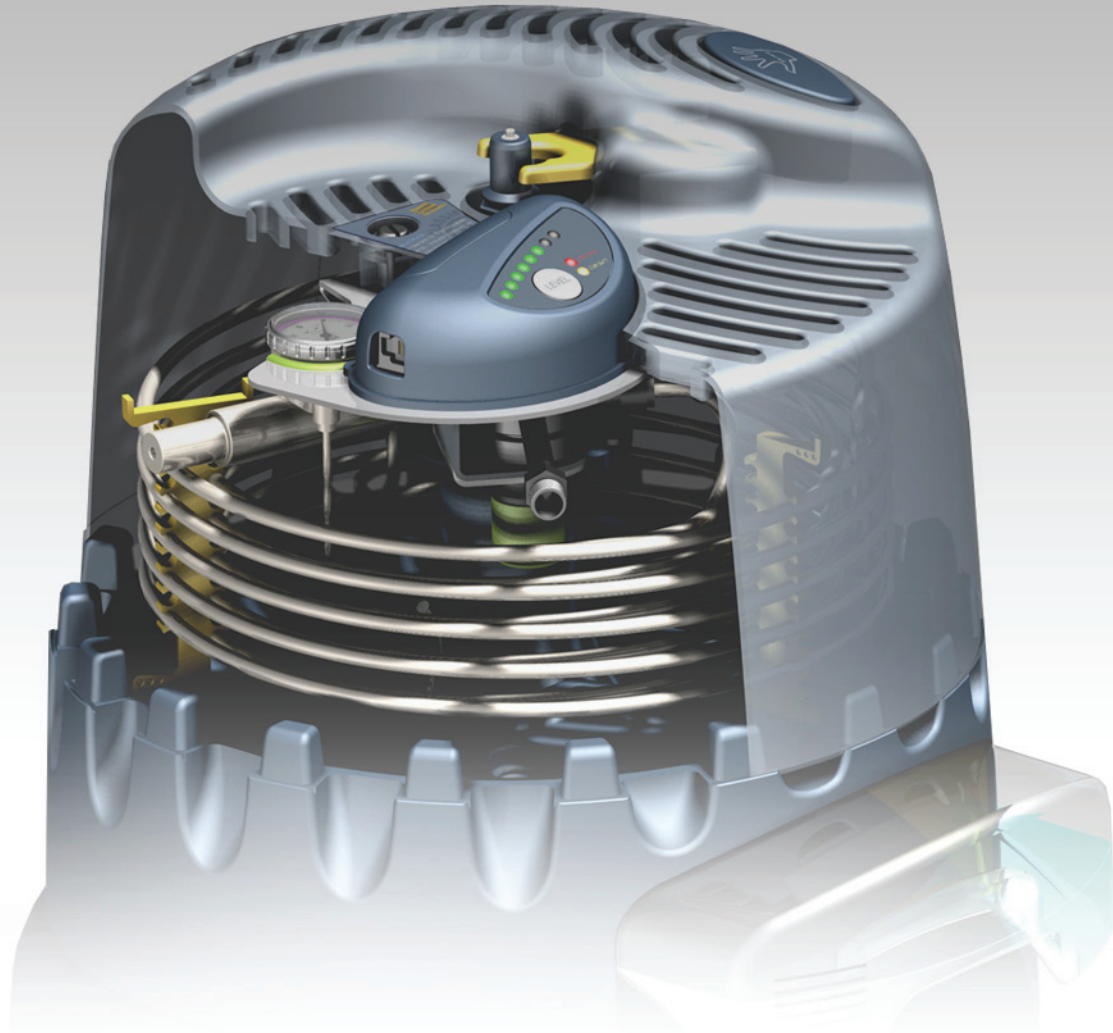


# SolidWorks Enterprise PDM and FDA 21CFR Part 11



This Technical Paper discusses the technical solutions provided by SolidWorks Enterprise PDM to address the FDA 21 CFR Part 11 requirements.

## Introduction

Companies are facing many challenges in heavily regulated industries such as the Pharmaceutical, Medical devices, Cosmetic and Agro-food Industries. One important challenge is the validation of their electronic records by the FDA to comply with the 21 CFR Part 11 Rule.

The 21 CFR Part 11 consists of a number of rules pertaining mainly to:

- Creation and Protection of Electronic Records
- Access Authorization and Security
- Traceability and Audit Trail on all electronic records
- Requirements for electronic signature.

SolidWorks Enterprise PDM provides solutions to help capture documents, processes and procedures to adhere to regulations as specified in the FDA 21 CFR Part 11 Rule.

SolidWorks Enterprise PDM can help reduce time, costs and risks associated with the process of implementing and validating the process for companies to comply with the FDA rules.

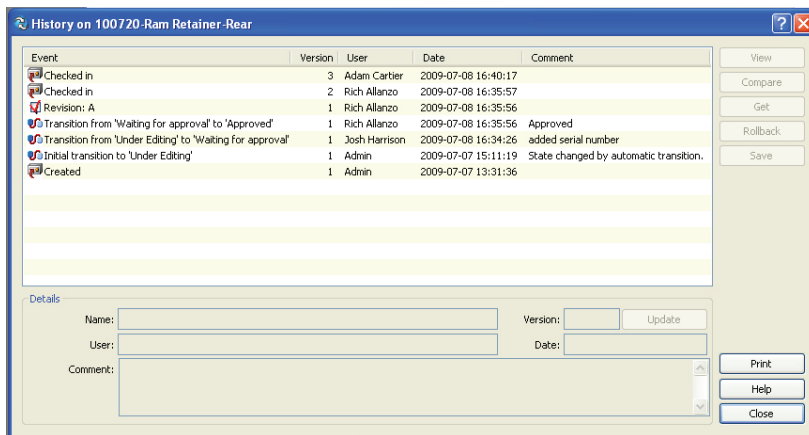
Approval processes with double electronic signatures and full audit trails help companies use this SolidWorks Enterprise PDM as part of their FDA 21 CFR Part 11 Compliance and Quality Program. Additionally, SolidWorks Enterprise PDM is a powerful, robust, yet easy-to-use and implement product data management system that can be used to capture, automate and monitor processes dealing with document management and engineering design management.

This Technical Paper discusses the technical solutions provided by SolidWorks Enterprise PDM to address the FDA 21 CFR Part 11 requirements.

### 11.10 Controls for Closed Systems

#### 11.10(a)

- Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records
- SolidWorks Enterprise PDM manages records and versions them each time they are checked in. Upon check-in the person that modified the file and the date it was modified is captured. All versions are retained and available to determine changes from one version to another. The history report on the file provides an audit trail.



#### Disclaimer:

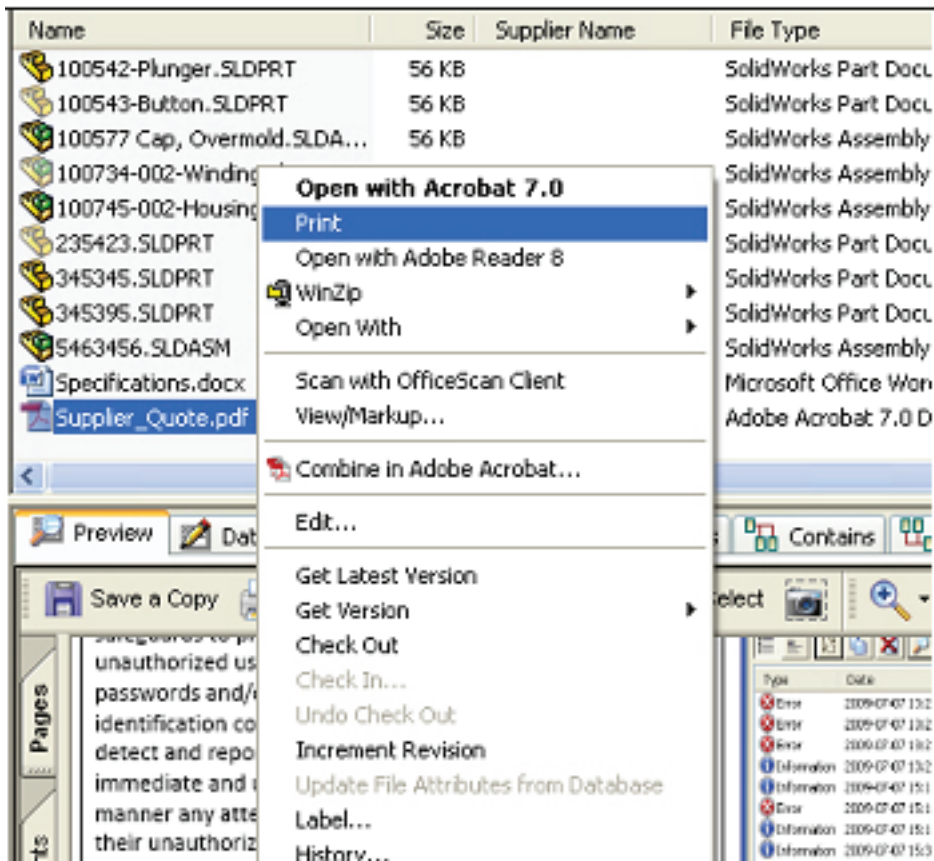
This document does not constitute a recognition or compliance of SolidWorks Enterprise PDM Software by the United States Food and Drug Administration for the 21 CFR Part 11 Regulation.

Compliance with 21 CFR Part 11 of Processes and Methodologies is the Sole responsibility of the Customer and SolidWorks has no responsibility or liability in this regard.

This document is provided by SolidWorks for information purpose only without representation or warranty of any kind. SolidWorks shall not be liable for errors or omissions of any kind for the materials herein..

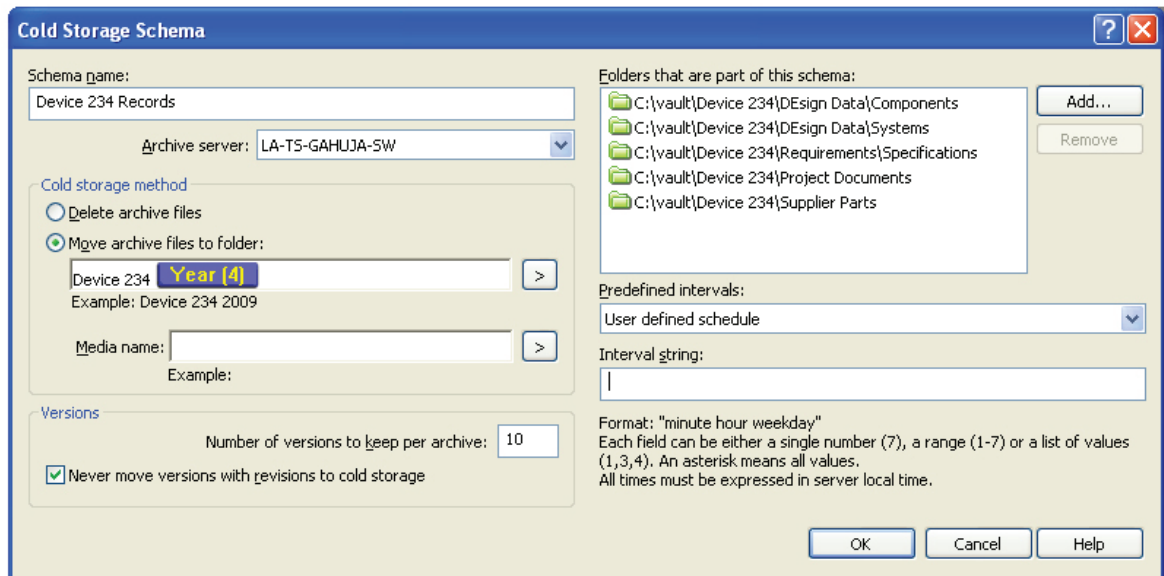
### 11.10(b)

- Provide 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
- SolidWorks Enterprise PDM manages files so they can be retrieved for review by anyone with proper access. The file is retrieved in its native format, allowing user to view and print the file.  
SolidWorks Enterprise PDM can read and write all file formats that are recognized by the Windows operating system, including popular formats such as .pdf.



### 11.10(c)

- Protection of records to enable their accurate and ready retrieval throughout the records retention period.
- This may be supported out of the box or with customization depending on site-specific requirements. Enterprise PDM allows you to retain documents for as long as you desire. However, if a large bulk of data needs to be retained for many years, you may choose to utilize the 'Cold Storage' option of Enterprise PDM. This will allow meta-data to be searchable and corresponding documents can be retrieved from storage state on as-needed basis.



The 'Cold Storage Schema' dialog box is used to configure archival settings. It includes fields for 'Schema name' (Device 234 Records) and 'Archive server' (LA-T5-GAHUJA-SW). Under 'Cold storage method', the 'Move archive files to folder' option is selected, with a folder path 'Device 234 Year (4)' and an example 'Device 234 2009'. A 'Media name' field is also present. The 'Versions' section shows 'Number of versions to keep per archive' set to 10, with a checked option 'Never move versions with revisions to cold storage'. On the right, a list of folders is shown, including 'Components', 'Systems', 'Specifications', 'Project Documents', and 'Supplier Parts'. Below this, 'Predefined intervals' is set to 'User defined schedule', and an 'Interval string' field is empty. A format note explains the syntax for the interval string.

Schema name: Device 234 Records

Archive server: LA-T5-GAHUJA-SW

Cold storage method

☐ Delete archive files

☒ Move archive files to folder:

Device 234 Year (4)

Example: Device 234 2009

Media name:

Example:

Versions

Number of versions to keep per archive: 10

☒ Never move versions with revisions to cold storage

Folders that are part of this schema:

- C:\vault\Device 234\Design Data\Components
- C:\vault\Device 234\Design Data\System
- C:\vault\Device 234\Requirements\Specifications
- C:\vault\Device 234\Project Documents
- C:\vault\Device 234\Supplier Parts

Predefined intervals: User defined schedule

Interval string:

Format: "minute hour weekday"

Each field can be either a single number (7), a range (1-7) or a list of values (1,3,4). An asterisk means all values.

All times must be expressed in server local time.

OK Cancel Help

### 11.10(d)

- Limiting system access to authorized individuals.
- System access is restricted by user name and password. In addition, Enterprise PDM provides an elaborate structure for user access management. You can control user access to vault, folders or documents by individual users or groups. Permission at each level – vault, group, individual – is independent of other permissions.



The EPDM login screen features the EPDM logo at the top left. Below it, there are input fields for 'User name' (John Smith) and 'Password' (masked with dots). To the left of the password field is a graphic of a blue globe with a white key and a coiled orange cable. At the bottom right, there are 'Log In' and 'Cancel' buttons.

EPDM

User name: John Smith

Password: .....

Log In

Cancel

### 11.10(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.
- SolidWorks Enterprise PDM manages each record by versioning it each time it is checked in, capturing the person that modified the file and the date it was modified and the time checked back in. A history report shows access to records and use of the Comment field can document the purpose of the access. A user can review any version to determine what has changed from version to version. All managed records also possess the capability to set their delete flag to “do not destroy”.

Event	Version	User	Date	Comment
Checked in	3	Adam Cartier	2009-07-08 16:40:17	
Checked in	2	Rich Allanzo	2009-07-08 16:35:57	
Revision: A	1	Rich Allanzo	2009-07-08 16:35:56	
Transition from 'Waiting for approval' to 'Approved'	1	Rich Allanzo	2009-07-08 16:35:56	Approved
Transition from 'Under Editing' to 'Waiting for approval'	1	Josh Harrison	2009-07-08 16:34:26	added serial number
Initial transition to 'Under Editing'	1	Admin	2009-07-07 15:11:19	State changed by automatic transition.
Created	1	Admin	2009-07-07 13:31:36	

Details

Name:  Version:  Update

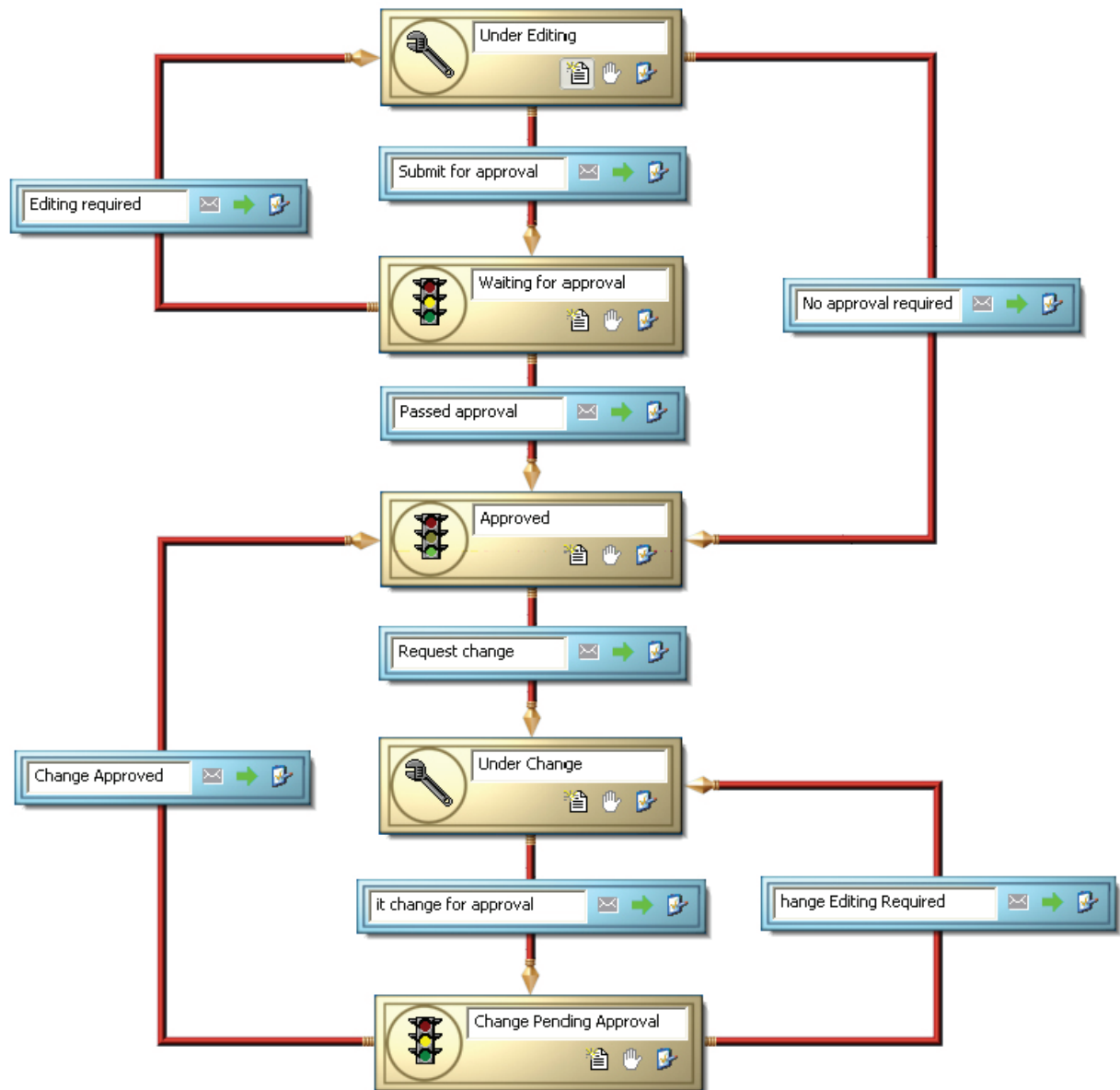
User:  Date:

Comment:

Print Help Close

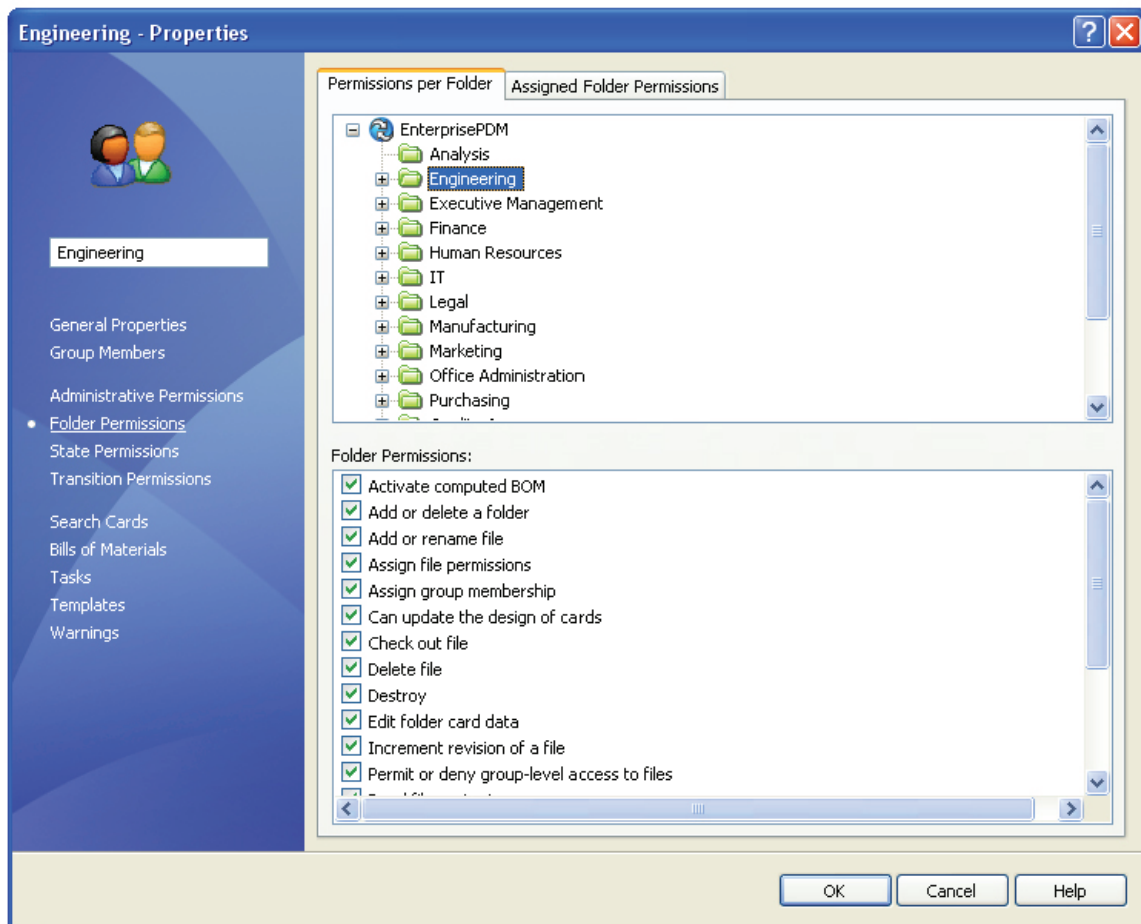
### 11.10(f)

- Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
- SolidWorks Enterprise PDM applies a customizable workflow to each record that enables you to define a series of sequential steps that a record must pass in its lifecycle and to enforce and record the execution of each step.



### 11.10(g)

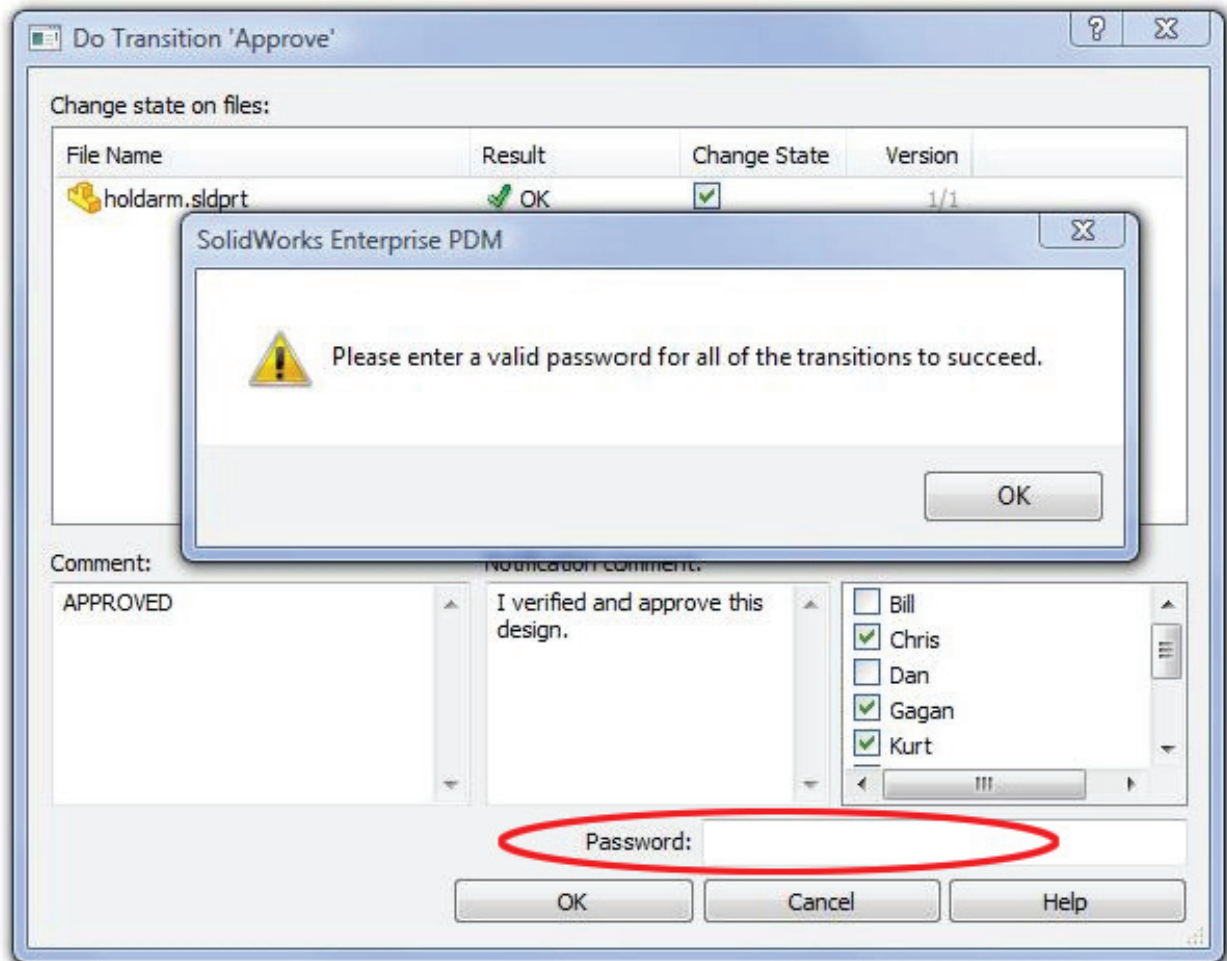
- Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.
- Access to the system and all permissions are administered via the user name and password.





### 11.10(h)

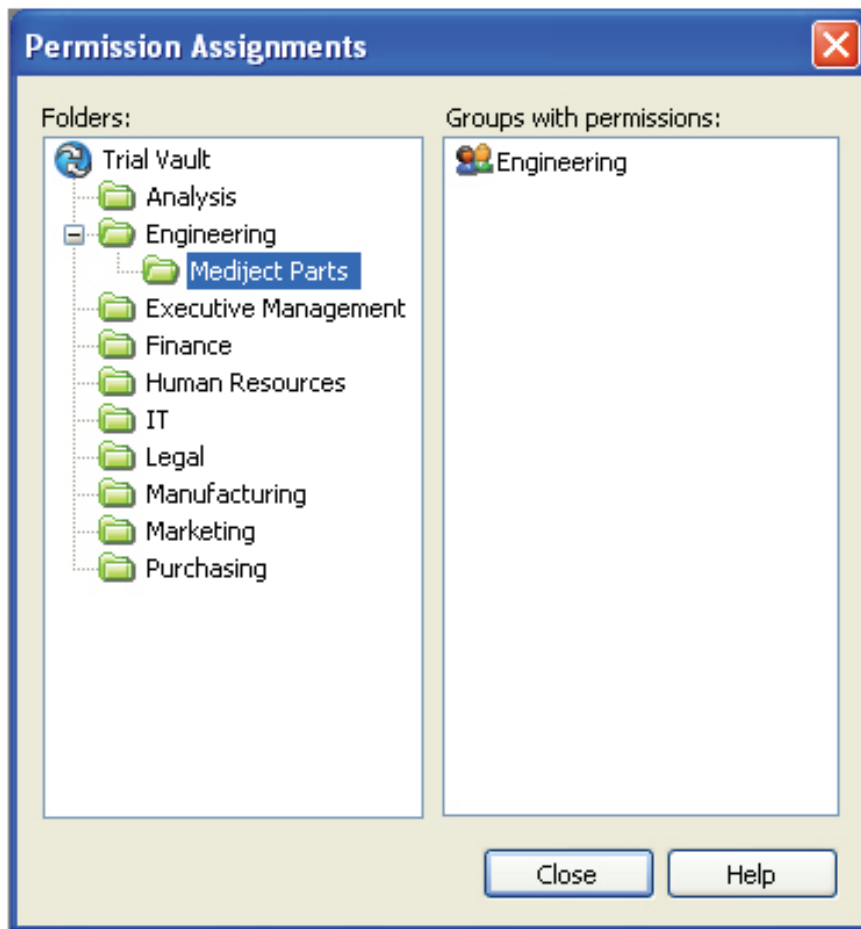
- Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.
- All security is handled by user name and password. An additional level of protection is provided by double electronic signature feature. This means that even after the user has logged in and obtained access to the system, he or she must enter their password again to indicate approval or "signature" on a document or step in a process.





#### 11.10(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.
- You are responsible for the education and training of the persons using this system. Once you identify qualified users, groups can be created for different Certifications. Users can be added to appropriate Groups. Tasks and document access can be restricted to specific Groups.



#### 11.10(j)

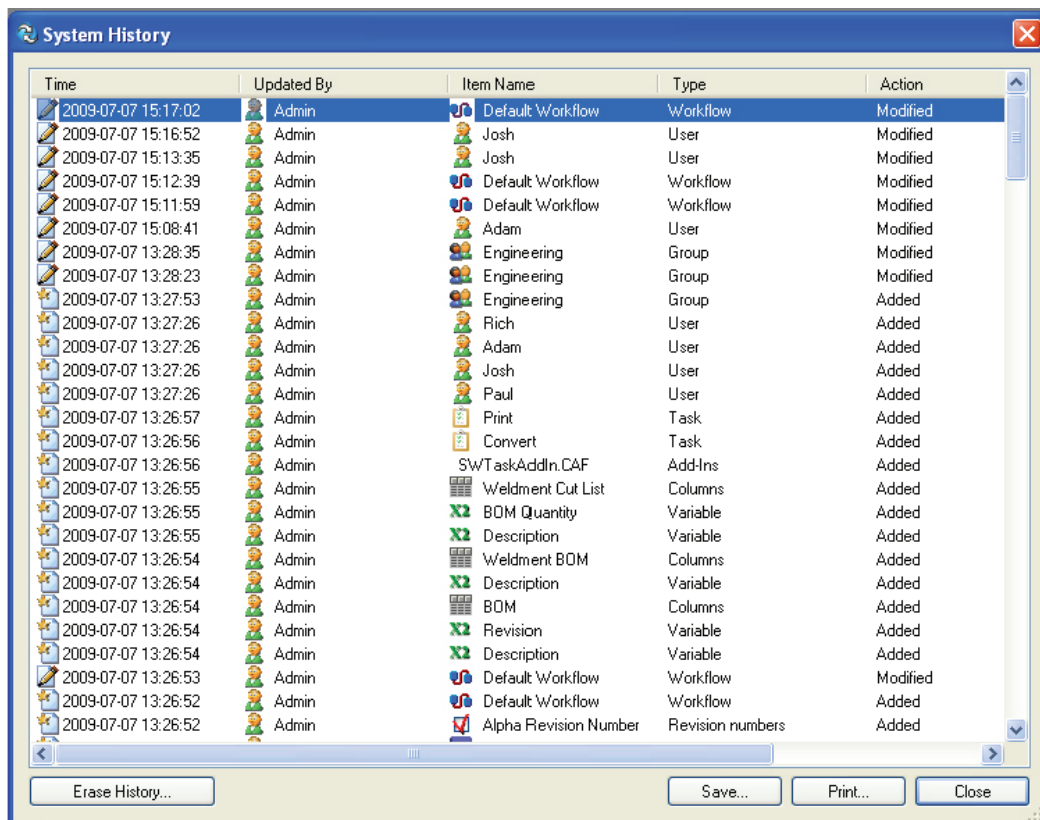
- The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.
- This is supported by company policy and procedure.

### 11.10(k.1)

- Use of appropriate controls over systems documentation including adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
- This is supported through company policy and procedure. "System history" provides documentation of the actions that administrators have taken.

### 11.10(k.2)

- Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.
- This is supported through company policy and procedure. "System history" provides documentation of the actions that administrators have taken.



The screenshot shows a window titled "System History" with a table of system changes. The table has five columns: Time, Updated By, Item Name, Type, and Action. The data is as follows:

Time	Updated By	Item Name	Type	Action
2009-07-07 15:17:02	Admin	Default Workflow	Workflow	Modified
2009-07-07 15:16:52	Admin	Josh	User	Modified
2009-07-07 15:13:35	Admin	Josh	User	Modified
2009-07-07 15:12:39	Admin	Default Workflow	Workflow	Modified
2009-07-07 15:11:59	Admin	Default Workflow	Workflow	Modified
2009-07-07 15:08:41	Admin	Adam	User	Modified
2009-07-07 13:28:35	Admin	Engineering	Group	Modified
2009-07-07 13:28:23	Admin	Engineering	Group	Modified
2009-07-07 13:27:53	Admin	Engineering	Group	Added
2009-07-07 13:27:26	Admin	Rich	User	Added
2009-07-07 13:27:26	Admin	Adam	User	Added
2009-07-07 13:27:26	Admin	Josh	User	Added
2009-07-07 13:27:26	Admin	Paul	User	Added
2009-07-07 13:26:57	Admin	Print	Task	Added
2009-07-07 13:26:56	Admin	Convert	Task	Added
2009-07-07 13:26:56	Admin	SWTaskAddIn.CAF	Add-Ins	Added
2009-07-07 13:26:55	Admin	Weldment Cut List	Columns	Added
2009-07-07 13:26:55	Admin	BOM Quantity	Variable	Added
2009-07-07 13:26:55	Admin	Description	Variable	Added
2009-07-07 13:26:54	Admin	Weldment BOM	Columns	Added
2009-07-07 13:26:54	Admin	Description	Variable	Added
2009-07-07 13:26:54	Admin	BOM	Columns	Added
2009-07-07 13:26:54	Admin	Revision	Variable	Added
2009-07-07 13:26:54	Admin	Description	Variable	Added
2009-07-07 13:26:53	Admin	Default Workflow	Workflow	Modified
2009-07-07 13:26:52	Admin	Default Workflow	Workflow	Added
2009-07-07 13:26:52	Admin	Alpha Revision Number	Revision numbers	Added

At the bottom of the window, there are buttons for "Erase History...", "Save...", "Print...", and "Close".

## 11.30 Controls for Open Systems

### 11.30

- 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 as document encryption and use of appropriate digital signature standards.
- Enterprise PDM is designed for use as a closed system.

## 11.50 Signature Manifestations

### 11.50(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
  3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature
- Enterprise PDM records the event (check in, approve, reject, etc.) in the history file along with the user id while allowing/forcing the user to provide a comment.

The screenshot shows a software window titled "History on Valve.SLDPRT". It contains a table of events and a section for transition details.

Event	Version	User	Date	Comment
Revision: B	2	Martin	2009-07-31 14:37:26	
Revision: A	2	Martin	2009-07-31 14:37:23	
Transition from 'Waiting for approval' to 'Approved'	2	Martin	2009-07-31 14:37:23	Approved
Checked in	2	Martin	2009-07-31 14:37:23	
Transition from 'Under Editing' to 'Waiting for appr...	1	Adam	2009-07-31 14:35:50	
Transition from 'Waiting for approval' to 'Under Ed...	1	Martin	2009-07-31 14:29:20	Cannot manufacture with the ribs too close ...
Transition from 'Under Editing' to 'Waiting for appr...	1	Gagan	2009-07-31 14:27:27	New part approval requested
Initial transition to 'Under Editing'	1	Admin	2009-07-31 14:26:25	State changed by automatic transition.
Renamed from 'Part2.SLDPRT'		Admin	2009-07-31 14:26:06	
Created	1	Admin	2009-07-31 14:26:00	

Transition details

Name: Transition from 'Default Workflow.Waiting for approval' to 'Default Workflow.Under Edit' Version: 1 Update

User: Martin Date: 2009-07-31 14:29:20

Comment: Cannot manufacture with the ribs too close to hole

Buttons: View, Compare, Get, Rollback, Save, Print, Help, Close

## 11.70 Signature/Record Linking

### 11.70

- 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.
- Enterprise records the event (check in, approval, reject, etc.) in the history file along with the user id while allowing/forcing the user to provide a comment. Handwritten signatures can be appended as PDF to the relevant record.

## 11.100 General Requirements

### 11.100(a)

- Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.
- Each user that is added to the application will be assigned unique credentials (login name and password) to log in. All transactions that are logged by the application will be attributed to that user's unique login name, ensuring traceability for all key transactions. The user is responsible for providing and protecting both their login name and password at secondary authentication step.  
Administrator can refuse login to terminated employees. This maintains their data in system and prevents re-issuance of same user name.

The screenshot displays a user management window with the following fields and controls:

- Login name:** Adam Cartier
- Full name:** Adam Cartier
- Initials:** AC
- E-mail:** (empty field)
- User data:** (empty text area with scrollbars)
- Column view:** <No column views have been defined.>
- Set Password...** button

A modal dialog box titled "Change Password - Adam Cartier" is open, containing:

- New password:** (text input field)
- Confirm new password:** (text input field)
- Password of logged in user:** (text input field)
- OK**, **Cancel**, and **Help** buttons at the bottom.

At the bottom of the main window, there are **OK**, **Cancel**, and **Help** buttons.

#### 11.100(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.
- This is supported by company policy and procedure.

#### 11.100(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.
- This is supported by company policy and procedure.

### 11.200 Electronic Signature Components and Controls

#### 11.200(a)(1)

- Electronic signatures that are not based upon biometrics shall:  
Employ at least two distinct identification components such as an identification code and password.
- Enterprise PDM requires the combination of 'User name' and 'Password' as the two distinct identification components.

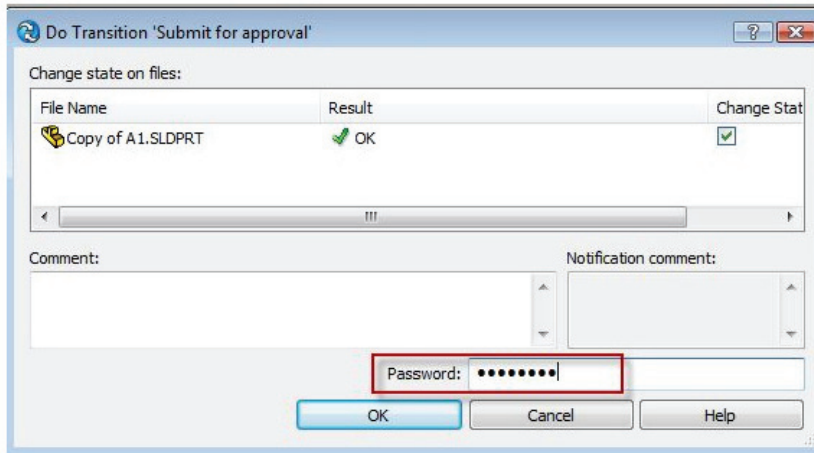


#### 11.200(a)(1)(i)

- In a continuous session:
  1. first signing shall be executed using all electronic signature components
  2. 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.
- Enterprise PDM requires 'User Name' and 'Password' at the beginning of every new session. Subsequent Workflow events like Approvals & Sign offs can be set to require Password.

### 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.
- This is supported by Enterprise PDM. Every new session requires both the identification components to login, i.e. "User Name & Password". Subsequent approvals via Workflow can be set to pose double challenge by requiring "Password" again.



### 11.200(a)(2)

- Electronic signatures that are non biometric must be used only by genuine owner.
- The Electronic Signatures are unique to one individual. For added security, un-authorized account access can be reduced by enabling 'Inactivity Timeout' on Windows Desktop. In addition, subsequent approvals via Workflow can be set to pose double challenge by requiring "password" again.

### 11.200(a)(3)

- Electronic signatures that are not based upon biometrics shall:  
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.
- Enterprise PDM is not designed to enable use by other than the genuine owner of the electronic signature. However, this requirement can be supported by defining a parallel approval process which will require multiple review and sign-offs if original approver is not available.

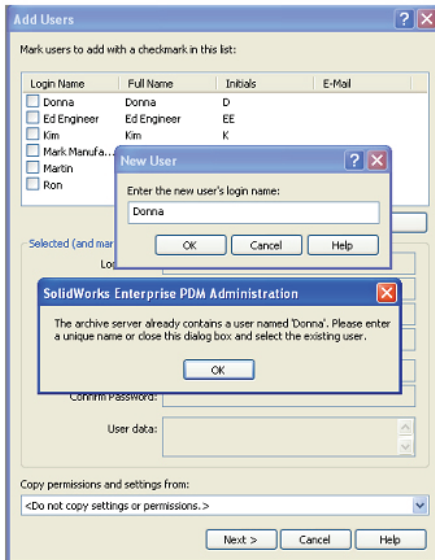
### 11.200(b)

- Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.
- Enterprise PDM does not support biometrics.

### 11.300 Controls for Identification Codes/Passwords

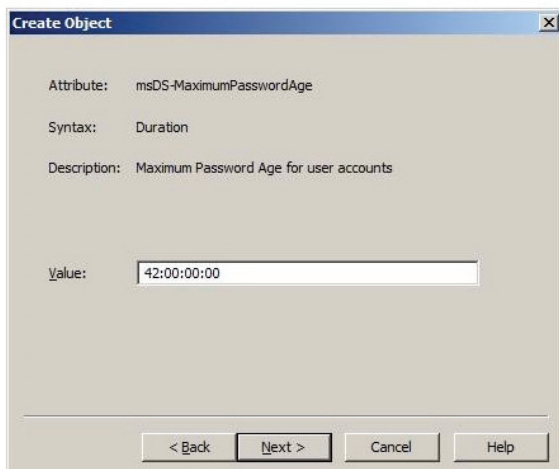
#### 11.300 (a)

- Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
- Enterprise PDM does not allow you to create duplicate 'user name' thereby assuring that no two individuals can have same combination of identification and password.  
Administrator can refuse login to terminated employees. This maintains their data in system and prevents re-issuance of same user name.



#### 11.300 (b)

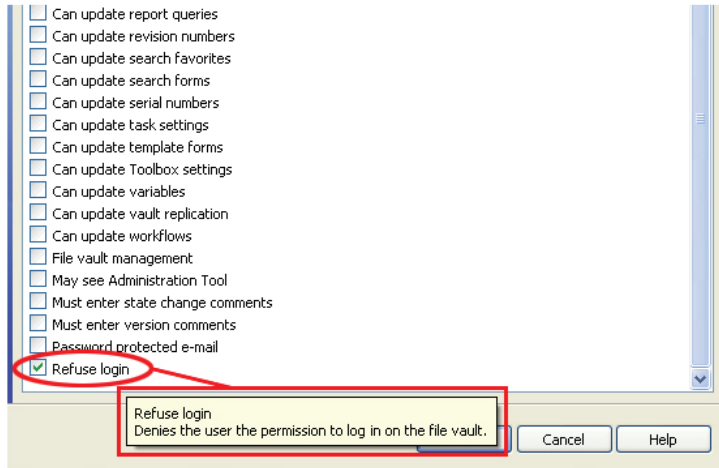
- Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).
- Usually there are set company security policies for password aging etc. Since Enterprise PDM can re-use the existing authentication thru Active Directory or LDAP servers, same password aging policies can be applied to Enterprise PDM Users.





### 11.300(c)

- Following loss management procedures to electronically de-authorize 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
- This is supported through Company policies and procedures. The administrator can choose to refuse login to potentially compromised users.

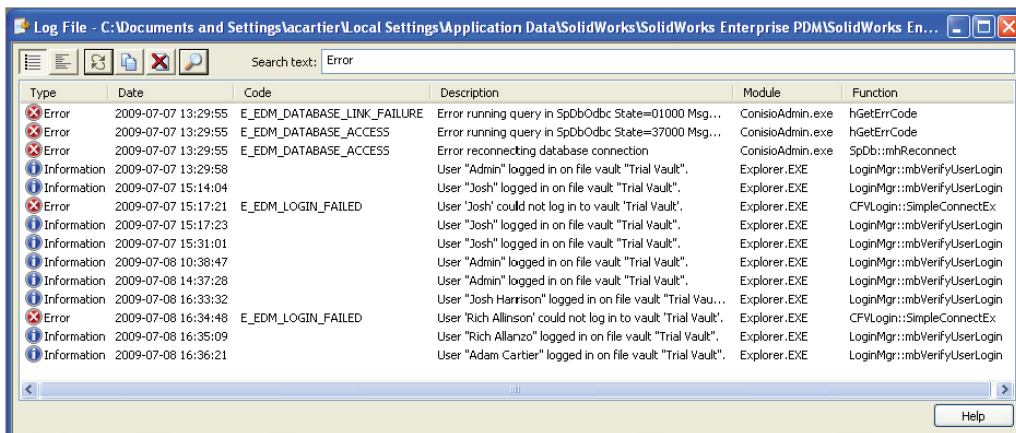


### 11.300(d)

- 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
- This requirement speaks directly to the logging and management of failed login/electronic signature attempts. Enterprise PDM Clients capture all account access activity on that local machine, including failed attempts with timestamps in a log file.

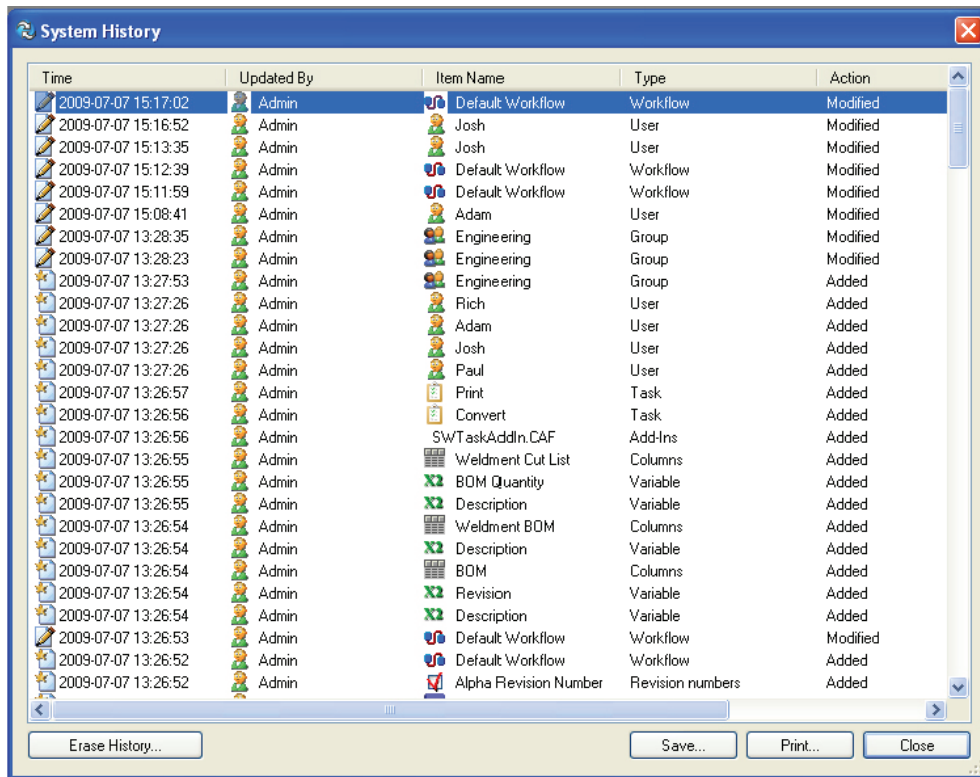
On the Server side, you may generate SQL reports to audit user logins with their respective timestamps and computer names for monitoring any suspicious activity.

Again, since Enterprise PDM can re-use the existing authentication thru Active Directory or LDAP servers, same transaction safeguards can be applied to Enterprise PDM Users. You can customize point at which system is locked down and all further attempts to gain access are denied.



### 11.300(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 is supported by Company procedures. User access management maintains complete history of changes & modifications.



The screenshot shows the 'System History' window in SolidWorks. It contains a table with the following columns: Time, Updated By, Item Name, Type, and Action. The table lists various system changes, including modifications to workflows, user additions, and the creation of new tasks and variables. At the bottom of the window, there are buttons for 'Erase History...', 'Save...', 'Print...', and 'Close'.

Time	Updated By	Item Name	Type	Action
2009-07-07 15:17:02	Admin	Default Workflow	Workflow	Modified
2009-07-07 15:16:52	Admin	Josh	User	Modified
2009-07-07 15:13:35	Admin	Josh	User	Modified
2009-07-07 15:12:39	Admin	Default Workflow	Workflow	Modified
2009-07-07 15:11:59	Admin	Default Workflow	Workflow	Modified
2009-07-07 15:08:41	Admin	Adam	User	Modified
2009-07-07 13:28:35	Admin	Engineering	Group	Modified
2009-07-07 13:28:23	Admin	Engineering	Group	Modified
2009-07-07 13:27:53	Admin	Engineering	Group	Added
2009-07-07 13:27:26	Admin	Rich	User	Added
2009-07-07 13:27:26	Admin	Adam	User	Added
2009-07-07 13:27:26	Admin	Josh	User	Added
2009-07-07 13:27:26	Admin	Paul	User	Added
2009-07-07 13:26:57	Admin	Print	Task	Added
2009-07-07 13:26:56	Admin	Convert	Task	Added
2009-07-07 13:26:56	Admin	SWTaskAddIn.CAF	Add-Ins	Added
2009-07-07 13:26:55	Admin	Weldment Cut List	Columns	Added
2009-07-07 13:26:55	Admin	BOM Quantity	Variable	Added
2009-07-07 13:26:55	Admin	Description	Variable	Added
2009-07-07 13:26:54	Admin	Weldment BOM	Columns	Added
2009-07-07 13:26:54	Admin	Description	Variable	Added
2009-07-07 13:26:54	Admin	BOM	Columns	Added
2009-07-07 13:26:54	Admin	Revision	Variable	Added
2009-07-07 13:26:54	Admin	Description	Variable	Added
2009-07-07 13:26:53	Admin	Default Workflow	Workflow	Modified
2009-07-07 13:26:52	Admin	Default Workflow	Workflow	Added
2009-07-07 13:26:52	Admin	Alpha Revision Number	Revision numbers	Added

Additional information is available on the SolidWorks web site at [www.solidworks.com](http://www.solidworks.com). The SolidWorks eNewsletter, press releases, and information on seminars, trade shows, and user groups are available at [www.solidworks.com/pages/news/newsandevents.html](http://www.solidworks.com/pages/news/newsandevents.html).



Dassault Systèmes SolidWorks Corp.  
300 Baker Avenue  
Concord, MA 01742 USA  
Phone: 1 800 693 9000  
Outside the US: +1 978 371 5011  
Email: [info@solidworks.com](mailto:info@solidworks.com)

[www.solidworks.com](http://www.solidworks.com)