Enabling compliance with PLM audit management

SIEMENS

White Paper

Verifying control of intellectual property and compliance with security and regulatory requirements

You can use Teamcenter® software's PLM audit management capabilities to establish audit logs that track the product and process information managed by your PLM system and to determine how specific changes affect this information. More specifically, audit logs enable you to define what PLM information you want to monitor and to capture how events and project-related activities change that information. Audit logs can also help you determine who participated in these activities. Once this information has been captured, you can search, sort, filter and view the audit log and leverage its records from multiple applications.

Contents

Executive summary

To compete today, companies must collaborate globally within business units and with partners and suppliers throughout the product lifecycle. However, the more people are included in your collaborative product development and manufacturing processes, the more your intellectual property is exposed to misuse or theft.

To keep control of your valuable product knowledge, you need to know what information is being changed, by whom, and in some cases, simply who is accessing it. You need to manage your knowledge throughout the product lifecycle, whether to protect your business or to demonstrate compliance with regulatory requirements.

Teamcenter establishes a product lifecycle management (PLM) environment that is scalable, secure and flexible. Teamcenter facilitates global collaboration across the supply chain by providing a single, secure source of enterprise product and process knowledge. From concept ideation to product retirement Teamcenter supports the complete product lifecycle.

Teamcenter provides PLM audit management capabilities to enable you to track activities managed by your PLM environment and retain it as an audit log. With Teamcenter, you can:

- Configure what you want to be tracked
- Identify what information was changed
- Identify what specific properties of the information were changed
- See who changed it
- See what event triggered the change
- Compare the old and new values of the changed data
- Determine who is accessing your information and performing what actions on it

PLM audit management capabilities are typically used to support configuration audits that track who changed what information and whether there were appropriate authorizations in place to permit these activities. These capabilities also facilitate security audits that determine what information was accessed and by whom. Security audits are highly valued in the aerospace and defense industry but can apply to any industry where intellectual property is crucial for sustaining marketplace competitiveness.

This white paper is intended for technical decision makers who are interested in learning how you can use audit management to improve the business value and performance of your PLM environment.

Role of audit management

Teamcenter audit management capabilities enable you to establish an audit log to track the product and process knowledge managed by your PLM system, as well as to determine how specific events (activities) have affected this knowledge. Typically, one of your system administrators kicks off the PLM audit management process by configuring the audit log and deciding:

- What product and process knowledge should be audited
- What changes to this knowledge should be captured in the audit log (i.e., what information changes, requirements changes and/or project activities should be captured)
- Where the audit log should be stored (i.e., in the Teamcenter database or in separate text file)
- What searches, reports, and custom handling are permitted for the audit log in question

The audit log can also track who accessed what information. You can leverage the Teamcenter security model to protect the audit log by limiting who is permitted to query and/or view specific audited information and whether these privileged users attempted to perform any unauthorized action.

After the initial configuration is complete and tracked events/users have been captured in your audit logs, you are ready to leverage the audit log. At this point, you – as a privileged user – decide:

- How to search, sort, filter and view the audit log using Teamcenter
- How you want to leverage filtered log records from an application (e.g., such as My Teamcenter or Teamcenter Report Builder)

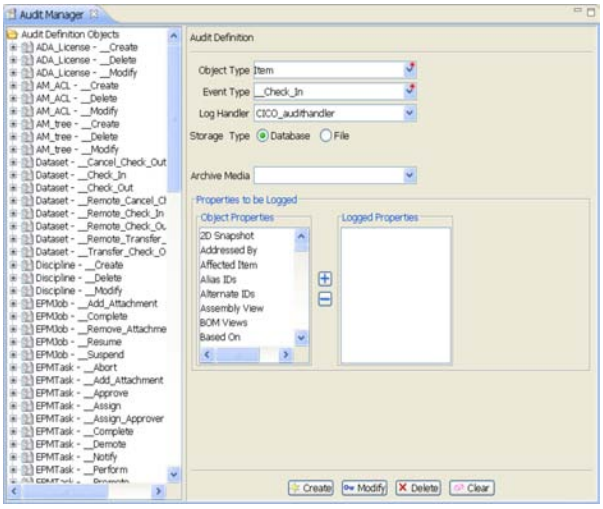
Configuring your PLM audit management solution

System administrators use the accompanying audit manager interface to perform the following basic configuration-related tasks:

Creating audit definition objects System administrators determine what audit logs should be created through the use of audit definition objects. When creating audit definition objects, the administrator must specify the object type, event type, log handler, storage type and object properties. The audit manager interface provides lists that the administrator can view when selecting these items.

Changing audit definition objects If an audit definition object needs to be modified, the administrator can use the audit manager interface to display and modify the audit definition object.

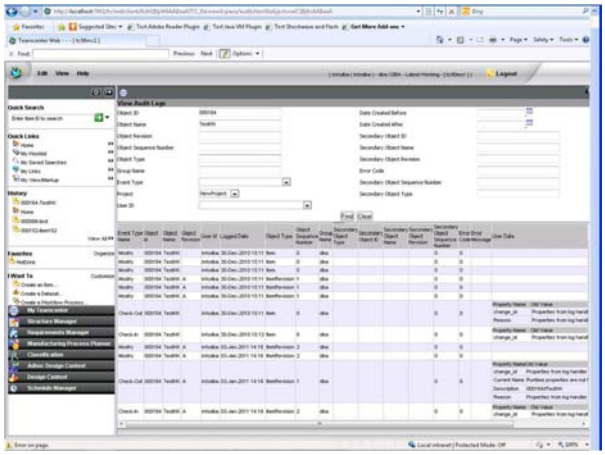
Defining permitted audit log activities The system administrators can use the audit manager interface to determine storage option. Archiving, log searches, custom reports and custom handling are permitted when using the audit log.



Audit manager interface.

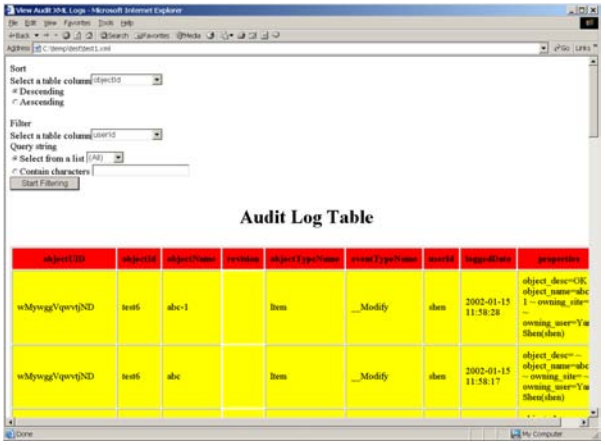
Searching audit logs

Privileged users (i.e., users who are permitted access for the purpose of auditing information and performing audit-related functions) employ the following audit dialog interface to search an audit log stored in the Teamcenter database. During the search process, users typically employ the interface to sort and filter their searches so that they can locate audit log records of particular interest. They can also use the dialog to view the records they have selected.



Searching audit log.

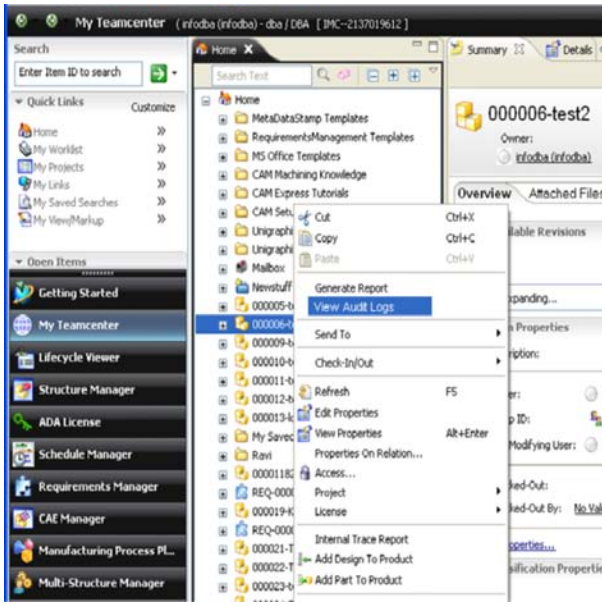
Alternatively, users whose audit logs have been stored in external text files can use provided XML program files to view the audit log in a web browser.



Using web browser to view audit log stored in external text file.

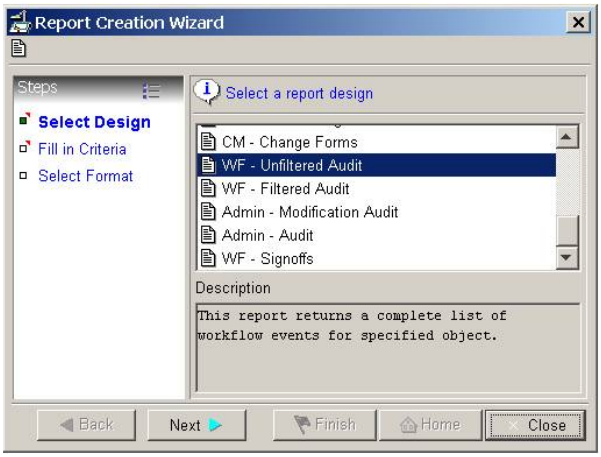
Viewing and leveraging audit log records

Users can use multiple applications – such as My Teamcenter or the Teamcenter Report Builder – to search, leverage and/or report on selected records. For example, you can access basic audit information through the **View>Audit** menu in My Teamcenter. Other My Teamcenter capabilities are supported, including the use of **View>Audit>View>Signoff Report** to generate a history report for given information objects or workflow processes. This capability is especially valuable for identifying when given events (such as review/approval processes, work tasks, notification procedures and other activities) were started and completed (or their current status), who has signed off, who was notified and who is primarily responsible for the task – as well as other pertinent task-related information.



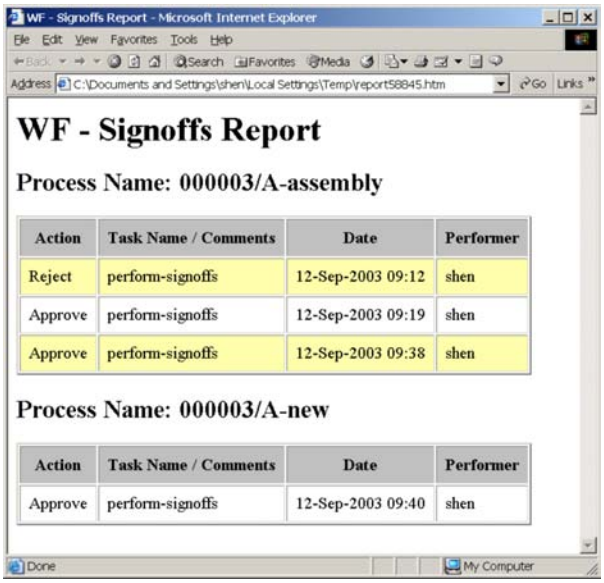
Initiating audit log view for My Teamcenter.

An alternative viewing approach is shown in the accompanying screen, where the Teamcenter report creation wizard is used to search audit records stored in the Teamcenter database, generate an audit report and design a report for a web browser, spreadsheet or text window.



Using Teamcenter report creation wizard to design an audit log report.

Taking this process to the next step, the accompanying screen illustrates how an audit log report created through the Teamcenter report designer can be viewed in a web browser.



Conclusion

Using Teamcenter software's PLM audit management capabilities, you can track specific history changes managed by your PLM environment and retain them as an audit log. More specifically, you can:

- Configure what you want to be tracked
- Identify what information was changed
- Identify what specific properties of the information were changed
- See who changed it
- See what event triggered the change
- Compare the old and new values of the changed data

While these capabilities are most commonly applied in the aerospace and defense industry, where it is essential to show proof of compliance with U.S. Department of Defense and other government agency regulations, audit management is becoming increasingly important in the automotive, high tech and electronics industries, as well as in other industries that require traceability of specific changes of interest.

In addition, you can leverage these PLM auditing capabilities for portfolio decision making by identifying intellectual property of high interest to your user communities. By determining what intellectual property is most frequently accessed, decision makers are able to learn what information is most important to their company's knowledge users, value chain and/or partners.

By leveraging PLM audit management to prove traceability and compliance, you can improve the business value and performance of your PLM environment.

About Siemens PLM Software

Siemens PLM Software, a business unit of the Siemens Industry Automation Division, is a leading global provider of product lifecycle management (PLM) software and services with 6.7 million licensed seats and more than 69,500 customers worldwide. Headquartered in Plano, Texas, Siemens PLM Software works collaboratively with companies to deliver open solutions that help them turn more ideas into successful products. For more information on Siemens PLM Software products and services, visit www.siemens.com/plm.

www.siemens.com/plm

X7 25138 6/11 C

Siemens Industry Software

Headquarters
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
1 972 987 3000
Fax 1 972 987 3398

Americas
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
1 800 498 5351
Fax 1 972 987 3398

Europe
3 Knoll Road
Camberley
Surrey GU15 3SY
United Kingdom
+44 (0) 1276 702000
Fax +44 (0) 1276 702130

Asia-Pacific
Suites 6804-8, 68/F
Central Plaza
18 Harbour Road
WanChai
Hong Kong
852 2230 3333
Fax 852 2230 3210