of sources. All forms of data content can be managed as users typically work via their desktops in user-friendly applications such as Microsoft Office or Outlook or Lotus Notes. By logging into the ECM Suite through their preferred browser (Internet Explorer, Firefox, Safari), users can download, upload and edit content within the repository, with all content controlled by access permissions.

As content is received by the ECM repository, it is indexed, associated with any default metadata (categories) and stored in a repository location as specified by the user. Access permissions are also set according to the administrator-configured parameters and the location chosen. It is then exposed to a rich search engine that can perform searches against both the content data and the contents of the metadata using simple and complex full-text and Boolean search strings. The domain of the search can be limited to just a portion of the repository or it can span the entire repository. Through the use of federated searches, the search can be expanded to include file systems and other repositories. A search query can return exact matches or similar matches including "sounds like" search criteria. The results of both the search and the search template can be stored, as desired by the user. Additional searches refining the search template are also available. As with all content stored in the repository, access permissions control what content is returned as a result of a search. If a user does not have permission to see that specific content exists, it will not be shown in the search results. Content is also exposed to a powerful business process engine (workflows) that allow organizations to route documents through the various stages in the documents lifecycle. Approval, review, edits and comments are all possible steps along the workflow process.

As changes occur to content (new versions, edits, deletions) all actions are logged in an audit trail so accountability of all content is maintained across the repository. The system administrator can review this audit log as desired.

When an additional version of the same content are stored in the repository, a newer version is added and becomes the default version when the content is search, opened for viewing or opened for editing. However, previous versions, back to a configured maximum number of versions, are still available for comparisons or as a backup to be reverted if necessary. While content is stored in folders in the repository, users can create shortcuts from their personal repository workspaces to their favorite content or folders for faster access.

When content is added to the ECM repository, notifications can be sent out automatically as desired by users. For instance, a user can choose to be notified by email whenever a new item or version is added to a specific folder. They can choose to receive such a notification immediately, hourly or daily. As workflows process corporate data, users are always notified via an assignment list, and can also be notified via email, when a workflow step requires their participation. This notification can be a review, approval, electronic signature or just informing them that a specific action is needed. A deadline can be imposed and when the user exceeds that deadline, escalations can occur as well. The administrator can review the system-wide list of assignments and tasks and outstanding items are clearly flagged for review. The administrator can re-assign any task if, for instance, a user is out on holiday or otherwise unavailable.

It is also possible for individual users to manage proxy users for approvals while they will be unavailable. Users can easily choose any other user within the system to receive workflow notifications while they are unavailable, such as being out of the office on vacation.

Content can be added to the repository through both local and remote user action, bulk loading utilities or connectors that draw content from other repositories. Content can be kept on file storage or moved to the OpenText Archive Server which performs single-instance archiving, compression and encryption as desired. Storage via the Archive Server can be on disk or worm or optical media or magnetic tape. Content stored within the Archive Server is managed and accessed like all other repository content.

3.3 **Language Support**

Global companies demand localization of applications for their users. OpenText supports this requirement in both the user interface and metadata management. OpenText ECM code is fully internationalized and therefore can support any language. This internationalization has enabled localization into several languages including German, French, Japanese, Dutch, Spanish, Russian, Chinese, and Italian.

OpenText ECM Suite is internationalized and natively supports Unicode. Internationalization is a key requirement for each new product version and testing is part of the standard development process. The internationalization of the ECM Suite includes the following features and capabilities:

- The underlying repository supports Unicode (UTF-8), so no effort is needed to support different character encodings during the localization process.
- Text strings that appear in the GUI are stored in properties files. Online help files are UTF-8 encoded HTML files
- Multi-lingual full text and metadata searching are supported - Different regional options are supported (e.g. different date and time formats).
- Due to the solid internationalization of Content Server ECM, the actual localization is a straightforward process.

OpenText provides standard releases in the following languages: English, French, German, Spanish, Japanese, Chinese, Russian, and Italian. In addition, OpenText has also started a new strategy to engage reseller partners that localize products into languages specific to their regions.

To extend the languages supported out of the box, OpenText has developed the concept of a language pack. A language pack allows reseller partners that localize products into languages specific to their regions giving companies a truly global reach.

3.4 Accessing Content Server

Web Interface

Content Server provides a web-based interface to its repository and functions. This allows anyone, anywhere access to Content Server functionality. Being a web-based application reduces support requirements on IT, and gives users an easy and well understood tool for performing their daily tasks.

OpenText provides a web services interface to Content Server which offers specific support for both .NET and J2EE application servers. This allows customers to integrate Content Server content and functionality with other systems and web services. Web Services for OpenText uses standard protocols such as the Simple Object Access Protocol (SOAP) and Web Services Definition Language (WSDL).

Enterprise Connect

Open Text Enterprise Connect lets users access Content Server servers using Windows Explorer and Microsoft Outlook. Users can browse and search the Content Server repository, upload and download items using drag-and-drop functionality and work with Content Server items in a Windows Explorer view. In addition it provides integration with other desktop applications. Users can open and save Content Server items when working in popular desktop applications, such as Microsoft Word and Microsoft Excel. Content Server Email Integration works with Enterprise Connect to let users browse Content Server using Microsoft Outlook. Users can save email messages to Content Server using drag-and-drop and save email attachments with the email message or as separate documents.

Mobility

OpenText takes advantage of the productivity and efficiency made possible by today's mobile devices. Our mobile solutions provide your workforce with the ability to access and manage business content, keep workflow processes moving, and stay up-to-date with colleagues by using social collaboration capabilities within a single native application designed specifically for your ECM deployments.

By marrying your enterprise content management and mobility strategies, you can realize a higher return on investment (ROI) through increased user adoption of your content management systems that results from your workforce having meaningful mobile access to your enterprise. Furthermore, content chaos can be avoided by keeping content consistent across Web, desktop, and mobile environments.

Best of all, there is no longer a need to adopt a single device operating system support policy as OpenText supports all popular smartphone and tablet devices such as BlackBerry® and Apple iPhone® and iPad®. Now you can review, approve and electronically sign documents from your mobile device.

ERP

Content exists throughout the organization in variety of systems ranging from ECM repositories to file shares, and from email boxes to file system servers to ERP. Within the pharmaceutical industry content also resides in a number business applications including: quality systems, laboratory systems, and learning systems as examples.

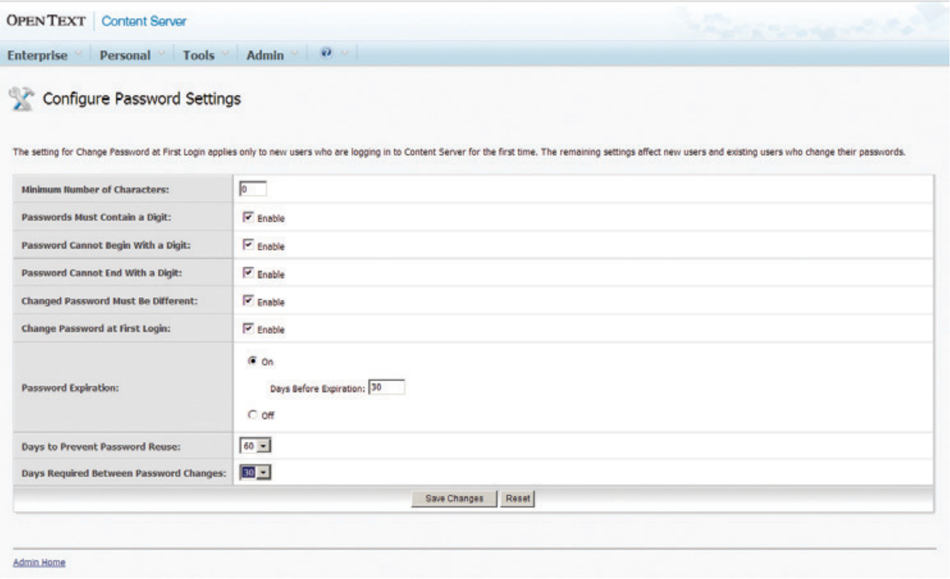
Content Server has integrations with many other leading applications such as SAP®, Oracle® J.D. Edwards, Oracle E-Business and Oracle PeopleSoft. Integrations with these leading ERPs allow users to access content managed by the Content Server directly from their application, reducing wasted time spent looking for documents.

3.5 User Authentication and Privileges

Content Server requires that each user be authenticated to the application prior to accessing any content or processes. Authentication can be directly from the application, through any LDAP compliant application such as Active Directory, or web access management application such as CA Siteminder. Log-in, log-out and failed log-in attempt event types can all be audited by Content Server.

Each username/password combination in Content Server is unique and can only be assigned to one individual at a time. To facilitate username and password changes, an internal system identification number is assigned that identifies the relationships between documents and user activity. The deletion of a username does not remove the unique userid, meaning that metadata, including the audit trail, remains intact.

When using the application to manage usernames, the Content Server Administrator can set specific rules for password creation, including password length, the presence of numeric digits, the password expiration period, requirement to change the password the first time that the user logs in, lockout after multiple failed access attempts, inactive session timeout, and more.



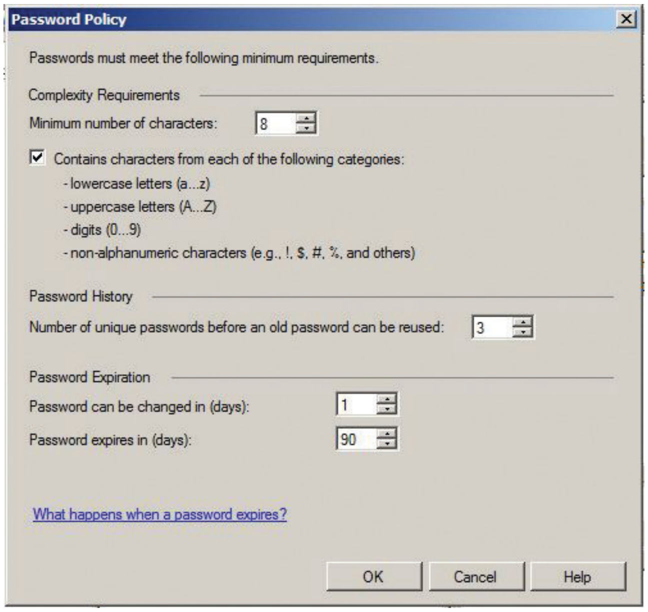
Configure Password Settings

The setting for Change Password at First Login applies only to new users who are logging in to Content Server for the first time. The remaining settings affect new users and existing users who change their passwords.

Minimum Number of Characters:	0
Passwords Must Contain a Digit:	☑ Enable
Password Cannot Begin With a Digit:	☑ Enable
Password Cannot End With a Digit:	☑ Enable
Changed Password Must Be Different:	☑ Enable
Change Password at First Login:	☑ Enable
Password Expiration:	● On Days Before Expiration: 30 ○ Off
Days to Prevent Password Reuse:	60
Days Required Between Password Changes:	30

PASSWORD CONTROLS SET BY THE CONTENT SERVER ADMINISTRATOR

When using OTDS to manage users in a non-synchronized capacity, the administrator can set specific rules for password creation, password expiration period, and uniqueness based on password history and enforce a password change the first/next time that the user logs in. Users are locked out after three failed access attempts and inactive session timeouts are configurable.



Passwords must meet the following minimum requirements.

Complexity Requirements

Minimum number of characters: 8

☑ Contains characters from each of the following categories:
- lowercase letters (a...z)
- uppercase letters (A...Z)
- digits (0...9)
- non-alphanumeric characters (e.g., !, $, #, %, and others)

Password History

Number of unique passwords before an old password can be reused: 3

Password Expiration

Password can be changed in (days): 1

Password expires in (days): 90

What happens when a password expires?

PASSWORD CONTROLS SET BY THE CONTENT SERVER ADMINISTRATOR

Content Server controls which operations can be performed in Content Server based on system-wide privileges and on object-specific permissions granted to users and/or groups. Based on the username by which a user logs in and on the groups of which the username is a member, Content Server displays only those items that a user has the permission to view. Similarly, Content Server displays only those functions that a user has the privilege to perform globally or the permission to perform on a given object or within a given container. Only the Content Server Administrator can set system-wide privileges, whereas object owners and other users with sufficient permissions can set permissions on individual objects.

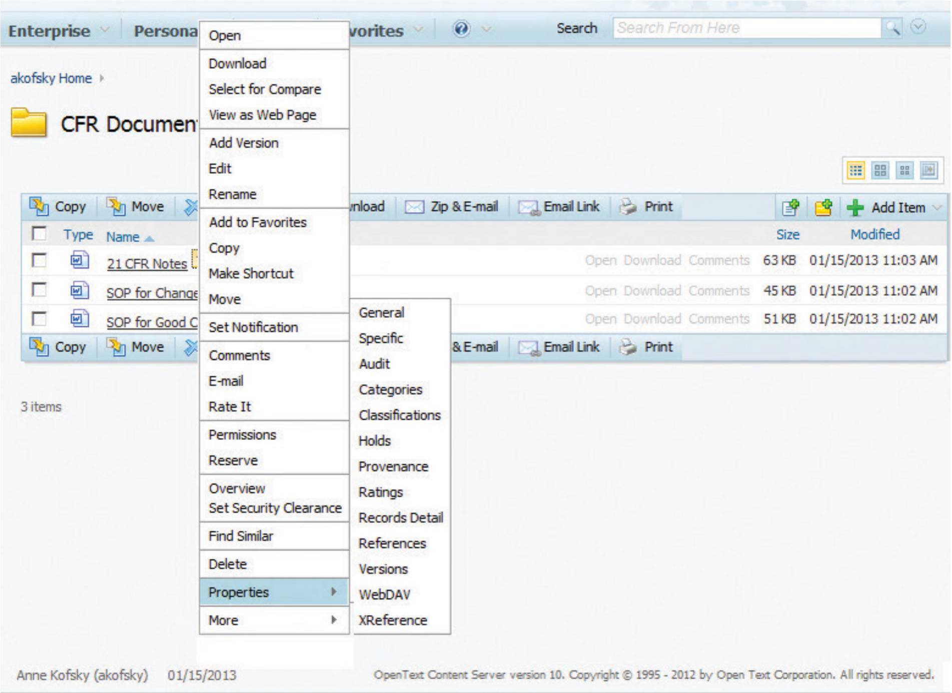
3.6 Document Management and Version Control

In Content Server, documents are not updated directly in the Content Server database. With correct privileges a user edits (checks out) the document, which opens it in its native application, modifies it, saves it, and then checks in the modified document to Content Server as a new version.

These operations do not overwrite previous versions, but instead add another copy (version) of the document to the repository. A document reserved (locked) by a given user cannot be updated (have a version added) by any other user until the first user unreserves (releases the lock) the document.

The complete set of functions available for a document object in Content Server is shown below. Depending on their access permissions for a given document, individual users may only be able to perform a subset of these functions.

DOCUMENT FUNCTIONS AVAILABLE IN CONTENT SERVER



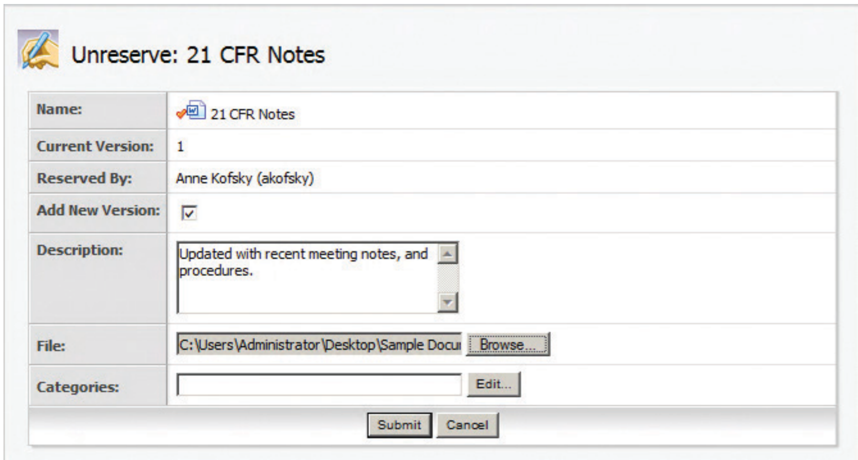
Type	Name		Size	Modified
	21 CFR Notes	Open Download Comments	63 KB	01/15/2013 11:03 AM
	SOP for Change	Open Download Comments	45 KB	01/15/2013 11:02 AM
	SOP for Good C	Open Download Comments	51 KB	01/15/2013 11:02 AM

Anne Kofsky (akofsky) 01/15/2013

OpenText Content Server version 10. Copyright © 1995 - 2012 by Open Text Corporation. All rights reserved.

When a user unreserves (checks in) a document and adds a new version, the user can enter a description identifying the nature of the change, as shown in the following image.

DESCRIBING REASON FOR NEW DOCUMENT VERSION

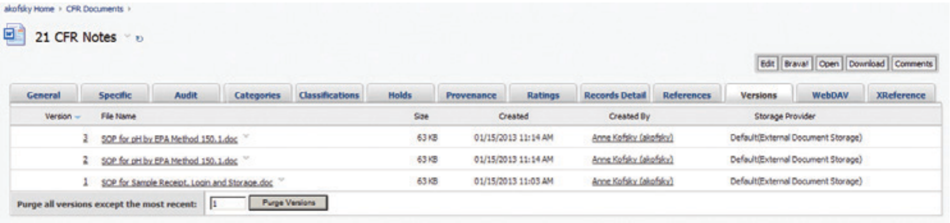


Unreserve: 21 CFR Notes

Name:	21 CFR Notes
Current Version:	1
Reserved By:	Anne Kofsky (akofsky)
Add New Version:	☑
Description:	Updated with recent meeting notes, and procedures.
File:	C:\Users\Administrator\Desktop\Sample Docu Browse...
Categories:	Edit...

When Enterprise Connect or WebDAV clients are used instead of a web browser, the download/check-out and upload/check-in steps are automated.

For each document object in the repository, Content Server supports either the retention of an unlimited number of versions or the setting of a maximum number of versions that can be retained. A specific version can be locked to prevent deletion. Purging versions of a Content Server object removes previous versions, beginning with the oldest version, up to the number of versions specified to be retained, with the exception of versions that have been locked.

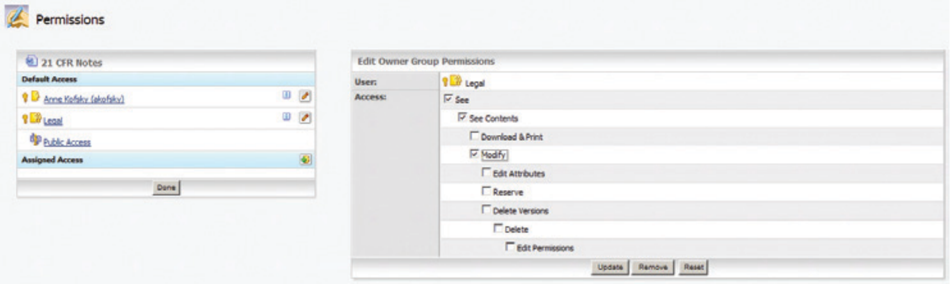


Version	File Name	Size	Created	Created By	Storage Provider
3	SOP for pH by EPA Method 150.1.doc	63 KB	01/15/2013 11:14 AM	Anne Kofsky (akofsky)	Default(External Document Storage)
2	SOP for pH by EPA Method 150.1.doc	63 KB	01/15/2013 11:14 AM	Anne Kofsky (akofsky)	Default(External Document Storage)
1	SOP for Sample Receipt, Login and Storage.doc	63 KB	01/15/2013 11:03 AM	Anne Kofsky (akofsky)	Default(External Document Storage)

Purge all versions except the most recent: 1

VERSIONS OF A DOCUMENT OBJECT IN OPENTEXT CONTENT SERVER

Each document in Content Server has eight levels of permission for each individual or group within the system. The document owner controls the access list and permissions and can grant the permission to modify permissions to other users or groups as desired. The Content Server Administrator can override permissions set by individual users.



21 CFR Notes

Default Access
- Anne Kofsky (akofsky)
- Legal
- Public Access

Assigned Access

Edit Owner Group Permissions

User: Legal

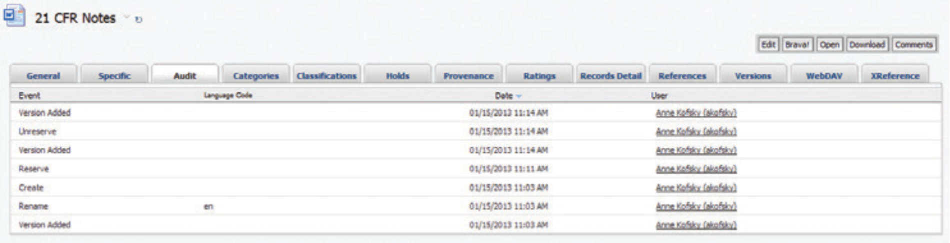
Access:
- ☑ See
  - ☑ See Contents
    - ☐ Download & Print
    - ☑ Modify
      - ☐ Edit Attributes
      - ☐ Reserve
      - ☐ Delete Versions
        - ☐ Delete
          - ☐ Edit Permissions

SETTING PERMISSIONS ON A OPENTEXT CONTENT SERVER DOCUMENT OBJECT

3.7 Event Auditing and Reporting

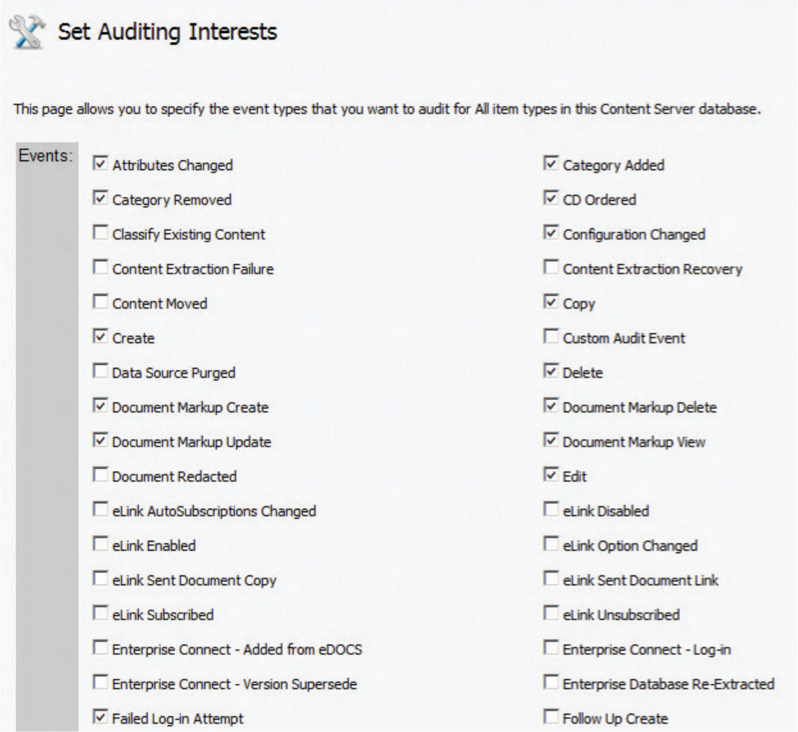
The Content Server Administrator can configure Content Server to create an audit trail log for each object type that logs a variety of events, including create, reserve, add-version, delete, rename, copy, and move events.

The audit log records the event type, the username of the person causing the event, and the date/time of the event. Anyone with the “See Content” permission can see the audit trail associated with a document, as shown in the following image.



Event	Language Code	Date	User
Version Added		01/15/2013 11:14 AM	Anne Kofsky (akofsky)
Unreserve		01/15/2013 11:14 AM	Anne Kofsky (akofsky)
Version Added		01/15/2013 11:14 AM	Anne Kofsky (akofsky)
Reserve		01/15/2013 11:11 AM	Anne Kofsky (akofsky)
Create		01/15/2013 11:03 AM	Anne Kofsky (akofsky)
Rename	en	01/15/2013 11:03 AM	Anne Kofsky (akofsky)
Version Added		01/15/2013 11:03 AM	Anne Kofsky (akofsky)

AUDIT TRAIL LOG OF AN OBJECT IN OPENTEXT CONTENT SERVER



Set Auditing Interests

This page allows you to specify the event types that you want to audit for All item types in this Content Server database.

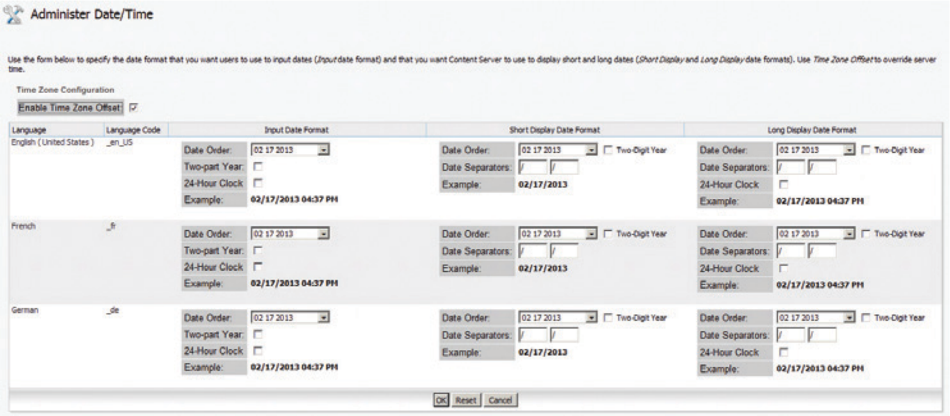
Events:

- ☑ Attributes Changed
- ☑ Category Added
- ☑ Category Removed
- ☑ CD Ordered
- □ Classify Existing Content
- ☑ Configuration Changed
- □ Content Extraction Failure
- □ Content Extraction Recovery
- □ Content Moved
- ☑ Copy
- ☑ Create
- □ Custom Audit Event
- □ Data Source Purged
- ☑ Delete
- ☑ Document Markup Create
- ☑ Document Markup Delete
- ☑ Document Markup Update
- ☑ Document Markup View
- □ Document Redacted
- ☑ Edit
- □ eLink AutoSubscriptions Changed
- □ eLink Disabled
- □ eLink Enabled
- □ eLink Option Changed
- □ eLink Sent Document Copy
- □ eLink Sent Document Link
- □ eLink Subscribed
- □ eLink Unsubscribed
- □ Enterprise Connect - Added from eDOCS
- □ Enterprise Connect - Log-in
- □ Enterprise Connect - Version Supersede
- □ Enterprise Database Re-Extracted
- ☑ Failed Log-in Attempt
- □ Follow Up Create

SPECIFYING AUDIT EVENTS TO BE LOGGED IN CONTENT SERVER

3.8 **Audit Event Configuration**

Content Server has a "Time Zone Offset" feature that the Content Server Administrator can enable if desired. When this feature is enabled, Content Server automatically calculates and displays the current time and the time of logged events according to the local time zone configured on each user's personal workstation. All dates shown on browsed content, audit trails and database query reports will display the date/time with the time zone offset calculated. By default, Content Server uses the local time configured on the computer hosting the server. Use of the 24-hour clock can also be selected.



Administer Date/Time

Use the form below to specify the date format that you want users to use to input dates (*Input date format*) and that you want Content Server to use to display short and long dates (*Short Display* and *Long Display* date formats). Use *Time Zone Offset* to override server time.

Time Zone Configuration

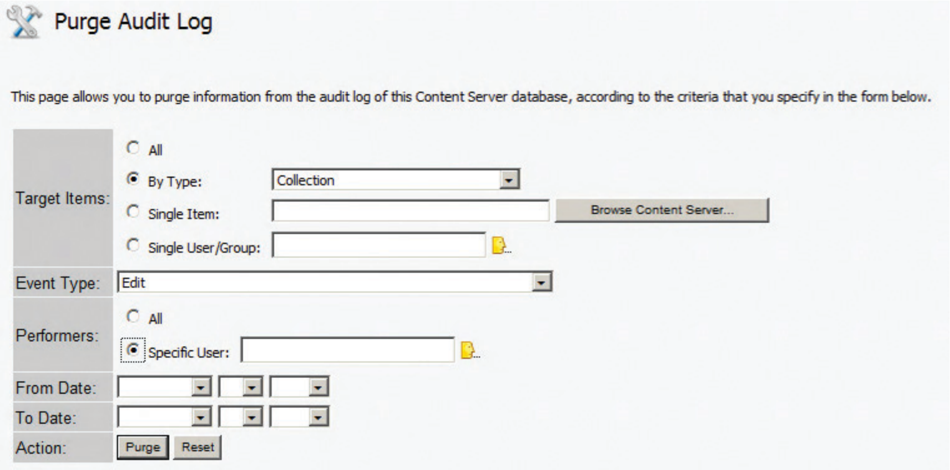
Enable Time Zone Offset: ☑

Language	Language Code	Input Date Format	Short Display Date Format	Long Display Date Format
English (United States)	_en_US	Date Order: 02 17 2013 Two-part Year: □ 24-Hour Clock □ Example: 02/17/2013 04:37 PM	Date Order: 02 17 2013 □ Two-Digit Year Date Separators: / / Example: 02/17/2013	Date Order: 02 17 2013 □ Two-Digit Year Date Separators: / / 24-Hour Clock □ Example: 02/17/2013 04:37 PM
French	_fr	Date Order: 02 17 2013 Two-part Year: □ 24-Hour Clock □ Example: 02/17/2013 04:37 PM	Date Order: 02 17 2013 □ Two-Digit Year Date Separators: / / Example: 02/17/2013	Date Order: 02 17 2013 □ Two-Digit Year Date Separators: / / 24-Hour Clock □ Example: 02/17/2013 04:37 PM
German	_de	Date Order: 02 17 2013 Two-part Year: □ 24-Hour Clock □ Example: 02/17/2013 04:37 PM	Date Order: 02 17 2013 □ Two-Digit Year Date Separators: / / Example: 02/17/2013	Date Order: 02 17 2013 □ Two-Digit Year Date Separators: / / 24-Hour Clock □ Example: 02/17/2013 04:37 PM

CONFIGURING TIME SETTINGS IN CONTENT SERVER

After audit trail events have been recorded, they cannot be modified. However, the Content Server Administrator can purge them if desired. OpenText recommends that policies be created to identify the circumstances, if any, under which audit records can be purged. The administrator can select to purge audit event records based on event type, username, or date range.

PURGING CONTENT SERVER AUDIT TRAIL LOGS



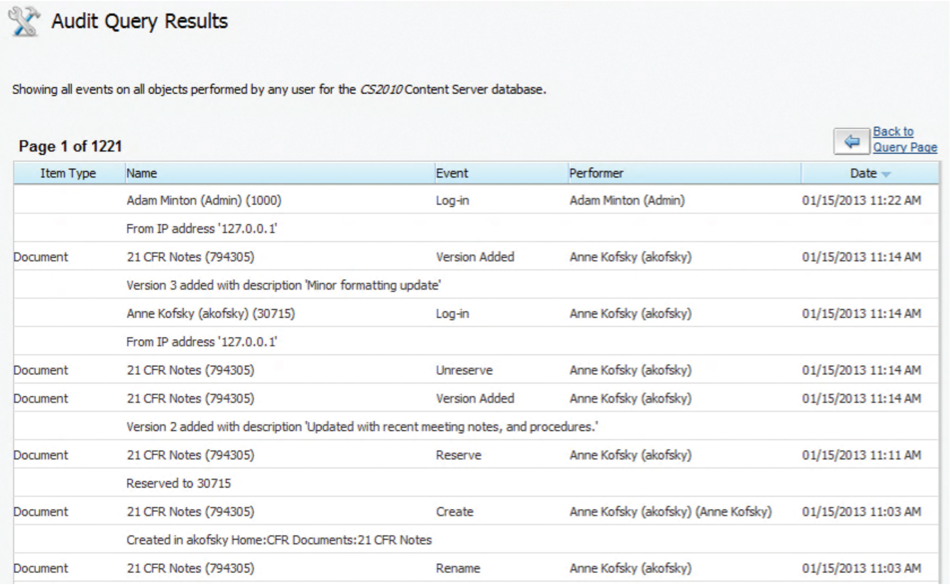
Purge Audit Log

This page allows you to purge information from the audit log of this Content Server database, according to the criteria that you specify in the form below.

Target Items:	○ All ● By Type: Collection ○ Single Item: [Browse Content Server...] ○ Single User/Group:
Event Type:	Edit
Performers:	○ All ● Specific User:
From Date:	
To Date:	
Action:	[Purge] [Reset]

The Content Server Administrator can generate a report of audit events at any time. The report can be filtered by username, object type, event type, and date range. The report can be saved in the Content Server repository as a controlled document.

AUDIT LOG QUERY REPORT



Audit Query Results

Showing all events on all objects performed by any user for the *CS2010* Content Server database.

Page 1 of 1221

Item Type	Name	Event	Performer	Date
	Adam Minton (Admin) (1000)	Log-in	Adam Minton (Admin)	01/15/2013 11:22 AM
	From IP address '127.0.0.1'			
Document	21 CFR Notes (794305)	Version Added	Anne Kofsky (akofsky)	01/15/2013 11:14 AM
	Version 3 added with description 'Minor formatting update'			
	Anne Kofsky (akofsky) (30715)	Log-in	Anne Kofsky (akofsky)	01/15/2013 11:14 AM
	From IP address '127.0.0.1'			
Document	21 CFR Notes (794305)	Unreserve	Anne Kofsky (akofsky)	01/15/2013 11:14 AM
Document	21 CFR Notes (794305)	Version Added	Anne Kofsky (akofsky)	01/15/2013 11:14 AM
	Version 2 added with description 'Updated with recent meeting notes, and procedures.'			
Document	21 CFR Notes (794305)	Reserve	Anne Kofsky (akofsky)	01/15/2013 11:11 AM
	Reserved to 30715			
Document	21 CFR Notes (794305)	Create	Anne Kofsky (akofsky) (Anne Kofsky)	01/15/2013 11:03 AM
	Created in akofsky Home:CFR Documents:21 CFR Notes			
Document	21 CFR Notes (794305)	Rename	Anne Kofsky (akofsky)	01/15/2013 11:03 AM

4.0 Electronic Signatures

4.1 Workflow

Content Server provides the ability to create workflows that automate business processes, such as document review and approval processes. Content Server workflows can be used to ensure that the sequence of events prescribed in the organizational policies and procedures for a given process are strictly observed.

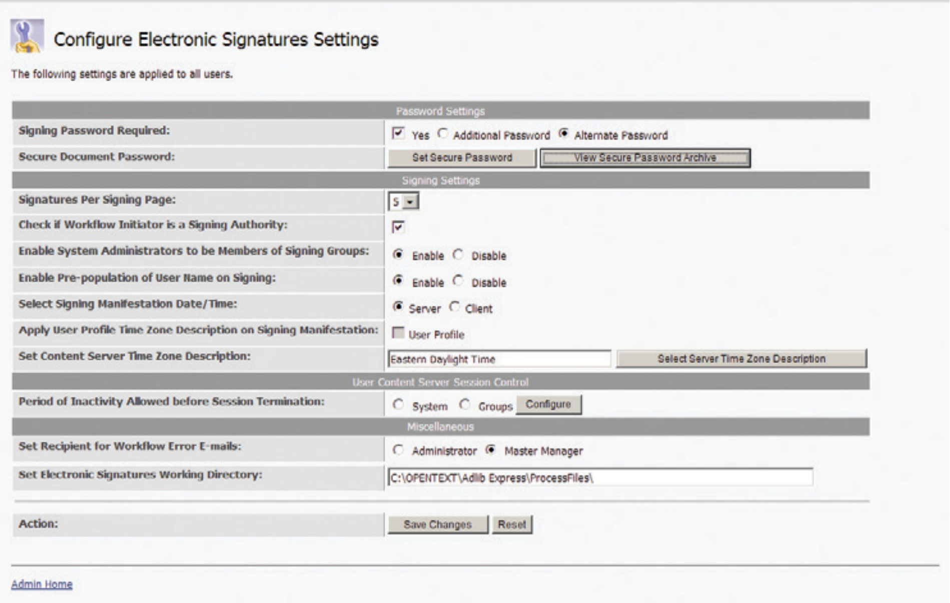
Each step in a workflow only becomes available to be performed after all prerequisite steps are completed. When a workflow task is ready to be performed by a Content Server user, an email is sent to the user and the task appears on the user's personal assignment list in the Content Server interface. The task for the next step in the workflow is not created until the user completes the task for the current step. In some cases, a workflow step can assign a task to a group of users, requiring only one, a majority, or all of them to perform the task before the next step is enabled.

4.2 OpenText Electronic Signatures

Electronic Signatures enhances access controls, audit and administration features, and adds electronic signature capabilities. Electronic Signatures enhancements can be used to manage a wide range of approval and change control processes in compliance with 21CFR Part 11. Electronic Signatures provides the following:

- Enhanced access control
- Visual indicator of current user
- Extended event auditing functions
- Electronic signature features, including Signing Authority administration, signature step in workflows, and signature audit trails
- Additional workflow features, including signing and PDF manipulation steps, username/password challenge for workflow steps, and the ability to initiate a workflow from a document
- Signing Administration features that can be assigned to specific, authorized users who then control the granting and revocation of signing rights to Content Server users
- Locking out users after a predetermined number of failed log-in attempts
- Monitoring of all log-in attempts whether successful or not
- Timing out inactive sessions

CONFIGURING ELECTRONIC SIGNATURE SETTINGS IN CONTENT SERVER



Configure Electronic Signatures Settings

The following settings are applied to all users.

Password Settings	
Signing Password Required:	☑ Yes ○ Additional Password ● Alternate Password
Secure Document Password:	Set Secure Password · View Secure Password Archive
Signing Settings	
Signatures Per Signing Page:	5
Check if Workflow Initiator is a Signing Authority:	☑
Enable System Administrators to be Members of Signing Groups:	● Enable ○ Disable
Enable Pre-population of User Name on Signing:	● Enable ○ Disable
Select Signing Manifestation Date/Time:	● Server ○ Client
Apply User Profile Time Zone Description on Signing Manifestation:	□ User Profile
Set Content Server Time Zone Description:	Eastern Daylight Time · Select Server Time Zone Description
User Content Server Session Control	
Period of Inactivity Allowed before Session Termination:	○ System ○ Groups · Configure
Miscellaneous	
Set Recipient for Workflow Error E-mails:	○ Administrator ● Master Manager
Set Electronic Signatures Working Directory:	C:\OPENTEXT\Adlib Express\ProcessFiles\
Action:	Save Changes · Reset

Admin Home

Current User Indicator

When the Electronics Signatures module is installed, every page displays the user's name as well as the date and time of the server running Content Server.

Extended Event Auditing Functions

Electronic Signatures extends Content Server audit functions to include changes to user profiles (including permissions) and group rights, as well as signing events.

To apply an electronic signature to a document in Content Server, a workflow with a signing step is used. When the document attached to the workflow step is signed, the signing event is recorded in the audit trail logs of both the copy of the document attached to the workflow and the original source document. This "signature" audit trail contains the user's name, title, the date and time of signing, and the meaning of the signing, and a link to the signing workflow.

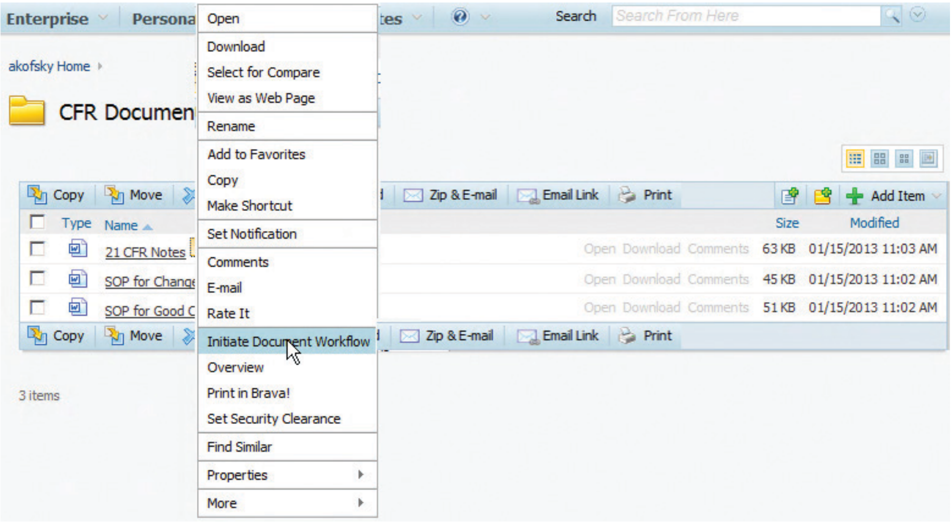
Additional Workflow Features

Electronic Signatures adds a number of features to Content Server Workflow to enable the application of electronic signatures to electronic documents in a manner compliant with 21 CFR Part 11. These additional workflow features include:

- Ability to initiate a workflow from the Function menu of a document object
- Ability to assign signing steps to individual users as well as groups
- Requirement of two-part authentication (username and password) at each signing for each signatory and an optional secondary signing password
- New signing and PDF manipulation steps
- Ability to maintain the association the signed copy of a document in a workflow and the original source document, as well as any renditions

The image below shows the Initiate Workflow function that Electronic Signatures adds to the Function menu of document objects in Content Server. This function enables users to initiate signing workflows from the document object that is to be reviewed and signed.

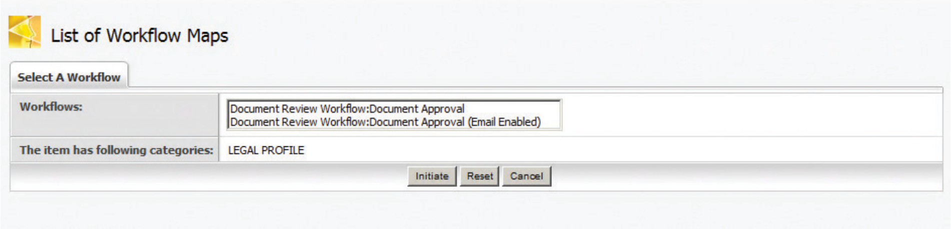
INITIATING A WORKFLOW FROM THE FUNCTION MENU OF A DOCUMENT



Type	Name		Size	Modified
	21 CFR Notes	Open Download Comments	63 KB	01/15/2013 11:03 AM
	SOP for Change	Open Download Comments	45 KB	01/15/2013 11:02 AM
	SOP for Good C	Open Download Comments	51 KB	01/15/2013 11:02 AM

After selecting the Initiate Workflow function, the user is prompted to select the approval workflow to which they want to submit the document. A copy of the document from which the workflow was initiated is automatically added to the work package that is routed through the workflow.

SELECTING AN APPROVAL WORKFLOW

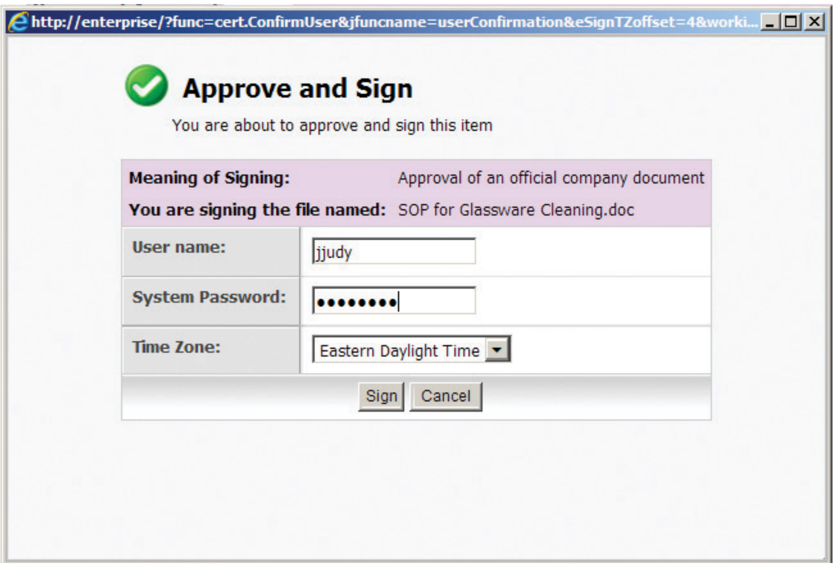


List of Workflow Maps

Workflows: Document Review Workflow:Document Approval
Document Review Workflow:Document Approval (Email Enabled)

The item has following categories: LEGAL PROFILE

“Approval” steps in a workflow imply the application of an approval signature to the document. Approval steps indicate the meaning of the signing event and force the performer to select one of the disposition options for the document, which are either to “approve and sign” or “reject” the document. To ensure than only the authorized individual can apply their signature, the step performer is required to re- authenticate themselves by re-entering their username and password as shown in the image below. The workflow designer also has the option of requiring the signing step performer to enter a special “signing password” for added security.



http://enterprise/?func=cert.ConfirmUser&jfuncname=userConfirmation&eSignTZoffset=4&worki...

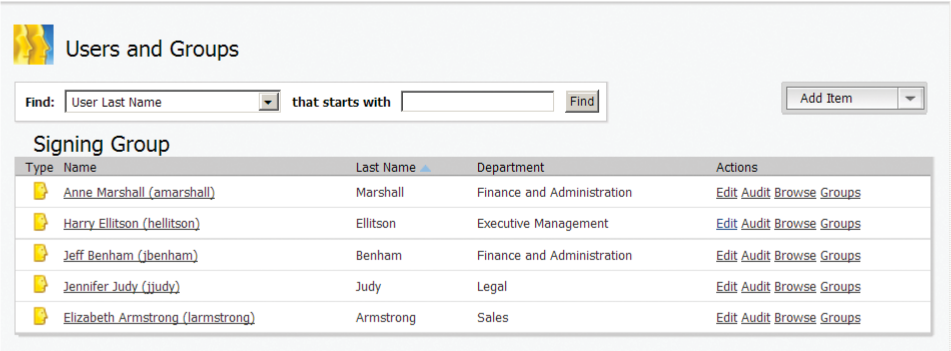
Approve and Sign

You are about to approve and sign this item

Meaning of Signing:	Approval of an official company document
You are signing the file named:	SOP for Glassware Cleaning.doc
User name:	jjudy
System Password:	••••••••
Time Zone:	Eastern Daylight Time

APPROVAL STEP SHOWING DISPOSITION OPTIONS AND PASSWORD CHALLENGE

Electronic Signatures restricts the signing of electronic records to authorized individuals. When a workflow designer is selecting users and or groups to perform a signature approval step, the designer is prompted to select only authorized users and groups as shown in the image below. For more information about the administration of signing authorities, see “Signing Authority Administration.”



Users and Groups

Find: User Last Name that starts with

Signing Group

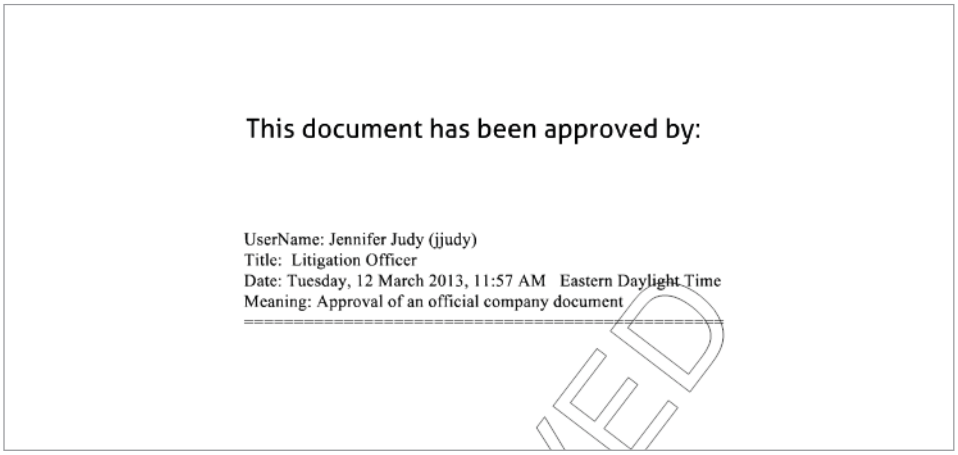
Type	Name	Last Name	Department	Actions
	Anne Marshall (amarshall)	Marshall	Finance and Administration	Edit Audit Browse Groups
	Harry Ellitson (hellitson)	Ellitson	Executive Management	Edit Audit Browse Groups
	Jeff Benham (jbenham)	Benham	Finance and Administration	Edit Audit Browse Groups
	Jennifer Judy (jjudy)	Judy	Legal	Edit Audit Browse Groups
	Elizabeth Armstrong (larmstrong)	Armstrong	Sales	Edit Audit Browse Groups

AUTHORIZED SIGNING GROUP USER LIST

In addition to the signing step, Electronic Signatures also provides a “PDF manipulation” step that allows automated changes to be made to PDF documents, including:

- Generation of a PDF rendition of Microsoft Word and other document formats prior to signature application
- Addition of a signature page (to which information about each signing event is added), that is selected from available templates, to a PDF rendition of the document being signed
- Modification of PDF security settings on a signed PDF rendition
- Addition of watermarks to a signed PDF rendition

The image below shows an example of a signature page that can be added to the PDF rendition of a signed document in a PDF manipulation step.



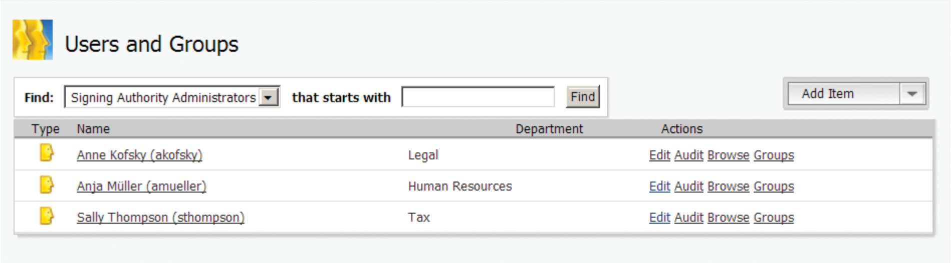
This document has been approved by:

UserName: Jennifer Judy (jjudy)
Title: Litigation Officer
Date: Tuesday, 12 March 2013, 11:57 AM Eastern Daylight Time
Meaning: Approval of an official company document
==

SIGNATURE PAGE ADDED TO THE PDF RENDITION OF A SIGNED DOCUMENT

Signing Authority Administration

Electronic Signatures adds a mechanism to Content Server for administering which users and groups have the authority to apply electronic signatures to documents in the signing step of a workflow. To enable the application of electronic signatures, the Content Server Administrator adds at least one user as a Signing Authority Administrator as shown in the image below.



Users and Groups

Find: Signing Authority Administrators that starts with [Find] [Add Item]

Type	Name	Department	Actions
	Anne Kofsky (akofsky)	Legal	Edit Audit Browse Groups
	Anja Müller (amueller)	Human Resources	Edit Audit Browse Groups
	Sally Thompson (sthompson)	Tax	Edit Audit Browse Groups

EDITING THE SIGNING AUTHORITY ADMINISTRATORS

Only users who are Signing Authority Administrators can create groups of Content Server users who are allowed to approve and sign documents in the signing step of a workflow.

Signing Authority Administrators themselves are not allowed to perform the signing step of a workflow. This prevents a Signing Authority Administrator from improperly granting signing authority to themselves when they are not authorized to have such authority. Members of an organization's quality control, security, or human resource departments would typically perform this administration function. As a further safeguard, a user with Content Server Administration privileges cannot add him/herself as a Signing Authority Administrator.

5.0 Summary

Coordinating and streamlining the efforts of research and development, production, distribution and marketing, while achieving regulatory compliance, are challenges that face Life Sciences organizations today. The opportunity to cut costs and reduce dependency on paper processes is of enormous benefit. 21 CFR Part 11 is a key regulation to which Life Sciences companies must conform if they want to take advantage of electronic records and electronic signatures.

The regulations in 21 CFR Part 11 seek to reduce fraud by ensuring that electronic signatures and records are as reliable as their traditional paper versions. Content Server is a solution that allows companies to closely adhere to these regulations.

Life Sciences organizations can rely on Content Server to perform the following functions in a manner that is compliant with the requirements in 21 CFR Part 11:

- Store and access documents for review
- Deliver information about clinical trials
- Track regulatory applications
- Manage records
- Communicate and assign tasks
- Monitor research and development
- Control workflows and processes
- Store and manage changes to SOPs

6.0 Appendix A - How OpenText Regulated Documents Addresses 21 CFR Part 11

Regulated Documents addresses each of the various requirements of 21 CFR Part 11 either by:

- Functionality contained in the core Content Server product
- Functionality contained in Regulated Documents bundle which includes:
  - Electronic Signatures (eSign)
  - XML Workflow Extensions
  - XML Workflow Interchange
  - Controlled Viewing & Printing
- Other means such as functionality contained in other OpenText products

The table below summarizes how Regulated Documents addresses each of the requirements of 21CFR Part 11, by indicating whether the requirement is satisfied by the core Content Server product, by the Regulated Documents module, or by some other software or service from OpenText.

Subsequent sections of this appendix contain more detailed descriptions of how Regulated Documents addresses 21 CFR Part 11 requirements.

21 CFR PART 11 SECTION	ADDRESSED?	ADDRESSED BY	SEE PAGE
REQUIREMENTS FOR CLOSED SYSTEMS			
11.10 (a) – Validation	■	Policies and procedures	25
11.10 (b) – Inspection	■	OpenText Content Server	25
11.10 (c) – Protection	■	OpenText Content Server Records Management module	26
11.10 (d) – Security	■	OpenText Content Server, OpenText Electronic Signatures, and OpenText Directory Services (OTDS), Controlled Viewing and Printing	26
11.10 (e) – Audit	■	OpenText Content Server, Controlled Viewing and Printing	27
11.10 (f) – Operational	■	OpenText Content Server	27
11.10 (g) – Authority	■	OpenText Content Server and OpenText Electronic Signatures	28
11.10 (h) – Device	■	OpenText Content Server and OpenText Electronic Signatures	28
11.10 (i) – Personnel	■	OpenText on-site audit	29
11.10 (j) – Policies	■	Policies and procedures	30
11.10 (k) – Documentation	■	Policies and procedures	30
REQUIREMENTS FOR OPEN SYSTEMS			
11.30 – Authenticity	■	OpenText Directory Services module (OTDS)	30-31
11.30 – Integrity	■	OpenText Content Server	30-31
11.30 – Confidentiality	■	Secure Sockets, Firewalls	30-31
11.30 – Digital Signature	■	Available through 3rd party module	30-31

21 CFR PART 11 SECTION	ADDRESSED?	ADDRESSED BY	SEE PAGE
REQUIREMENTS FOR SIGNATURE MANIFESTATIONS			
11.50 (a) – Signing	■	OpenText Electronic Signatures	31
11.50 (b) – Display/Print	■	OpenText Electronic Signatures	32
11.70 – Linking	■	OpenText Electronic Signatures	33
REQUIREMENTS FOR ELECTRONIC SIGNATURES			
11.100 (a) -Uniqueness	■	Policies and procedures	33
11.100 (b) -Verification	■	Policies and procedures	33
11.100 (c) -Certification	■	OpenText Electronic Signatures	34
11.200 (a) (1) (i) -Signature	■	OpenText Content Server	34
11.200 (a) (1) (ii) -Signing	■	OpenText Content Server and OpenText Electronic Signatures	34
11.200 (a) (2) and (3) – Identity	■	OpenText Content Server andOpenText Electronic SIgnatures	35
11.200 (b) – Biometrics	Not applicable		
11.300 (a) -Uniqueness	■	OpenText Content Server	36
11.300 (b) -Passwords	■	OpenText Content Server	36
11.300 (c) -Lost codes	■	OpenText Content Server	36
11.300 (d) -Attempts	■	OpenText Electronic Signatures	36
11.300 (e) -Devices	Not applicable		

6.1 **Addressing Requirements for Electronic Records (Subpart B)**

6.1.1 Controls for Closed Systems (Section 11.10)

This section describes how Regulated Documents addresses the controls that Life Sciences companies must put in place for “closed systems,” which are environments in which the persons who are responsible for the content control system access. An example of a closed system would be an information system that is contained within an organization’s local area network or intranet.

These controls require that “Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.”

The subsequent sub-sections describe the specific requirements of Section 11.10 and how Content Server addresses the requirements.

REQUIREMENT 11.10 (A)

Description of Requirement

Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

How OpenText Regulated Documents Addresses Requirement

In deploying Content Server, OpenText recommends that an organization implement policies and procedures that include a periodic audit of the production system to ensure accuracy, reliability, and consistent intended performance in the installed, active environment. OpenText can assist in the development of such policies and procedures, as well as in system configuration, to ensure that the system is optimally configured and used in a way that complies with 21 CFR Part 11.

Content Server provides a comprehensive auditing function that tracks creation, modification, and deletion of records identifying both user and date of action. No alteration to records can be accomplished without an audit trail entry being created.

REQUIREMENT 11.10 (B)

Description of Requirement

The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.

How OpenText Regulated Documents Addresses Requirement

Content Server stores records (documents or files) in their native format as binary objects. Objects stored in Content Server can be opened individually with the application that was used for their creation, such as Microsoft Word, or using another application that can view their content. Content Server also includes conversion filters for over 200 file formats that convert Microsoft Word and other document types to HTML on the fly for viewing in the browser via the Content Server web interface.

Content Server allows you to grant secure, read-only access to FDA staff so that they can review and inspect records as appropriate. Read-only accessed is granted not only to the documents themselves, but also to:

- Associated system metadata such as the owner, file description, and permissions
- Audit trail events such as record creation, modification, or deletion
- Specific user-assigned (custom) attributes entered along with the document, such as document type or retention period

Records can be exported and provided to the FDA as requested in one of the following ways:

- As documents in their native formats
- As PDF renditions
- As part of an XML export data stream

REQUIREMENT 11.10 (C)

Description of Requirement

Protection of records to enable their accurate and ready retrieval throughout the records retention period.

How OpenText Regulated Documents Addresses Requirement

OpenText recommends that organizations develop policies and procedures covering document (file) retention (how long a document should be maintained) and disposition (what is done with the document at the end of its lifecycle). The policy should include specific rules for deleting and purging documents at the end of their lifecycle. OpenText can assist in the development of these policies and procedures, as well as in system configuration. OpenText can provide backup and recovery scenarios that are specific to an organization's platform and deployment and customize them as necessary.

Content Server does not contain an archiving mechanism. All records (documents) and associated audit trails, system metadata and user-defined attributes are available for retrieval until they are deleted from the Content Server repository. Custom attributes can be used to classify each document, such as indicating whether it is a vital record or general business record. If desired, the Records Management module can be added to provide tighter controls on document retention and disposition.

For each object in the repository, Content Server supports either the retention of an unlimited number of versions or the setting of a maximum number of versions that can be retained. A specific version can be locked to prevent deletion. Purging versions of a Content Server object removes previous versions, beginning with the oldest version, up to the number of versions specified to be retained, with the exception of versions that have been locked.

Records Management by OpenText delivers complete lifecycle management for corporate records and information holdings, in paper or electronic format.

REQUIREMENT 11.10 (D)

Description of Requirement

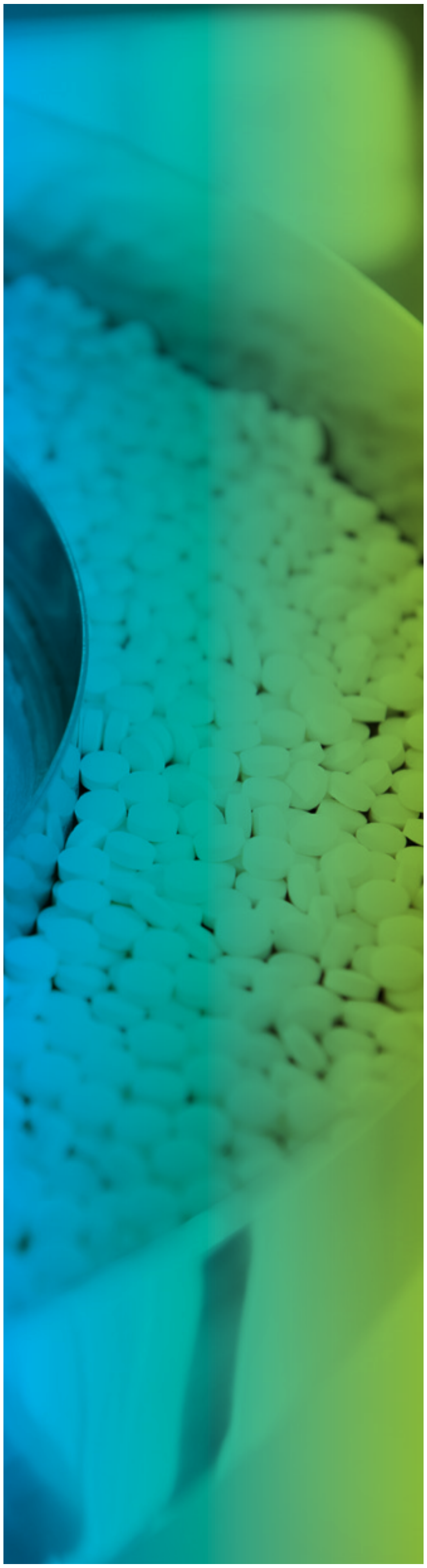
Limiting system access to authorized individuals.

How OpenText Regulated Documents Addresses Requirement

As described in **"3.5 User Authentication and Privileges"**, Content Server requires that each user log in with a username and password to gain access to the system. When the user specifies their password, it is encrypted using a one-way algorithm and stored in the database. When the user logs in, Content Server verifies the password entered. It encrypts the password using the same algorithm and compares the encrypted password with the stored version. The encrypted password cannot be decrypted.

The Content Server Administrator is normally responsible for setting up user access. OpenText recommends that an organization implement policies and procedures to control the circumstances under which system access is granted. For example, Content Server can be configured to require the user to follow specific rules for password creation, including password length, the presence of numeric digits, the password expiration period, and the requirement to change the password the first time that the user logs in.

As described in **"4.2 OpenText Electronic Signatures"**, the Electronic Signatures module enables the Content Server Administrator to configure Content Server to lock out a user after a specified number of unsuccessful log-in attempts. This feature minimizes the opportunity for persons attempting to masquerade as a valid user. Electronic Signatures also allows the Content Server Administrator to configure the system to log a user out after a specified period of inactivity to protect against use of the system by unauthorized individuals.



At any point in time, each combination of username and password is unique within the Content Server system. To facilitate username and password changes, an internal system identification number is assigned that identifies the relationships between documents and user activity. The deletion of a username does not remove the unique userid, meaning that metadata remains intact.

Electronic Signatures monitors and logs all access attempts. It records username used, the date and time of the attempt, and whether there was success or failure. The log file can be exported to a Microsoft Excel spreadsheet to allow for further analysis prior to purging.

REQUIREMENT 11.10 (E)

Description of Requirement

Use of secure, computer-generated time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

How OpenText Regulated Documents Addresses Requirement

OpenText Content Server addresses this requirement through:

- Its ability to generate detailed audit trails of events on Content Server objects. For more information about Content Server event auditing features, see **"3.7 Event Auditing and Reporting."** For information about how Electronic Signatures enhances Content Server auditing features, see **"Extended Event Auditing Functions" (Section 4.2).**
- Its document management and version control features. For more information, see **"3.6 Document Management and Version Control."**
- Electronic Signatures current user indicator. For more information, see **"Current User Indicator" (Section 4.2).**
- OpenText Controlled Viewing and Printing provides a full audit trail of all controlled print jobs including who requested the print, a reason for the requested print, and the call back status of a each document.

REQUIREMENT 11.10 (F)

Description of Requirement

Use of operational system checks to enforce permitted sequencing of steps and events as appropriate.

How OpenText Regulated Documents Addresses Requirement

Content Server ensures version control by enforcing that a document reserved (locked) by a given user cannot be updated (have a version added) by any other user until the first user unreserves (releases the lock) the document. In other words, Content Server enforces that the "unreserve" step must precede the "add version" step to ensure that document modifications occur sequentially.

As described in **"4.1 Workflow"**, Content Server also provides the ability to create workflows that automate business processes, such as document review and approval processes. Content Server workflows can be used to ensure that the sequence of events prescribed in the organizational policies and procedures for a given process is strictly observed.

Each step in a workflow only becomes available to be performed after all prerequisite steps are completed. When a workflow task is ready to be performed by a Content Server user, the task appears on the user's personal assignments list in the Content Server interface. The task for the next step in the workflow is not created until the user completes the task for the current step. In some cases, a workflow step can assign a task to a group of users, requiring only one, a majority, or all of them to perform the task before the next step is enabled.

REQUIREMENT 11.10 (G)

Description of Requirement

Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

How OpenText Regulated Documents Addresses Requirement

Content Server addresses this requirement through:

- System-wide object creation privileges granted to users via their individual usernames or via groups of which they are members. For more information, see **"3.5 User Authentication and Privileges."**
- Object-specific permissions that grant users and/or groups the right to perform certain functions on the object. For more information, see **"3.6 Document Management and Version Control."** Double password authentication for users performing signing steps in workflows. For more information, see **"Additional Workflow Features" (Section 4.2).**
- A special mechanism for administering which users are authorized to apply electronic signatures. For more information, see **"Signing Authority Administration" (Section 4.2).**

REQUIREMENT 11.10 (H)

Description of Requirement

Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

How OpenText Regulated Documents Addresses Requirement

When a user logs in to Content Server, an encrypted "cookie" is created, saved by the Web browser on user's local workstation, and retained until the browser is closed. This cookie is presented to the Web server as identification each time the user clicks a link during the current session. The web server decrypts the cookie, which is used by Content Server to verify the username and password and the permissions that the user has for each object.

The Electronic Signatures module enhances this security by enabling the Content Server Administrator to set a timeout for inactivity. If a user logs in to Content Server and then performs no action on their workstation for longer than the set period of time, Content Server will challenge the user to re-enter their username and password. This prevents an unauthorized individual from using the workstation of another user to gain access to restricted information if the user leaves their workstation unattended for an extended period of time.

OpenText recommends that organizations develop policies and procedures for protecting user workstations from unauthorized access. For example, the use of a timeout for inactivity should be enforced.

REQUIREMENT 11.10 (I)

Description of Requirement

Determination that persons who develop, maintain, or use electronic record/electronic signature systems has education, training, and experience to perform their assigned tasks.

How OpenText Regulated Documents Addresses Requirement

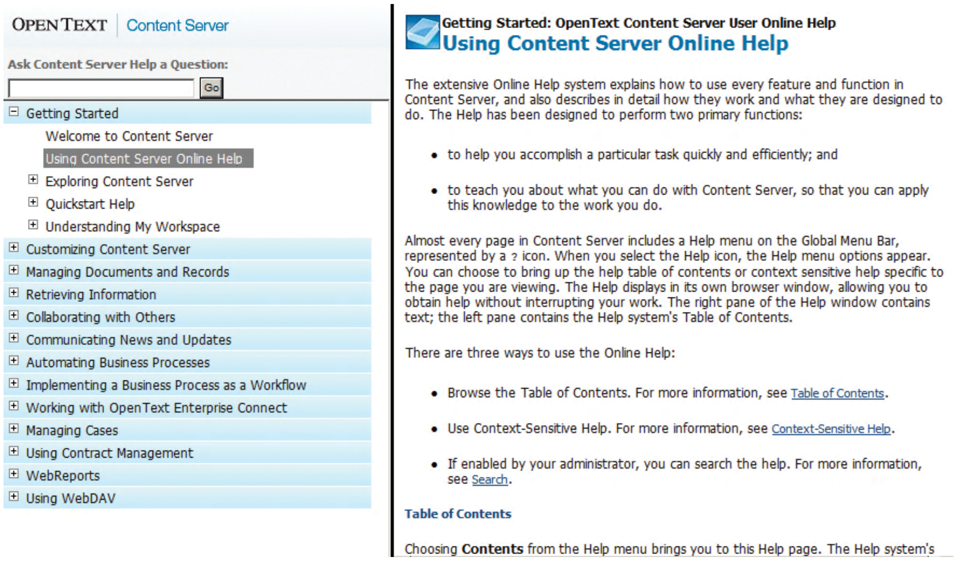
As part of its deployment of Content Server, an organization can perform a quality assurance audit of OpenText development processes, procedures and standards, and can review the history of employee training. OpenText will provide access to personnel and documentation as necessary to support the following quality assurance activities:

- Organizational structure, history, and background
- Personnel qualifications and training
- Security
- Disaster recovery and backup/restore procedures
- Software quality control
- Change management
- Documentation
- Software development methodology, processes, and standards

An organization should ensure that training is provided for employees who will use the Content Server system. OpenText provides a selection of classroom and Web-based training for both end users and administrators. There are general, basic, and end-user courses as well as specialized courses covering such things as system design, administering users and groups, advanced workflows, forms, and LiveReports.

A complete list of available courses can be found at:
http://www.opentext.com/2/global/services/ls-learning-services-home.htm

The Content Server system contains a comprehensive online help facility including a table of contents menu, context-sensitive instructions, and full search capabilities.


OPENTEXT | Content Server
Ask Content Server Help a Question:
Go
⊟ Getting Started
Welcome to Content Server
Using Content Server Online Help
⊞ Exploring Content Server
⊞ Quickstart Help
⊞ Understanding My Workspace
⊞ Customizing Content Server
⊞ Managing Documents and Records
⊞ Retrieving Information
⊞ Collaborating with Others
⊞ Communicating News and Updates
⊞ Automating Business Processes
⊞ Implementing a Business Process as a Workflow
⊞ Working with OpenText Enterprise Connect
⊞ Managing Cases
⊞ Using Contract Management
⊞ WebReports
⊞ Using WebDAV

Getting Started: OpenText Content Server User Online Help

Using Content Server Online Help

The extensive Online Help system explains how to use every feature and function in Content Server, and also describes in detail how they work and what they are designed to do. The Help has been designed to perform two primary functions:

- to help you accomplish a particular task quickly and efficiently; and
- to teach you about what you can do with Content Server, so that you can apply this knowledge to the work you do.

Almost every page in Content Server includes a Help menu on the Global Menu Bar, represented by a ? icon. When you select the Help icon, the Help menu options appear. You can choose to bring up the help table of contents or context sensitive help specific to the page you are viewing. The Help displays in its own browser window, allowing you to obtain help without interrupting your work. The right pane of the Help window contains text; the left pane contains the Help system's Table of Contents.

There are three ways to use the Online Help:

- Browse the Table of Contents. For more information, see Table of Contents.
- Use Context-Sensitive Help. For more information, see Context-Sensitive Help.
- If enabled by your administrator, you can search the help. For more information, see Search.

Table of Contents

Choosing **Contents** from the Help menu brings you to this Help page. The Help system's

OPENTEXT CONTENT SERVER'S ONLINE HELP VIEWER

REQUIREMENT 11.10 (J)

Description of Requirement

The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

How OpenText Regulated Documents Addresses Requirement

As part of its deployment of Content Server, OpenText recommends that an organization develop policies and procedures covering the actions that administrators and end users must perform in the Content Server system. For administrators, policies and procedures should be developed for system-related actions such as user and group management, password management, and audit trail configuration and purging. For end users, policies and procedures should be developed for actions such as object creation, reserve/unreserve, and review and approval. OpenText can assist in the development of these policies and procedures as well as in system configuration.

REQUIREMENT 11.10 (K)

Description of Requirement

Use of appropriate controls over systems documentation including:

1. *Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.*
2. *Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.*

How OpenText Regulated Documents Addresses Requirement

As part of its deployment of Content Server, OpenText recommends that an organization develop policies and procedures covering the control of system operational documentation, system maintenance schedules, and software upgrade activities. Content Server itself is an excellent tool for controlling systems documentation.

6.1.2 Controls for Open Systems (Section 11.30)

This section describes how Regulated Documents addresses the controls that Life Sciences companies must put in place for "open systems," which are environments that are not controlled by persons who are responsible for the content of electronic records that are on the system. An example of an open system is the Internet.

Description of Requirement

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of receipt.

How OpenText Regulated Documents Addresses Requirement

As part of its deployment of Content Server, OpenText recommends that an organization implement usage policies and procedures to satisfy this requirement. Content Server provides user authentication, data integrity, and confidentiality as follows:

- **Authentication—**System access is controlled through the use of usernames and passwords. For more information, see the response to Requirement 11.10 (d). It is also possible to utilize Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory identification and authentication services with OpenText Directory Services . A server running one of these directory services performs user identification and authentication before passing the request to the server.
- **Integrity—**It is impossible to overwrite an existing object using the OpenText Content Server system. A user with appropriate permissions may only add a new version, either directly or through the reserve/unreserve process. The ability to delete an object can be strictly controlled through the use of object permissions.
- **Confidentiality—**To ensure confidentiality, OpenText recommends that Content Server be deployed in a secure communications network employing the Secure Sockets Layer (HTTPS) security mechanism, which encrypts the data stream between the browser and the server. Firewalls and proxy servers can be used to limit access to a specific, predefined set of users and IP addresses. Within Content Server, each document object has eight levels of access permissions inherited from its container object. The owner of an object (or other authorized user) can modify the permissions to restrict access to confidential records. For more information, see the response to Requirement 11.10 (g).
- **Digital Signatures—**This functionality is not currently available in the core product, but OpenText partners are offering Digital Signature functionality as an add-on to Content Server.

6.1.3 Requirements for Signature Manifestations (Section 11.50)

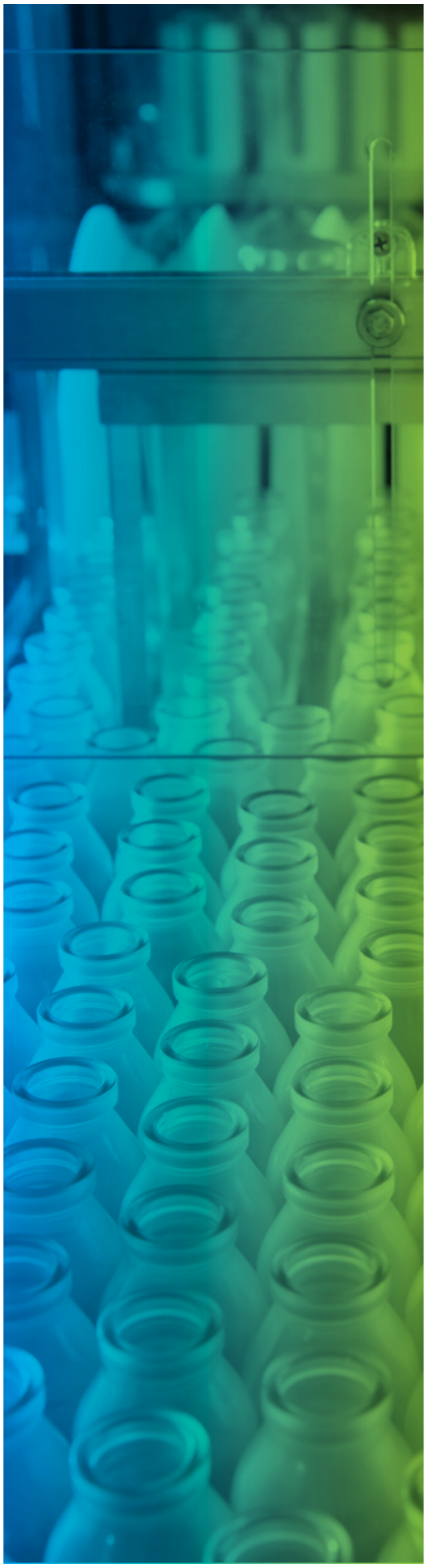
This section of 21 CFR Part 11 requires signature manifestations to contain information associated with the signing of electronic records.

REQUIREMENT 11.50 (A)

Description of Requirement

Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

1. *The printed name of the signer;*
2. *The date and time when the signature was executed; and*
3. *The meaning (such as review, approval, responsibility or authorship) associated with the signature.*



[3] The OpenText Directory Services module provides synchronization and authentication with LDAP, Windows NTLM, or Windows Active Directory central directory services, to provide single log- in access for network users.

How OpenText Regulated Documents Addresses Requirement

The Electronic Signatures module uses workflows to enable the signing/approving of electronic records. Workflow designers can create workflow maps that allow a user to submit a document to a signing step for approval, such as the sample SOP approval shown in **"Additional Workflow Features" (Section 4.2).**

The **"Additional Workflow Features" (Section 4.2)** also describes how a user can initiate a workflow from the Function menu of a document object and select a workflow, such as a document review workflow, to which to submit the document for approval.

The workflow designer can associate attributes and permissions with "document review" steps to:

- Request the user to indicate that they have read the document.
- Allow the user to add comments about the document.
- Allow for the review task to be delegated to another user.

"Approval" steps in a workflow indicate the meaning of the signing event and force the performer to select one of the disposition options for the document, which are either to "approve and sign" or "reject" the document. The performer is also required to re-authenticate themselves by reentering their username and password and by optionally entering a special signing password.

As described in **"Extended Event Auditing Functions" (Section 4.2),** when the document attached to the workflow is signed, the signing event is recorded in the audit trail logs of both the copy of the document attached to the workflow and the original source document. This "signature" audit trail contains the user's name, title, the date and time of signing, and the meaning of the signing, and a link to the signing workflow.

As described in **"Signing Authority Administration" (Section 4.2),** the Electronic Signatures module enhances Content Server by making it possible to restrict the list of users who are allowed to sign documents using a signature step in a workflow. Only users or groups that have been designated as signing authorities can be selected as performers of signing steps in a workflow.

REQUIREMENT 11.50 (B)

Description of Requirement

The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of electronic record (such as electronic display or printout).

How OpenText Regulated Documents Addresses Requirement

The Electronic Signatures module provides the ability to convert a document to PDF prior to the signing step to enable the information about the signing event to be added directly to the document on an additional page. The signing information is also linked to the document as metadata. When the user clicks the Approve and Sign button, the user's name, title, the date and time, and the meaning of the signing are "stamped" onto the signing page such as the example shown in **"Additional Workflow Features" (Section 4.2).** The signing page is a predefined customizable template that is associated with the workflow map from which approval workflow instances are initiated.

6.1.4 Requirements for Signature/Record Linking (Section 11.70)

This section of 21 CFR Part 11 requires that signatures be linked with records and that the signature cannot be removed from the record.

Description of Requirement

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

How OpenText Regulated Documents Addresses Requirement

Content Server with the Electronic Signatures module installed provides comprehensive audit trails of user activity linking the electronic signature to the document as described in the response to Requirement 11.50 (b) (Appendix B). This signing metadata associated with the document cannot be removed or overwritten. The creation of PDF files with appended signing pages and appropriate security ensures that the signatures cannot be removed, copied, or transferred.

6.2 Addressing Requirements for Electronic Signatures (Subpart C)

General Signature Requirements (Section 11.100) - The section of 21 CFR Part 11 specifies general requirements for electronic signatures.

REQUIREMENT 11.100 (A)

Description of Requirement

Each electronic signature will be unique to one individual and shall not be reused by, or reassigned to, anyone else.

How OpenText Regulated Documents Addresses Requirement

As part of its deployment of Content Server, OpenText recommends that an organization implement policies and procedures to ensure that a given username is assigned to only one individual, that each individual sets their own password at the first log-in, and that each individual agrees not to divulge their password under any circumstances. For more information, see the response to **Requirement 11.10 (d).**

REQUIREMENT 11.100 (B)

Description of Requirement

Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such signature, the organization shall verify the identity of the individual.

How OpenText Regulated Documents Addresses Requirement

As part of its deployment of Content Server, OpenText recommends that an organization implement policies and procedures to ensure that usernames are assigned to individuals with proper authorization and approval from their superiors.

REQUIREMENT 11.100 (C)

Description of Requirement

Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency [FDA] that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signature.

How OpenText Regulated Documents Addresses Requirement

The Electronic Signatures module is used to identify a group of users in an organization who have signing authority as described in previous sections of this paper. A Content Server report can then be generated to provide the FDA with a list of the users that are authorized to apply electronic signatures. A Content Server workflow map can be designed to manage this process and generate the appropriate letter(s) to be sent to the FDA. The letter(s) would attest to the legally binding equivalence of users and their electronic signatures.

6.2.1 Electronic Signature Components and Controls (Section 11.200)

This section of 21 CFR Part 11 outlines the requirements for electronic signatures not based on the use of biometrics, which would include OpenText Regulated Documents.

REQUIREMENT 11.200 (A)

Description of Requirement

11.200(a) Electronic signatures that are not based upon biometrics shall:

11.200 (A) SUB-REQUIREMENT	HOW OPENTEXT REGULATED DOCUMENTS ADDRESSES REQUIREMENT
11.200 (a) (1): Employ at least two distinct identification components such as an identification code and password.	Content Server utilizes a combination of username and password as the two components of the electronic signature. For more information, see the response to **Requirement 11.10 (d)**
11.200 (a) (1) (i): When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual	Content Server has this facility. The user logs in with both username and password once per session and then reenters the password when challenged to authenticate again during an approval step in a workflow. For more information, see the response to **Requirement 11.50 (b)**
11.200 (a) (1) (ii): When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	Content Server with the Electronic Signatures module installed requires that users who are actively signing documents must enter both their username and their password to re-authenticate themselves.

11.200 (a) (2): Be used only by their genuine owners; and	A user must be logged into the system to change his/her password. If a user forgets his/her password or there have been illegal attempts to log in, the administrator can change the password so that the user can once again access the system. The user can be forced to select a new password upon first login after reset. For more information, see the response to **Requirement 11.10(d).** I most organizations, users' workstations are configured with an inactivity screen that starts after a fixed period and locks the computer until the correct login credentials are entered. Content Server with Electronic Signatures module installed has the ability to automatically log out inactive user, as described I the response to **Requirement 11.10 (d).**
11.200 (a) (3): Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals	A user must be logged into the system to change his/her password. If a user forgets his/her password or there have been illegal attempts to log in, the administrator can change the password so that the user can once again access the system. The user can be forced to select a new password upon first login after reset. For more information, see the response to **Requirement 11.10(d).** In most organizations, users' workstations are configured with an inactivity screen that starts after a fixed period and locks the computer until the correct login credentials are entered. Content Server with Electronic Signatures module installed has the ability to automatically log out inactive user, as described I the response to **Requirement 11.10 (d).**

REQUIREMENT 11.200(B)

Description of Requirement

Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

How OpenText Regulated Documents Addresses Requirement

Content Server does not currently support electronic signatures based on biometrics.

6.2.2 Controls for Identification Codes/Passwords (Section 11.300)

This section of 21 CFR Part 11 covers controls that must be in place to ensure security and integrity when using electronic signatures based on identification codes and passwords.

Description of Requirement

Persons who use electronic signatures based upon identification codes in combination with passwords shall employ controls to ensure their security and integrity.

Such controls shall include:

11.300 SUB-REQUIREMENT	HOW OPENTEXT REGULATED DOCUMENTS ADDRESSES REQUIREMENTS
(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	The Server system ensures that each username is unique.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	The Content Server Administrator can configure OpenText Content Server or OpenText Directory Services so that all user passwords expire after a fixed period.
(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	Content Server allows usernames and/or passwords to be revoked and replaced at any time by an authorized system administrator.
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Content Server with the Electronic Signatures module installed has the ability to monitor log-in attempts for detection of misuse, as described in the response to **Requirement 11.10 (d).**
(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	This requirement is not applicable to Content Server.

For more information about using OpenText Content Server in the pharmaceutical industry, visit our Web site at **www.opentext.com**