Title 21 CFR Part 11 User Guide

Introduction

This document describes functionalities within EKP which are related to Title 21 CFR Part 11. (For the sake of brevity, we will use the shorthand "CFR" when referring to "Title 21 CFR Part 11".) It outlines steps administrators need to make in EKP in order for the system to support CFR compliance. There will follow descriptions of various enhancements added into the system which make it comply with CFR regulations.

This document discusses CFR from system implementation stand point only and does not explain other procedural aspects of CFR compliance.

Please note that you will need a CFR Installation Pack to enable this functionality in EKP.

Title 21 CFR Part 11

Title 21 CFR Part 11 of the Code of Federal Regulations deals with the Food and Drug Administration (FDA) guidelines on electronic records and electronic signatures in the United States. Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable and equivalent to paper records.

For clients wishing to submit electronic evidence to FDA, they must have the appropriate policies, procedures, and technical controls in place to be Part 11 compliant. This involves audits, system validations, audit trails, electronic signatures, and documentation for software and systems that are involved in the processing of data as part of their business practices and product development – including their learning management system.

Of particular relevance to EKP on a technical level are Part 11's Subpart B on Electronic Records and Subpart C on Electronic Signatures. Here we map the requirements to specific features of EKP, where applicable. A requirement may be reliant on EKP or on some external procedure, or on a combination of both.

Subpart A--General Provisions	**EKP Functionality**

Sec. 11.1 Scope.

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b)This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

(f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.
[62 FR 13464, Mar. 20, 1997, as amended at 69 FR 71655, Dec. 9, 2004]

Sec. 11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

Sec. 11.3 Definitions. (a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part. (b) The following definitions of terms also apply to this part: (1)*Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)). (2)*Agency* means the Food and Drug Administration. (3)*Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable. (4)*Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system. (5)*Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. (6)*Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. (7)*Electronic signature* means 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. (8)*Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark. (9)*Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.	
Subpart B---Electronic Records	**EKP Functionality**
Sec. 11.10 Controls for closed systems.	
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. Such procedures and controls shall include the following:	
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	EKP implements auditing, at the database level via database table triggers, on data pertaining to course set-up, exam set-up, learner transcripts and learner exams. Whenever an insert, update or deletion is carried out on one of audited database tables, an entry is automatically created in the corresponding audit history table, recording what has changed, when it changed and who carried out the change.
(b) 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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	EKP has a comprehensive set of standard reports and also a Report Wizard function for creating custom reports. The reports can be exported in HTML, CSV, Excel and, where appropriate, PDF formats.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	
(d) Limiting system access to authorized individuals.	Using EKP requires a user ID and password. These credentials are validated at login. Subsequently these credentials are requested at critical points in the system through electronic signature prompts.

(e) 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.	EKP implements auditing, at the database level via database table triggers, on data pertaining to course set-up, exam set-up, learner transcripts and learner exams. Whenever an insert, update or deletion is carried out on one of audited database tables, an entry is automatically created in the corresponding audit history table, recording a copy of the new data, the current date and time, and who carried out the change. As the audit history data is only ever added to and never updated or deleted, it is always possible to see previously recorded information.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The order in which courses are taken can be enforced either by setting course prerequisites or through the use of the EKP learning type of Learning Program. A Learning Program would consist of a set of courses and the ordering in which these are taken can be enforced.
(g) 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.	EKP allows user roles to be set up, each having its own set of access controls. These then permit particular users to use certain functions within EKP and limit other users from using them. At critical points within the system, e.g. updating course set-up information, an electronic signature prompt would appear. This requires the user to input his user ID, password and to specify a meaning for the electronic signature, e.g. authorship, edit, etc. The electronic signature data is then stored against the updated data.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	
(j) 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.	
(k) 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.	
Sec. 11.30 Controls for open systems.	
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 their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	External systems can currently interact with EKP via the EKP API. Its use should be disabled so that the system remains closed.
Sec. 11.50 Signature Manifestations.	
(a)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. (b)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 the electronic record (such as electronic display or printout).	The electronic signature information can be viewed in a number of appropriate locations, e.g. a Learning Object's e-signature can be viewed in the Catalog Editor, and also in selected reports.
Sec. 11.70 Signature/record linking.	

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.	An electronic signature of a user contains the user's unique user ID, added automatically by the system. As a user cannot be deleted in a CFR-enabled instance of EKP, and the user ID cannot be changed, the link between an electronic signature and its executor's user ID cannot be broken.
Subpart C--Electronic Signatures	**EKP Functionality**
Sec. 11.100 General requirements.	
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Each EKP user's user ID is a unique identifier and therefore no two users' electronic signature can be the same. It is a business process to ensure that one user's ID is not reused or reassigned to someone else. EKP can ensure that a user ID cannot be changed and that it cannot be physically deleted and then re-created for use by someone else.
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency 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 signatures.	
(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	
(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	
Sec. 11.200 Electronic signature components and controls.	
(a) Electronic signatures that are not based upon biometrics shall:	
(1) Employ at least two distinct identification components such as an identification code and password.	EKP employs a unique user ID and a password as a user's credentials
(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 electronic 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.	Both the session login and the electronic signatures carried out during the session require both the user's user ID and password.
(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.	Should the user's session time-out through inactivity, the user is required to login again using both user ID and password. The time-out period is configurable in EKP.
(2) Be used only by their genuine owners; and	
(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.	
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	EKP currently does not support electronic signatures based upon biometrics. This can be implemented as and when required.
Sec. 11.300 Controls for identification codes/passwords.	
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:	
(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.	Since every user in EKP has a unique user ID, this guarantees the uniqueness of user ID and password combinations in the system.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	EKP can force the user to change their password periodically. The password change interval is configurable.
(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.	Functionality exists within EKP to allow a user's password to be reset and a temporary password to be sent to the user's registered email address.
(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.	When the number of consecutive failed login attempts reaches a specified limit, the user's account becomes suspended to prevent further login attempts. In such a situation, the system administrator must be notified before the user's account can be made active again.
(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.	EKP currently does not support the use of tokens or cards for identification purposes. This can be implemented as and when required.

EKP CFR Compliance

EKP 6.3 contains various new functionalities to support CFR compliance.

Auditing

All changes made to sensitive data are now audited in the database along with information on the type of change, who made the change and when. Types of changes include any creation, update and deletion of sensitive data. Following are the list of entities that are audited categorized by their functional area.

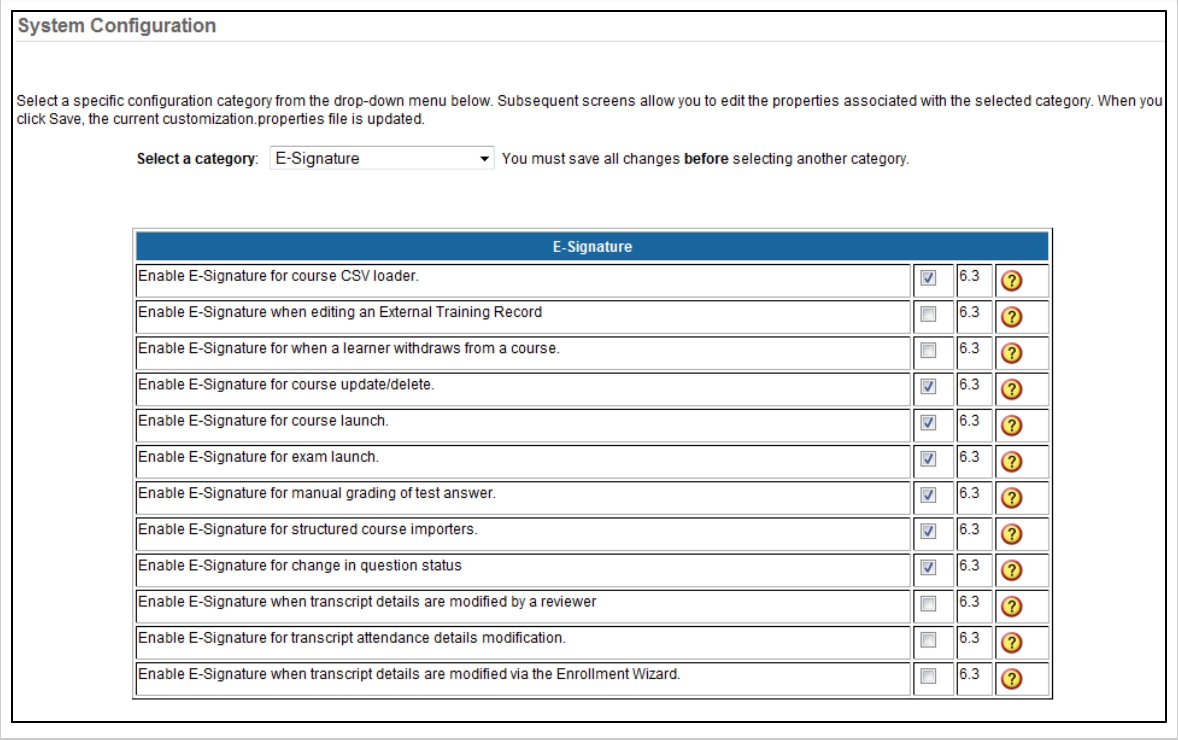
Cources, Sessions and Modules	Questions	Courseware
Learning Object	Question Attributes	Courseware Launch Options
Course Audience	Question Properties	Courseware Content Object
Course Auto-enroll	Single Choice Question	Courseware Content Item
Course Contact List	True or False Question	SCORM Sequencing
Course Details	Matching Question	SCORM Sequencing Rule
Course Access Level	Essay Question	SCORM Sequencing Rule Condition
Course Access User	Fill in the Blank Question	SCORM Objective
Course Content Server	Rating Question	SCORM Objective Map
Course Download	Multiple Choice Question	SCORM Rollup Rule
Course Session Cost	Triple Rating Question	SCORM Rollup Condition
Course Test	Triple Rating Question Item	Courseware Content Organization
Course Schedule	Drag and Drop Question	Courseware Content Organization Node
Course Session Schedule	Drag and Drop Question Draggable	Courseware Content Organization Objective
Program Courses	Audio Capture Question	Courseware Content Package
Course Evaluation	Hotspot Question	Courseware Vendor
Program Session	Hotspot Properties	CMI Assignable Unit
Homework File	Question Approval	CMI Descriptor
Instructor Comment		Courseware Content Organization Node Objective
Knowledge Center Options		
Course Cost	**Enrolments, Transcripts, Records**	
Program Session Cost	Transcript	

Course Registration	Course Withdrawal Reason	
Session Cost	External Training	
Course Revision	Approval Queue	
Course Optional Paid Items	Approval Queue Step	
Custom Course Enrollment Policy	Payment Details	
Optional Paid Item Refund Deduction	Purchased Optional Paid Items	
Course Objective	Learners Withdrawn from Course	
Course Misc. Details	Course Withdrawal Refund Deduction	
Course Owner	**Exams**	
Course Prerequisite	Exam Question Properties	
Program	Exam Section Properties	
Enrollment Policy	Exam Properties	
Enrollment Policy Step	Exam Attempt	
Course Instructor	Exam Answer Attempt	
Learning Object Attribute	Matching Question Attempt	
Virtual Classroom Session Details	Essay Question Attempt	
Automatic E-mail Set-up	Fill in the Blank Question Attempt	
getAbstract Launch Properties	Rating Question Attempt	
GlobalEnglish Launch Properties	Audio Capture Question Attempt	
Safari Books Launch Properties	Exam Attempt Section	
Generic Virtual Classroom Launch Properties	Exam Random Section	
WebEx Launch Properties	Hotspot Answer	
NETg Proxied Authentication	Drag and Drop Answer	
	Exam Comment	
	Triple Rating Question Attempt	
	Exam Print Properties	

All audit trails can be viewed using Compliance Reports discussed later.

Electronic Signatures

Before every important operation, an electronic signature prompt appears, asking for the logged-in user's user ID, password and update meaning. These three parameters collectively form an E-Signature. The user ID and password must be correct for the current user before the requested operation can be carried out. EKP allows fine-grain control over E-Signature collection via System Configuration options:



System Configuration

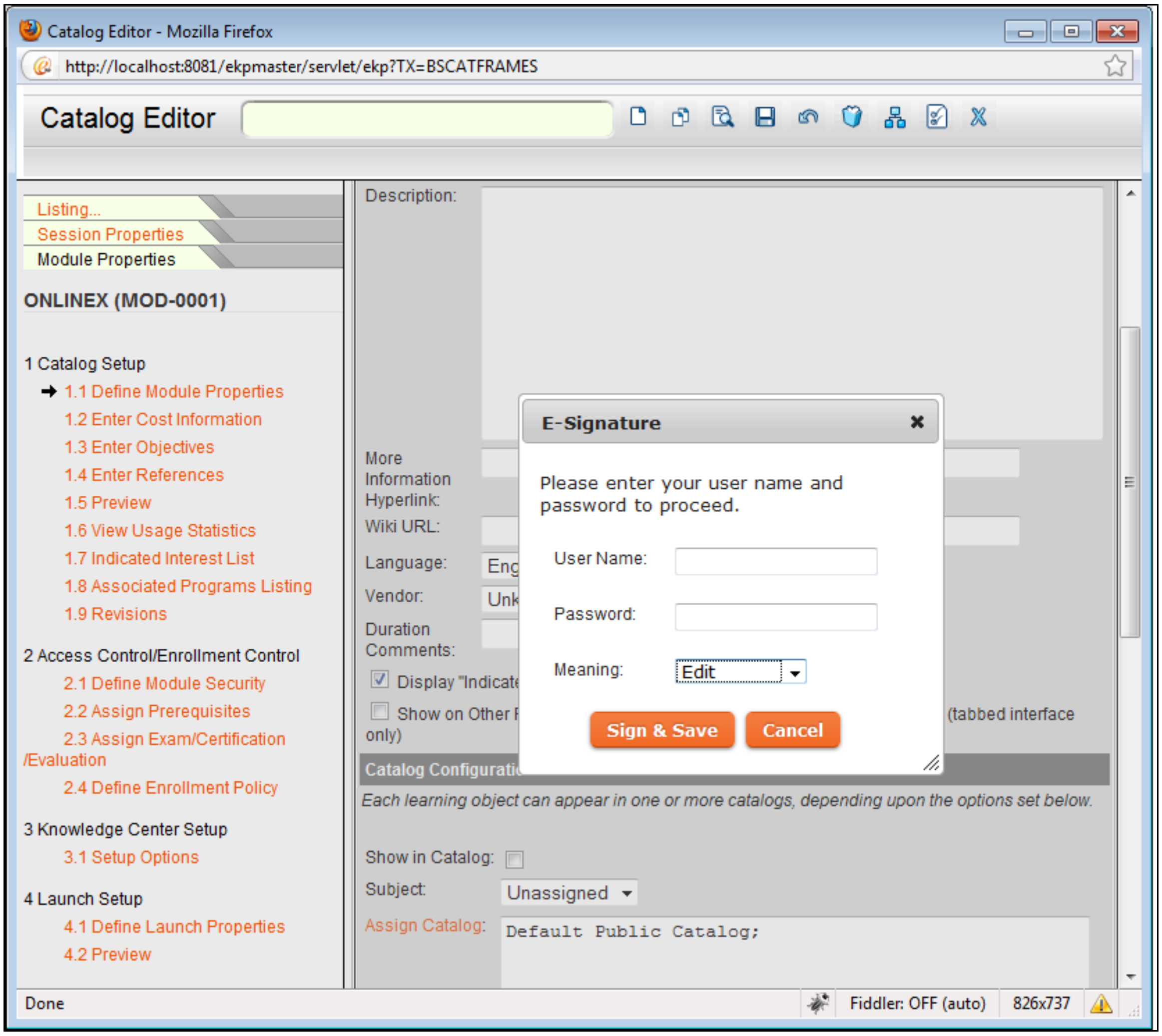
Select a specific configuration category from the drop-down menu below. Subsequent screens allow you to edit the properties associated with the selected category. When you click Save, the current customization.properties file is updated.

Select a category: E-Signature You must save all changes **before** selecting another category.

E-Signature			
Enable E-Signature for course CSV loader.	☑	6.3	?
Enable E-Signature when editing an External Training Record	□	6.3	?
Enable E-Signature for when a learner withdraws from a course.	□	6.3	?
Enable E-Signature for course update/delete.	☑	6.3	?
Enable E-Signature for course launch.	☑	6.3	?
Enable E-Signature for exam launch.	☑	6.3	?
Enable E-Signature for manual grading of test answer.	☑	6.3	?
Enable E-Signature for structured course importers.	☑	6.3	?
Enable E-Signature for change in question status	☑	6.3	?
Enable E-Signature when transcript details are modified by a reviewer	□	6.3	?
Enable E-Signature for transcript attendance details modification.	□	6.3	?
Enable E-Signature when transcript details are modified via the Enrollment Wizard.	□	6.3	?

E-Signature System Configuration

For example, from the above screen capture's settings, an E-Signature will be prompted when a user tries to manually grade a test answer or when the status of a question is changed or when course details are updated or deleted in Catalog Editor and so on. The E-Signature prompt in Catalog Editor looks like:



Catalog Editor - Mozilla Firefox

http://localhost:8081/ekpmaster/servlet/ekp?TX=BSCATFRAMES

Catalog Editor

Listing...
Session Properties
Module Properties

ONLINEX (MOD-0001)

1 Catalog Setup
- 1.1 Define Module Properties
- 1.2 Enter Cost Information
- 1.3 Enter Objectives
- 1.4 Enter References
- 1.5 Preview
- 1.6 View Usage Statistics
- 1.7 Indicated Interest List
- 1.8 Associated Programs Listing
- 1.9 Revisions

2 Access Control/Enrollment Control
- 2.1 Define Module Security
- 2.2 Assign Prerequisites
- 2.3 Assign Exam/Certification /Evaluation
- 2.4 Define Enrollment Policy

3 Knowledge Center Setup
- 3.1 Setup Options

4 Launch Setup
- 4.1 Define Launch Properties
- 4.2 Preview

Description:

More Information Hyperlink:

Wiki URL:

Language: Eng

Vendor: Unk

Duration Comments:

☑ Display "Indicate

□ Show on Other F (tabbed interface only)

Catalog Configurati

Each learning object can appear in one or more catalogs, depending upon the options set below.

Show in Catalog: □

Subject: Unassigned

Assign Catalog: Default Public Catalog;

E-Signature ✖

Please enter your user name and password to proceed.

User Name:

Password:

Meaning: Edit

Done

E-Signature Prompt in the Catalog Editor

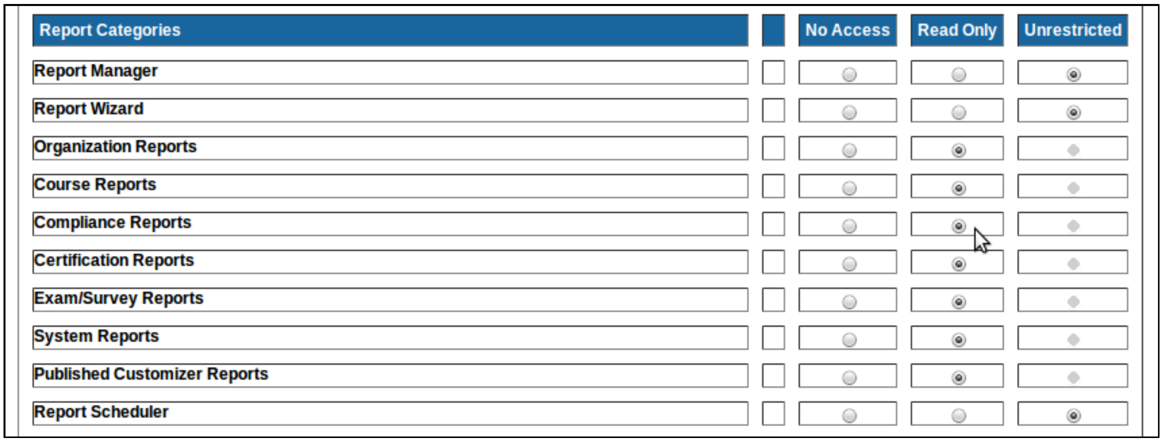
Here a user needs to provide their login Username and Password and select the most appropriate Meaning for the action they are about to perform. Clicking "Sign & Save" will validate the user ID and password, and if correct, the Save operation is performed. In EKP 6.3 there is no relationship or validation between selected Meaning and the action being performed. An error message is displayed when incorrect details are provided, including the case where the Username provided does not match that of the logged-in user. Successful validation will cause the changes (in this case course details) to be saved along with the E-Signature.

Please note that a CFR-enabled license is required in order to view the E-Signature settings in System Configuration.

Reporting

As discussed earlier, all audited data is conveniently presented as standard EKP reports. This means users can view this audited information in various electronic formats like HTML, CSV, PDF and Excel as with other standard EKP reports.

A user's role must have access to the Compliance Reports section of Report Manager in order to access the audit-related reports. By default a user does not have access to this functionality. This can be changed by granting the desired role "Read Only" access to Compliance Reports in the Role Access Control functionality of User Manager as shown below



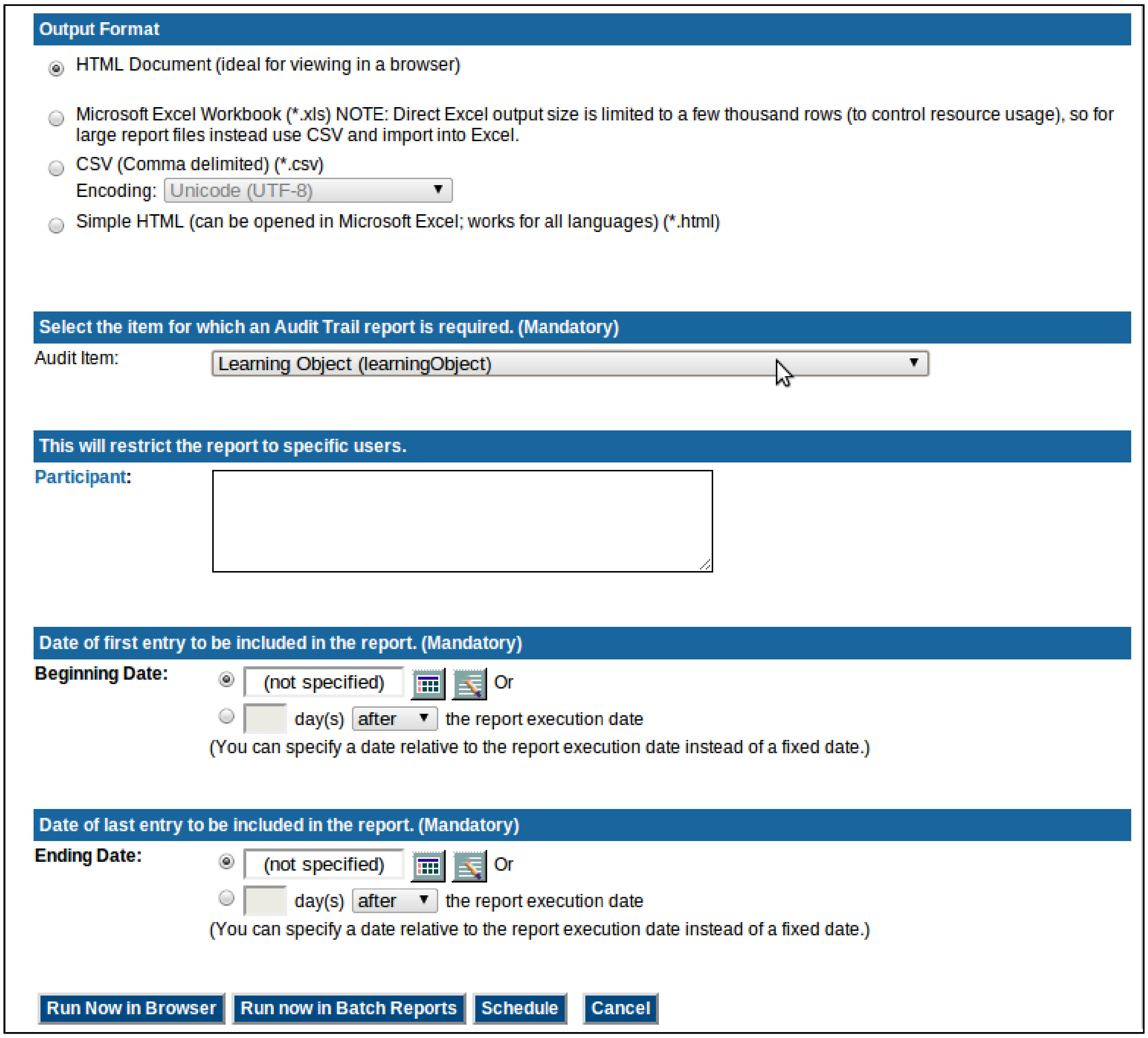
Report Categories		No Access	Read Only	Unrestricted
Report Manager	□	○	○	●
Report Wizard	□	○	○	●
Organization Reports	□	○	●	○
Course Reports	□	○	●	○
Compliance Reports	□	○	●	○
Certification Reports	□	○	●	○
Exam/Survey Reports	□	○	●	○
System Reports	□	○	●	○
Published Customizer Reports	□	○	●	○
Report Scheduler	□	○	○	●

Enabling Compliance Reports

Users with this role access can now navigate to the Compliance Reports section of Report Manager. There are two reports relevant to auditing in this section: the Audit Trail Report (R505) and the Audit Trail User Action Report (R506).

Audit Trail Report (R505)

This report displays the audit trail for the selected audit item within the specified date range. The audit trail is displayed in chronological order of audit date. Apart from the date range, a list of users whose updates have caused auditing (audit users) can also be selected:



Output Format

● HTML Document (ideal for viewing in a browser)

○ Microsoft Excel Workbook (*.xls) NOTE: Direct Excel output size is limited to a few thousand rows (to control resource usage), so for large report files instead use CSV and import into Excel.

○ CSV (Comma delimited) (*.csv)
Encoding: Unicode (UTF-8)

○ Simple HTML (can be opened in Microsoft Excel; works for all languages) (*.html)

Select the item for which an Audit Trail report is required. (Mandatory)

Audit Item: Learning Object (learningObject)

This will restrict the report to specific users.

Participant:

Date of first entry to be included in the report. (Mandatory)

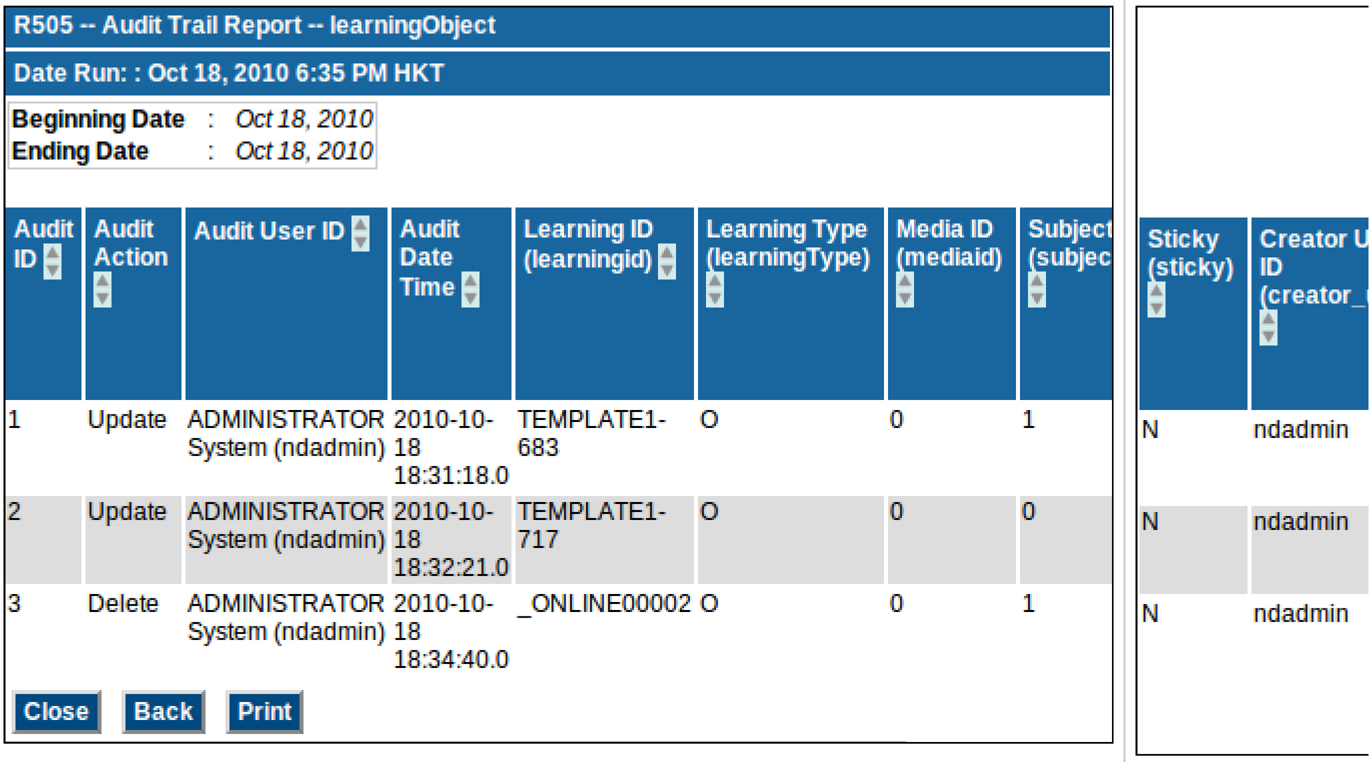
Beginning Date: ● (not specified) Or
○ day(s) after the report execution date
(You can specify a date relative to the report execution date instead of a fixed date.)

Date of last entry to be included in the report. (Mandatory)

Ending Date: ● (not specified) Or
○ day(s) after the report execution date
(You can specify a date relative to the report execution date instead of a fixed date.)

Report Options of R505

Audit items are data entities for which the user wants to view the audit reports. The text within the bracket holds the database table name of that entity. The audit item and the date range are mandatory options. Below is an example of the R505 report generated for the item "Learning Object". For brevity, only the starting and the ending sections are shown below.



R505 -- Audit Trail Report -- learningObject

Date Run: : Oct 18, 2010 6:35 PM HKT

Beginning Date	:	*Oct 18, 2010*
Ending Date	:	*Oct 18, 2010*

Audit ID	Audit Action	Audit User ID	Audit Date Time	Learning ID (learningid)	Learning Type (learningType)	Media ID (mediaid)	Subject (subjec	Sticky (sticky)	Creator U ID (creator_
1	Update	ADMINISTRATOR System (ndadmin)	2010-10-18 18:31:18.0	TEMPLATE1-683	O	0	1	N	ndadmin
2	Update	ADMINISTRATOR System (ndadmin)	2010-10-18 18:32:21.0	TEMPLATE1-717	O	0	0	N	ndadmin
3	Delete	ADMINISTRATOR System (ndadmin)	2010-10-18 18:34:40.0	_ONLINE00002	O	0	1	N	ndadmin

Audit Trail for Learning Object

A few important columns are

- Audit Action that indicates what sort of action has been performed on the Audit Item *i.e.* Update, Delete or Insert.
- Audit User indicates who has performed the aforementioned action.
- Update Meaning indicates the Meaning selected by the user in the E-Signature.
- the rest of the columns indicates the data newly inserted, or the new data if an update has occurred, or the data prior to the deletion if a deletion has occurred.

From the above example we can see that:

- System Administrator updated details on Learning Object with Id TEMPLATE1_683 and update meaning is blank which indicates E-Signature was disabled
- System Administrator updated details on Learning Object with Id TEMPLATE1_717 and Signed the E-Signature with update meaning "Edit"
- System Administrator deleted Learning Object with Id _ONLINE00002 and Signed it as "Rejection"

Audit Trail User Action Report (R506)

This report is similar to R505 and displays the audit trail for a given set of users within the specified date range. This report is geared around activities of a set of users.

CFR Installation Pack

Contents

- Database install script - a script that will install the database audit tables and triggers on an instance of EKP.
- Install Guide (this document) - instructions on how to run the database upgrade script and prepare EKP to support CFR compliance
- CFR Overview document - document on the technical requirements of Title 21 CFR Part 11 and how the functionalities of EKP help to meet them.

CFR Enabling EKP License

You need a special EKP license to enable CFR support functionalities in EKP. Rest of this document assumes that you have already acquired this license through sales channels and updated it in 'WEB-INF/conf' directory of your EKP installation directory. Please proceed only when you have the CFR enabling license.

Preparing EKP to Support CFR Compliance

Enabling Database Auditing

It is required to run the script in CFR Pack to enable database auditing in EKP.

Pre-requisite

- It is recommended to take backup of your production database before running this installation package.
- You must have EKP 6.3 installed on the system.
- Stop the tomcat server or the server that is hosting your EKP

Following are the instructions to run the script

On Windows System

- Edit the "webapps.ekp" in the "build.xml" to the appropriate location.
- Edit the "install.bat" and make sure JAVA_HOME environment variable is set correctly.
- Execute "install.bat".

On Linux/Unix Systems

- Edit the "webapps.ekp" in the "build.xml" to the appropriate location.
- Edit the "install.sh" and make sure JAVA_HOME environment variable is set correctly.
- Set execution permission to "install.sh" by running "chmod +x install.sh".
- Execute "install.sh".

Reverting upon Failure

CFR install script takes a backup of the original database scripts present in the 'nschema' folder of EKP to 'nschema.backup'. Upon failure the database can be recreated using these scripts and backed-up data can be restored. Please contact NetDimensions support (support@netdimensions.com) providing the error details.

Configurations

Next step after enabling auditing is to re-configure EKP

- Ensure that a CFR-enabled EKP license is installed.
- Ensure for all User Roles, the access control for "Allow User Deletes" is disabled.
- Ensure that access to the API is disabled so that EKP remains a closed system.
- Note that both the User ID Migration function and the Learning Object ID Migration function are hidden when EKP is using a CFR-enabled license. This is because both functions are incompatible with CFR requirements.

Enabling Electronic Signatures

- Under System Configuration, in the category of "E-Signature", enable electronic signatures for all required places. The available places where electronic signature prompts may be enabled are:

1. Course CSV Loader
2. When editing an External Training Record
3. When a learner withdraws from a course
4. Course update/delete
5. Course Launch
6. Exam Launch
7. Manual Grading of test answer
8. Structured course importers

9. Change in question status
10. Question Importers
11. When transcript details are modified by a reviewer
12. Transcript attendance details modification
13. When transcript details are modified via the Enrollment Wizard

It is recommended that these options are all enabled unless it is not practical to do so. Please note that a CFR-enabled license is required in order to view the E-Signature settings in System Configuration.

Enabling Audit Reports

1. Under Role Access Control, mark "Compliance Reports" as Read Only. The reports R505 - Audit Trail Report and R506 - Audit Trail User Action Report will then be available under "Compliance Reports" within Report Manager.