Security management

SIEMENS

White Paper

Leveraging Teamcenter security capabilities to protect your intellectual property and enable secure collaboration

You can use Teamcenter® software's security management capabilities to establish a security model for your product lifecycle management (PLM) environment and support multiple security-related initiatives. Once your security model is in place, you can use it to protect your environment's underlying systems and databases from unauthorized access/use, as well as to control how individual pieces of product and process information can be used and by whom. Teamcenter supports export control initiatives such as the International Traffic in Arms Regulations (ITAR), as well as standard internet security deployments and other additional security-related programs.

Contents

Executive summary

Today's companies face a challenging dilemma. On one hand, they need to vigorously engage global partners in commercial initiatives as they pursue many of their most promising revenue-generating opportunities. Typically, these opportunities involve forming strategic alliances with partners and suppliers to take advantage of both local and international competencies.

On the other hand, sharing information externally raises numerous security concerns, including but not limited to the need to protect intellectual property, as well as to comply with various contractual obligations and regulatory requirements. In essence, today's companies must be able to share information extensively as part of their collaborative product development and manufacturing processes, while at the same time protecting their intellectual property rights and mitigating the legal, financial and business risks of non-compliant and/or insecure security-related practices.

To address these issues, Teamcenter enables you to approach security management as a strategic business initiative. You can leverage the following security-related Teamcenter capabilities to establish a secure PLM environment that lets your company share its intellectual capital with entitled suppliers and customers in accordance with a wide variety of security-related restrictions.

Authentication Teamcenter determines the identity of every user who attempts to access your PLM environment, making certain that every user is, in fact, who he or she claims to be and that this person can only access data resources to which he or she is entitled.

Authorization Teamcenter determines what information each user is allowed to access based on the user's identity and/or the role, group, organization or project to which the user is assigned.

Audit Teamcenter provides comprehensive and configurable auditing tools that you can use to log detailed user activities performed against this controlled information and to analyze these activities using Teamcenter software's reporting and analytics capabilities or commercial off the shelf (COTS) tools.

Authorized data access You can leverage Teamcenter to establish a standards-based Authorized Data Access (ADA) model that facilitates item-level access control over all of the product, process and manufacturing information managed by your PLM environment, including documents, CAD models and JT™ data.

Taken together, these Teamcenter capabilities provide fine grain controls needed to protect your intellectual property, as well as the confidence you need to share information while vigorously pursuing a globalized business strategy. Just as importantly, best practice companies can leverage Teamcenter to approach security management as a strategic initiative that mitigates the legal and financial risks associated with sharing intellectual property in support of their globalization objectives. With these considerations in mind, Teamcenter provides the following security-related advantages and business benefits.

Improved security Teamcenter enables your administrators to control and restrict information access on the basis of authentication, authorization and entitlement specifications.

Reduced risk Teamcenter protects against future litigation by enabling you to deliver proof of regulatory and/or best practice compliance, thereby eliminating your exposure to costly penalties and enabling you to rapidly respond to legal discovery motions.

Greater productivity Teamcenter enables entitled users to easily and quickly locate controlled information by focusing their searches on active, up-to-date and accurate information and eliminating time wasted using outdated, inappropriate or irrelevant data.

Reduced cost Teamcenter enables your company to minimize its security-related administrative overhead by providing a single point of administration and audit control for your PLM environment that is compatible with the industry standard security infrastructure and its related conventions.

Authentication, authorization and entitlement

Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Teamcenter provides a common framework to facilitate third-party authentication, including user authentication to identify users as they log-in to the PLM environment through a single challenge and at the directory level. It also uses synchronization techniques to identify users as they access Teamcenter-provided applications.

Teamcenter security services provide support for standards-based username/password validation using commercial and standards-based directory servers, such as Active Directory or any server supporting the Lightweight Directory Access Protocol (LDAP) version.

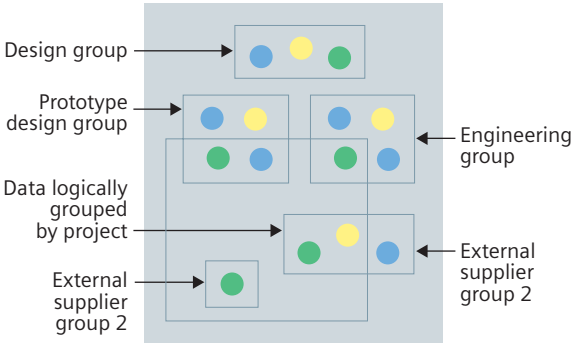
In addition, all Teamcenter software clients support secure internet communication protocols (HTTP with or without support for Secure Sockets Layer or HTTPS SSL encryption) so that the firewalls and proxies implemented in a data center can further prevent unwanted persons for accessing Teamcenter resources.

Authorization

As indicated by the accompanying table, Teamcenter facilitates authorization for users at six levels, enabling administrators to easily control user access to information managed by your PLM system. Teamcenter determines what information each user is allowed to access based on the user's identity and/or the role, group, organization or project to which the user is assigned. Teamcenter determines whether individual users have the rights/privileges required to perform a specific function or access specific information at any given point in time. Typically, Teamcenter does this by executing business rules against the authorization defined for the information in question.

Level	Advantages
User	Controls information access on the basis of an individual user's Teamcenter login user name and password
Person	Controls information access on the basis of an individual user's real-world identification, such as a person's name, address and phone number
Group	Provides information access to collections of people who function within an identified group
Hierarchical group	Provides information access to groups of people who function within a larger hierarchical group
Role	Controls information on the basis of the role that people perform within an identified group (a group can include people who perform multiple roles while a single role can be performed in multiple groups)
Project	Controls information access by indicating that only specific types of information are available for use by multiple groups (for example, you can limit access to an information-related work product to identified project teams, development teams, suppliers and customers)

Authorization example



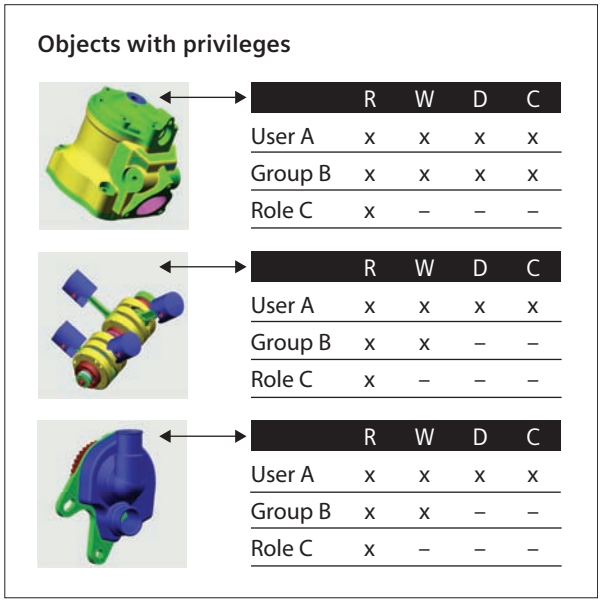
Authorization-controlled information is combined with the Teamcenter access manager, a rules-based access control system that you can leverage two ways.

- By creating rules-based access control lists (ACLs) and rules conditions configured in a rule tree. Each rule tests both the identity and affiliations of the user and plus characteristics of the data to grant or deny read and write privileges.
- By creating specific ACLs attached to individual information, which enables you to model exceptions to the rules-based system for specific pieces of data

In both instances, these controls can be used to specify what privileges have been assigned to individual users in terms of specific functions they are allowed to perform or specific information they are allowed to access.

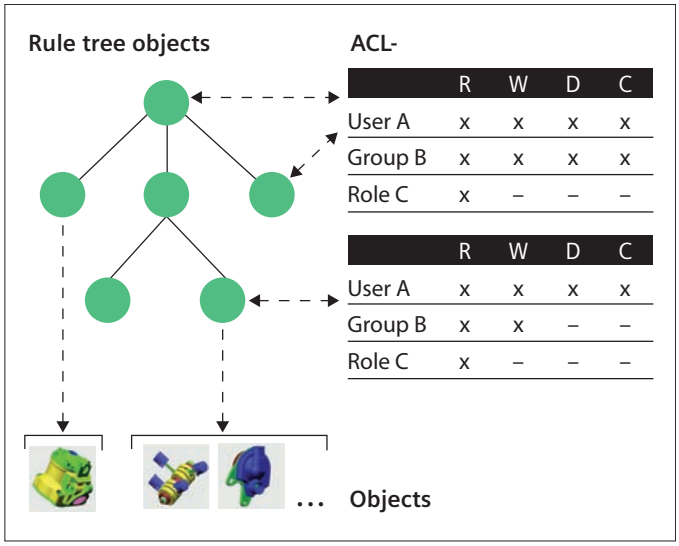
Entitlement concepts – object-based vs. rules-based control list (ACL)

Object-based



- Privileges are directly attached and stored with the objects
- Subsequent modifications of privileges may cause intensive processing

Rules-based



- Privileges are defined independent within global ACL-objects
- The rule tree structures the object spectrum while facilitating globally defined ACLs (for run time evaluation)
- The system administrator defines privileges according to a given access strategy of a company
- Rules-based control lists are highly flexible in terms of their ability to support subsequent modifications

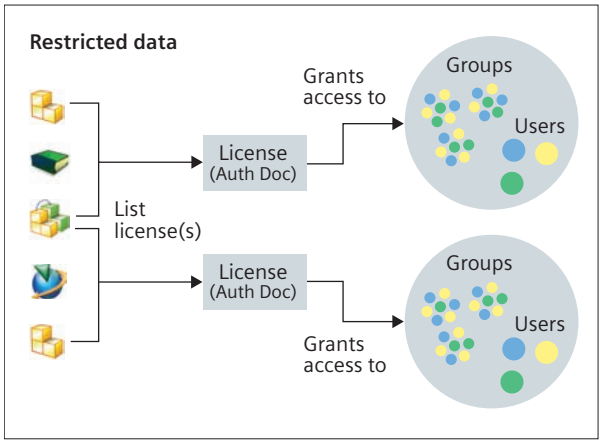
Authorized Data Access

Teamcenter uses an Authorized Data Access model (ADA) to enable you to securely manage sensitive information and other highly valued intellectual property in accordance with export control regulations such as the U.S. International Traffic in Arms Regulations (ITAR). Regardless of whether suppliers, partners or company employees are working with your intellectual property, you can leverage Teamcenter to reduce the effort needed to comply with requirements for exporting regulated information. Similarly, you can also use the same Teamcenter capabilities to comply with corporate policies for enforcing legal requirements documented in non-disclosure agreements and supplier contracts.

Teamcenter restricts access to information on the basis of terms and conditions specified by authorizing documents, including export licenses, technical assistance agreements (TAA), non-disclosure agreements and supplier controls. You can use Teamcenter to limit information access on the basis of the user's nationality, geography, security clearance, and the access time period granted by authorizing documents.

You can use Teamcenter software's ADA capabilities to establish information access control by:

- Identifying specific users as restricted
- Identifying given information as restricted
- Enabling restricted users to access restricted information through the use of authorizing documents
- Validating access when any restricted user attempts to access ADA-protected information



Using Teamcenter to limit restricted data through use of "authorizing documents".

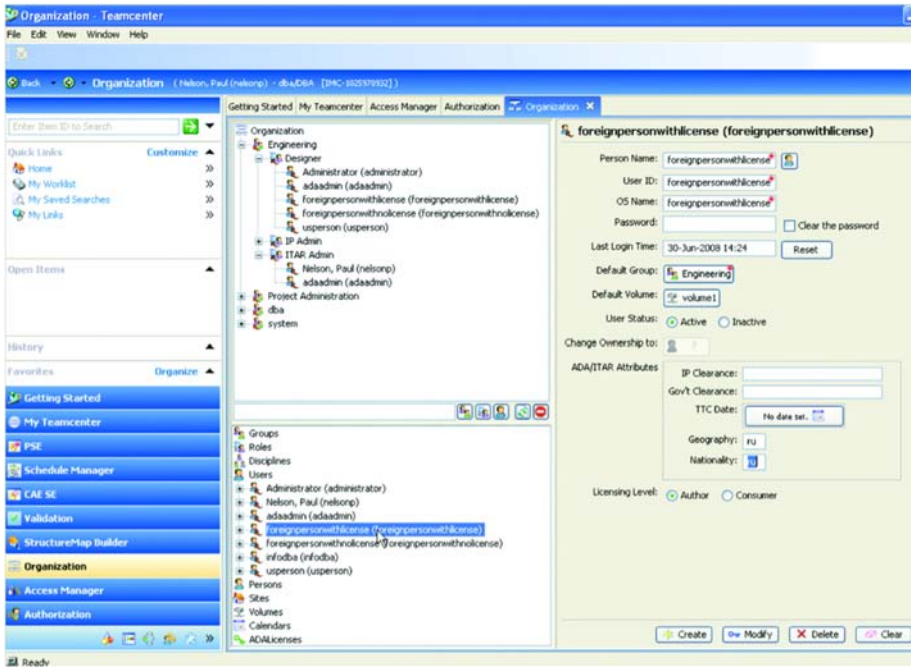
All information (including documents, CAD models and JT data) managed by Teamcenter can be controlled through ADA. In addition, Teamcenter provides out-of-the-box rules that let you restrict access of controlled information to "US persons." You can use technical authorizing agreements (export licenses) to grant individuals or groups access to controlled information. For example, a "foreign person" can be granted access to an ITAR-controlled document through an export license under terms authorized by the document.

Our ADA solution is especially adept at reducing the administrative activities associated with establishing and enforcing export controls while at the same time providing the ability to exercise these controls as flexibly as possible.

Auditing capabilities

Teamcenter also provides comprehensive and configurable auditing tools so that your company can monitor detailed user activity against controlled information and log this activity to external log files or to the Teamcenter database. Subsequently, you can analyze these logs using Teamcenter software's reporting and analytics capabilities or export them for later analysis using commercial off the shelf (COTS) tools such as Microsoft Excel.

You can leverage Teamcenter auditing capabilities to verify that your security requirements are intact, as well as to validate that your export controls have been met by performing regulatory-related security audits.



Using Teamcenter to enable administrators to grant access to an ITAR-controlled document via an export license.

Frequently asked questions

Does Teamcenter support "two factor" user authentication (such as SMART cards)?

Teamcenter security services can be configured to accommodate devices such as SMART cards with Kerberos on certain platforms.

Does Teamcenter use a FIPS 140-2 certified encryption library?

A FIPS 140-2 certified Teamcenter library is provided with Teamcenter; it is used for Secure Socket Layer (SSL) support.

Does Teamcenter support either Active Directory or LDAP-compliant directory servers for username/password authentication?

Teamcenter security services support authentication using either Microsoft Active Directory or other directory servers that support the LDAP v3 protocol.

Does Teamcenter support either Active Directory or LDAP-compliant directory servers for user group or role authorization?

Teamcenter keeps its own internal store of group and role authorizations. However, user group and role information can be updated from a directory server using one of two tools provided for that purpose.

Does Teamcenter support export regulations or supplier/joint venture "need to know" agreements?

The Teamcenter Advanced Data Access feature enables you to configure security to support and document compliance for security programs such as the ITAR and supplier confidentiality agreements.

Conclusion

Teamcenter software's security management functionality enables you and your external partners, suppliers and customer to share product, process and manufacturing information in a secure PLM environment with confidence that each participant's intellectual property is protected in accordance with established compliance-related conventions. Teamcenter security capabilities include authentication, authorization and entitlement features that support industry standards and proven best practices.

Just as importantly, Teamcenter security capabilities are designed to facilitate a cost effective security infrastructure that will enable you to assertively pursue today's promising global commercial initiatives – thereby transforming security from a challenging concern into a strategic advantage.

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

X4 25097 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