TEAMCENTER

Organization Management Using Groups, Roles, and Users

Teamcenter 2412

SIEMENS

About Siemens Digital Industries Software

Siemens Digital Industries Software is a global leader in the growing field of product lifecycle management (PLM), manufacturing operations management (MOM), and electronic design automation (EDA) software, hardware, and services. Siemens works with more than 100,000 customers, leading the digitalization of their planning and manufacturing processes. At Siemens Digital Industries Software, we blur the boundaries between industry domains by integrating the virtual and physical, hardware and software, design and manufacturing worlds. With the rapid pace of innovation, digitalization is no longer tomorrow’s idea. We take what the future promises tomorrow and make it real for our customers today. Where today meets tomorrow. Our culture encourages creativity, welcomes fresh thinking and focuses on growth, so our people, our business, and our customers can achieve their full potential.

Support Center: **support.sw.siemens.com**

Send Feedback on Documentation: **support.sw.siemens.com/doc_feedback_form**

Contents

Optional organizational setup tasks

Maintaining your organization

Setup required by Content Management application

1. Getting started with Organization

What is Organization?

The Organization application enables you to create and maintain your company's organization within Teamcenter by organizing user accounts and their respective permissions and user groups. User accounts help you:

- Track changes to objects.
- Control access and privileges.
- Manage default object ownership.

Use this administrative application to perform tasks like:

- Viewing information in your organization
- Setting up your organization for the first time
  - Required organizational tasks:
    - **Assigning administrative privileges**
    - **Establishing sites for each database that is used**
    - **Defining the structure of your organization**
    - **Defining volumes for your site**
    - **Assigning roles to users**
    - **Defining groups**
    - **Creating persons and creating user accounts**
  - Optional organizational tasks:
    - **Defining disciplines**
    - **Defining calendars**
    - **Defining part libraries**

- Setup required by Content Management application:
  - **Defining languages**
  - **Defining graphic priority lists**

Frequently asked questions for Organization

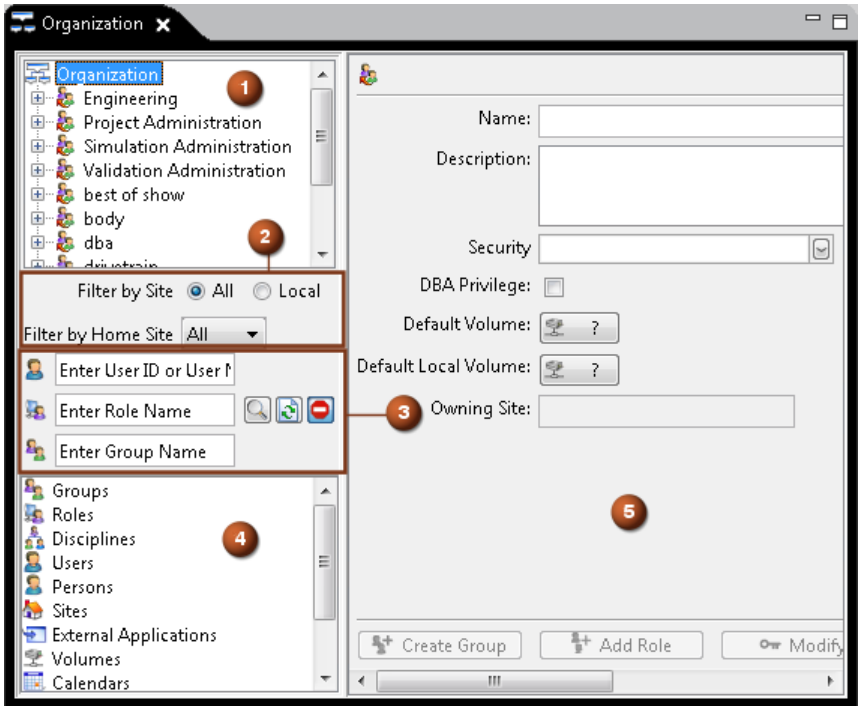
Before you create your virtual organization, consider these points.

Consideration	Description
What is the best way to structure my organization?	Creating your virtual organization based on your company's organization chart is not always a good idea because the structure of your company is always subject to change. You should look for a stable organization hierarchy that requires little or no changes.
How can I quickly set up my organization?	The **make_user** utility is especially helpful when first setting up your organization. This utility allows you to create your organization from a command line or script. It enables you to load your entire organization with one command.
What is a good suggestion for setting the user ID?	When setting the user ID, use your Human Resource department's recommendation as a possibility for a unique identifier.
What kind of security can I set for groups?	You can set different types of security: • Project-level • Authorized data access (ADA) Allows or restricts access to data based on clearance levels and data classification • International Traffic in Arms Regulations (ITAR)
What do I do if a user is out of the office for an extended period of time (for example, medical leave)?	You can **change the status of a user** from active to inactive. However, you cannot deactivate group members if they have any pending Workflow tasks. You must first delegate these tasks to another group member and then deactivate the user. You can use the **global_transfer** utility to transfer one user's tasks to another user. You can also reassign the user's tasks using the My Teamcenter inbox feature.
When users change groups within the organization,	When users leave the organization or change groups or roles within the organization, you can **deactivate their membership** within a group.

Consideration	Description
how can I deactivate their membership within a group?	This prevents them from logging on to the system as a member of the group and denies them access to information related to their previous group and role.
A user is leaving the company. What do I need to do?	Because database objects are owned by individual users, you must determine what to do with any objects owned by the user before deleting the user from the database. • Before deleting the user object from the organization, you must remove all relationships. • Also, you must delete all of the user's owned items or transfer the owned items to another user.

Exploring the Organization interface

Organization interface overview



1	**Organization** tree	The **Organization** tree enables you to view the structure of your organization at a glance. By expanding and collapsing branches of the tree, you can view and manage the organizational structure.

		Selecting a node starts **Organization** wizards used to create groups, subgroups, roles, disciplines, and users.
2	**Filter by Home Site** box	Use the **Filter by Home Site** box to filter objects (group, role, or user) by owning location.
3	Find boxes	Use the find boxes to filter the **Organization** tree to find groups  , roles  , and users  within the organization. You can also use the **find boxes** to reload the **Organization** tree and to locate inactive group members.
4	**Organization List** tree	The **Organization List** tree enables you to view and manage the components of your organization by listing groups, roles, disciplines, users, and persons. You can also use the **Organization List** tree to manage sites, external applications, volumes, and calendars.
5	Definition pane	Displays the properties for the selected Organization object.

Organization buttons

Buttons	Description
	Externally managed person definition.
	Remotely managed person definition.
	Internally managed person definition.
	Externally managed user definition.
	Remotely managed user definition.
	Internally managed user definition.
	Externally managed group definition.
	Remotely managed group definition.
	Internally managed group definition.
	Externally managed role definition.

Buttons	Description
	Remotely managed role definition.
	Internally managed role definition.

What are perspectives and views?

Within the rich client user interface, application functionality is provided in *perspectives* and *views*.

View	The basic display component that displays related information in a UI window.
Perspective	A collection of one or more views and their layout.

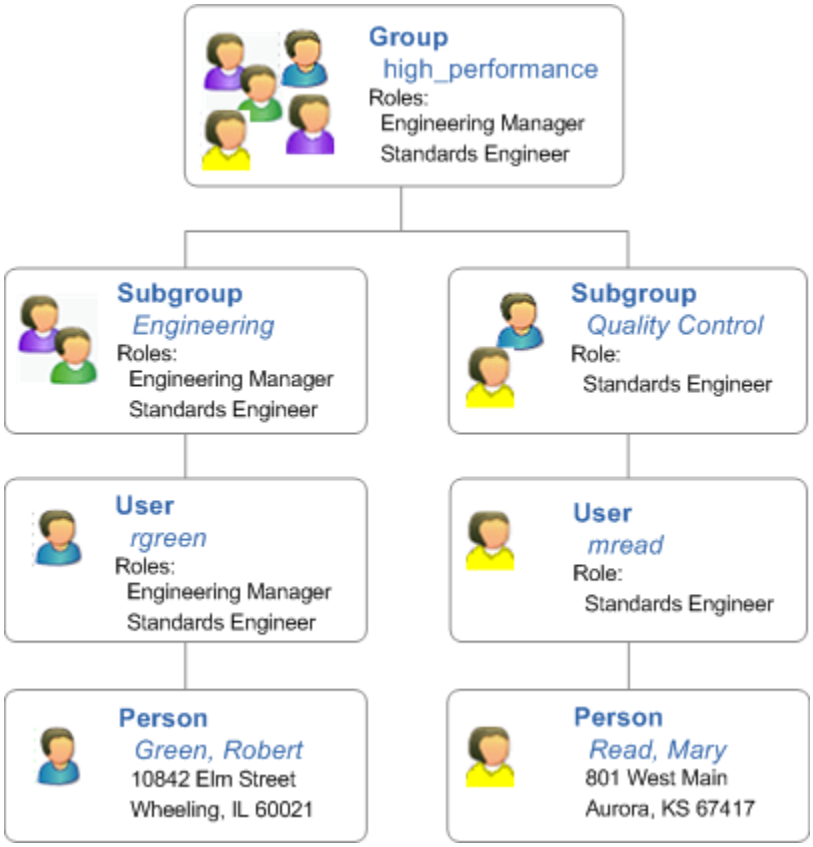
Some applications use a perspective with multiple views to arrange how functionality is presented. Other applications use a perspective with a single view.

You can use the **HiddenPerspectives** preference to prevent the display of some Teamcenter perspectives in the rich client.

If your site has online help installed, you can access the application and view help from the rich client **Help** menu.

Basic concepts for using Organization

An *organization* is made up of groups. Groups contain subgroups, users, and persons.



- A *group* is a grouping of users who share data.

  You can configure access to data owned by the group by:

  - Using the **Security** setting, which allows or restricts access to data.
  - Setting authorized data access (ADA) and International Traffic in Arms Regulations (ITAR), which allows or restricts access to data based on clearance levels and data classification.

- A *subgroup* is a group with another group designated as its parent. A subgroup can also be designated as a parent group itself. The position of subgroups within the Organization hierarchy can be managed by parenting and reparenting groups.

- A *role* represents specific skills and/or responsibilities. The same roles are typically found in many groups. The system grants data access based on group and role.

- A *user* can belong to multiple groups and must be assigned to a default group. Each user in the group is assigned a role.

  In addition, you can associate the following with users by:

  - Creating a calendar, which allows you to set days off, holidays, and hours in a day for individual resources.

- Setting ADA and ITAR attributes to allow or restrict data access.
- Setting the licensing level to determine whether the user can create and modify data or only view data.

- A *person* is a definition containing real-world information about each Teamcenter user, such as name, address, and telephone number.

Within Organization you can view both local and replicated (remote) objects.

> Note:
>
> Replicated (remote) objects (user, group, role, and person) have two green dots beside them to designate them as remote objects  .

Basic tasks using Organization

Building Organization hierarchies

The Organization application supports three methods of building the organization hierarchy:

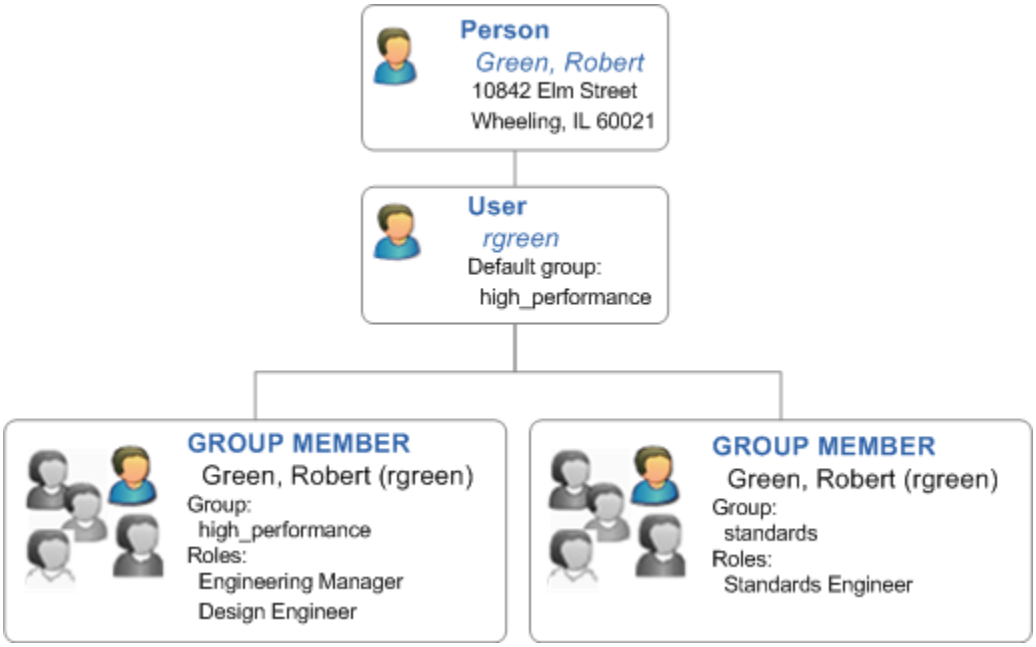
- Use the Setup Wizard when you need to set up multiple users using bulk data from an input file. This method speeds up the creation process. First you create an input file of user data, next use Setup Wizard to map the data. Then, once this data is mapped to create related elements in Teamcenter, you can add additional associations between users, volumes and groups.
- Use the **Organization** tree wizards to build the hierarchy from the top down.
- Use the **Organization List** tree to build the hierarchy from the bottom up.

Additionally, the **make_user** utility allows you to create your organization from a command line or script. Use this utility to:

- Increase productivity: Load your entire organization with one command.
- Perform disaster recovery: Back up your organization.
- Perform migration: You can populate your test and production environments.

Building the hierarchy using the Organization List tree

When building the hierarchy from the bottom up, a person definition precedes a user definition, which in turn precedes a subgroup and/or group definition. Each definition is constructed separately and manually associated to the other levels of the organization hierarchy.



For example, user X is hired by ABC Company as a designer. User X is working as a member of a new development group responsible for designing products A and B. The following sequential actions are required to add user X to the organization using the **Organization List** tree:

1. Create a person definition reflecting user X's real-world information, such as address and telephone number.

2. Create a user definition containing system-related information such as **Person Name** (this associates the person definition to the user definition), **User ID**, **OS Name**, and **Password**.

3. Create the groups. You create a parent development group and Product A and B subgroups. One of these groups is specified as the default group in user X's user definition.

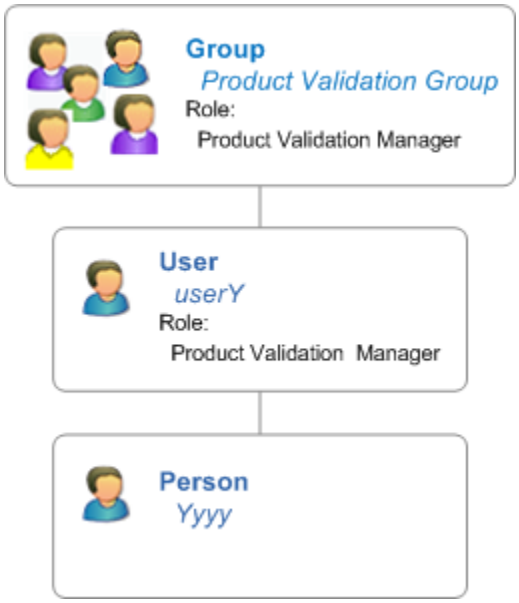
4. Create the Designer role. You assign the role to the subgroups using the **Groups** pane.

   To create persons, users, groups and subgroups, and roles by this method, select a node from the **Organization List** tree and use the corresponding pane to define the properties of the new entity.

Building the hierarchy using the Organization tree

Using the **Organization** tree, wizards are available to guide you through the creation of the groups and subgroups, users, roles, and persons that make up the organization hierarchy.

You can begin at the highest level in the **Organization** tree and seamlessly traverse the hierarchy, creating new objects and/or adding existing objects using the Organization wizards (Group, Role, and User). User and person definitions can be created simultaneously using the Organization User wizard.



For example, user Y is hired by ABC Company as product validation manager for a new group being established to assure the quality of ABC Company's products. In one seamless process, you can add the new product validation group, the product validation manager role, and user Y's user and person definitions to the ABC Company **Organization** tree using the Organization wizards. You:

- Create the new parent group, Product Validation, within the **Organization** tree.
- Add the role of Product Validation Manager to the Product C Development group.
- Add the user and person definitions to the role/group.

To create new definitions or add existing persons, users, groups and subgroups, and roles to the organization using this method, select a node from the **Organization** tree and start one of the Organization wizards from within the corresponding pane.

You can also perform organization management by creating, adding, modifying, and in some cases removing objects from the hierarchy, from within the **Organization** tree.

Note:

- You cannot delete organization objects from the database from within the **Organization** tree. You must use the **Organization List** tree instead.
- Use the **TC_org_tree_expansion** preference to enable the expansion of the **Organization** tree based on the number of tree nodes and to increase performance.

Creating your virtual organization

As a Teamcenter administrator, you use the Organization application to create and maintain your company's virtual organization within Teamcenter. Because your company's organizational structure can change over time, it is important when defining groups and roles that you look for a stable organization hierarchy that requires little or no change.

> Note:
>
> For group, role, user, and person objects, the **Owning site property** field specifies the site that manages the object. The **Home site property** field specifies the working site for the object. Both fields are displayed for each of these objects. However, if one of the property fields is null, it indicates the object is local.

The basic process of creating a virtual organization includes the following stages:

1. Establish **Teamcenter sites**.

2. Define the structure of your organization.

   Roles, volumes, and persons are independent definitions. Any of these can be created without consideration of the other definitions.

   a. **Create volumes**.

   b. Enable File Management System (FMS) control of new volumes.

   c. **Create roles**.

   > Warning:
   >
   > Do not delete the roles provided with Teamcenter. They are required for Teamcenter to function properly.

   d. **Create groups and subgroups**.

   > Warning:
   >
   > Do not delete the **system** group provided with Teamcenter. It is required for Teamcenter to function properly.

   Groups and users are dependent definitions. To create group and user definitions, other definitions must exist:

   - Group definitions require that a role is defined and suggest a volume be defined.

- User account definitions require a person definition and a group definition.

e. **Add roles to groups**.

3. Create **users** and persons.

   a. **Create person definitions**.

   b. Create user accounts.

      The **make_user** utility allows you to create your organization from a command line or script.

Exporting Organization objects

You can replicate organizational objects (users, groups, roles, persons, and group members) using the Multi-Site export function to provide a global organization. A global organization allows centralized administration for organization data using Multi-Site Collaboration technology. You select a central site in your environment to store the master copies or organization data' the other sites contain read-only replicas. You can make changes at the master site and synchronize the replicas at the other sites. Global organization objects can be imported and exported much the same as other Teamcenter objects, with the exception that they cannot have their ownership transferred to another site from the master site.

> Note:
>
> Existing sites that already have identical organization structures, also known as cloned organization objects, must migrate the structure to the replicated model to establish a true global organization.

These exported (replicated) objects are created with the owning site maintaining the master object, as with other Teamcenter objects. You can also synchronize the replica objects to the master objects using the **data_sync** utility.

The user objects are assigned a home or working site attribute that allows you to use them in global workflows. This allows Teamcenter to deliver a task to the correct user at the correct working site.

A user object is also assigned an attribute that controls the remote sites that a user can interactively log on to. Users can always log on to their home site.

As with other replicated objects, master Organization objects cannot be deleted until the export record for the replica objects is deleted. Master objects can be modified at the owning site. At the replica site, you can modify the following information:

- Replica user objects:
  - Last logon time can be reset using the **Reset** button.

  - Default volume can be updated.
  - Default local volume can be updated.
- Replica group objects:
  - Default volume can be updated.
  - Default local volume can be updated.

When you select an object from the **Organization List** tree, each object has different options that allow more flexibility than if you select them from **Organization** tree.

- User objects

  When you select a user object for remote export, you can select from the following options:

  - **All roles in the Default Group**

    If this option is not selected, only the default role is exported. Otherwise, all roles for this group are exported.

  - **All roles in all groups**

    If this option is selected, all group member roles associated with the user are exported.

    The group and role for the **GroupMember** object must already exist at the target site prior to exporting the user; otherwise, the export fails.

- Group objects

  When you select a group object for remote export, you can select from the following options:

  - **All roles in Default Group**

    If this option is not selected, only the default role is exported. Otherwise, all roles for this group are exported.

  - **All subgroups**

    If this option is not selected, no subgroups are exported. Otherwise, all subgroups are exported. Parent groups are always exported.

  - **All group members**

If this option is not selected, no group members are exported. Otherwise, all group members of all roles selected for export are exported.

- Role objects
- Person objects

  When you select a person object for remote export, there are no special options from which to choose.

Export Organization objects

1. Select an Organization object, for example, a role.

   You can export the following Organization objects: roles, groups, persons, and users.

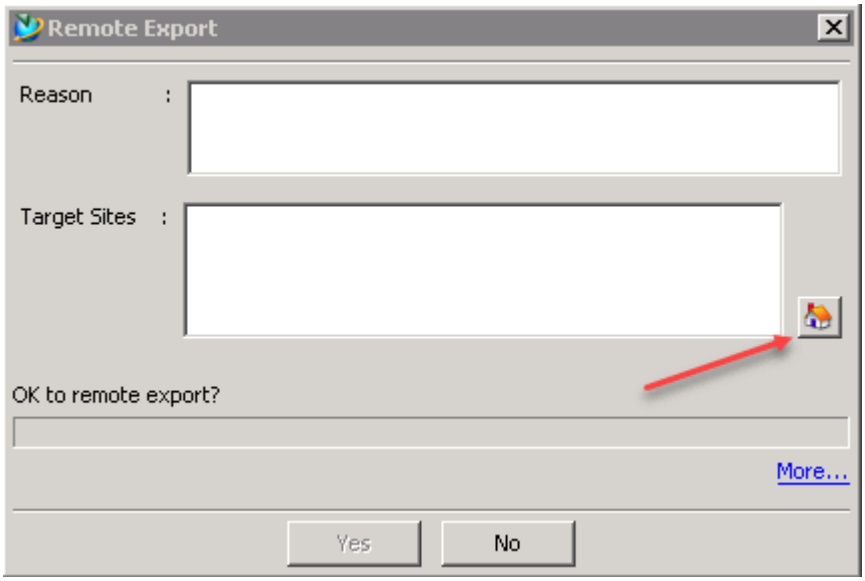
2. Choose **Tools→Export→Remote Export**.

   Teamcenter displays the **Remote Export** dialog box.

   The appearance of the **Remote Export** dialog box can vary depending on the object you select for export and whether you select it from either the **Organization** tree or the **Organization List** tree.

   > Caution:
   >
   > To support export of Teamcenter objects among multiple sites, site IDs must agree. Consider two sites: site **A** and site **B**. To export objects to one another, each site must be defined at both sites using exactly the same site ID in each definition. This is especially important if you are using Multi-Site Collaboration.

3. Select the target remote sites by clicking  next to the **Target Sites** box.



The system displays the **Remote Site Selection** dialog box.

Using administration data reports for Organization

What are administration data reports?

There are two main types of administration data reports that can be generated:

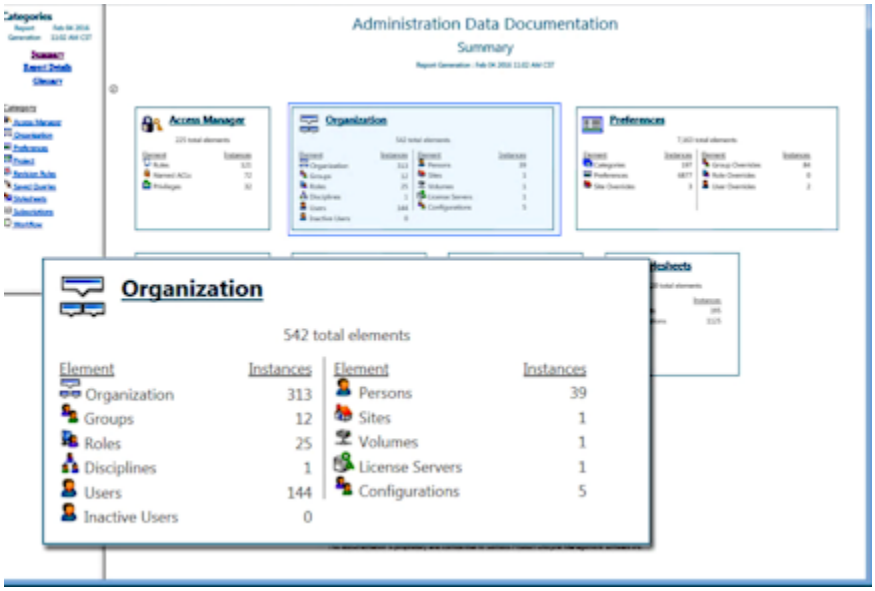
- **Administration data documentation report**

  Shows the specified administration data for the site where you run the utility or for an export package.

- **Administration data comparison report**

  Shows the differences between the administration data at two sites.

To view an administration data report, browse to the output directory location and select the **index.html** file.



Using the administration data documentation report

The *administration data documentation report* is an HTML report of administration data at a site. It is generated using the **generate_admin_data_report** utility.

This report is useful for generating a report about your organization. For instance, it breaks down your organization into a number of elements, for example:

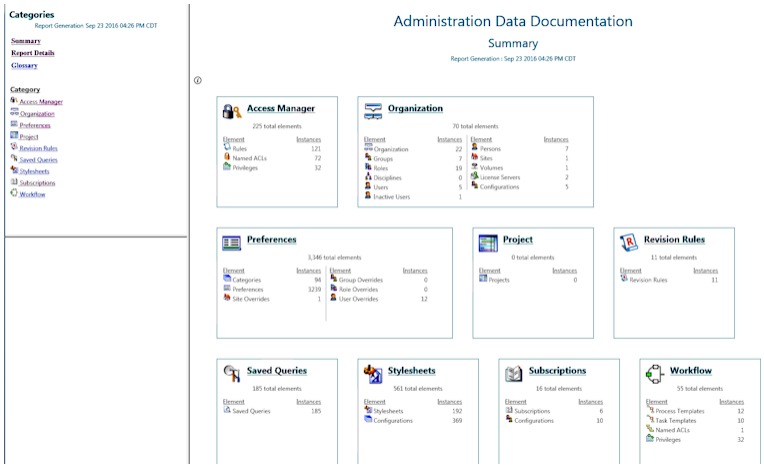
- Groups
- Roles
- Users
- Inactive users
- Persons
- Sites
- Volumes

The administration data documentation report is an HTML-style report that displays administration data for the site where you run the utility or for an export package.

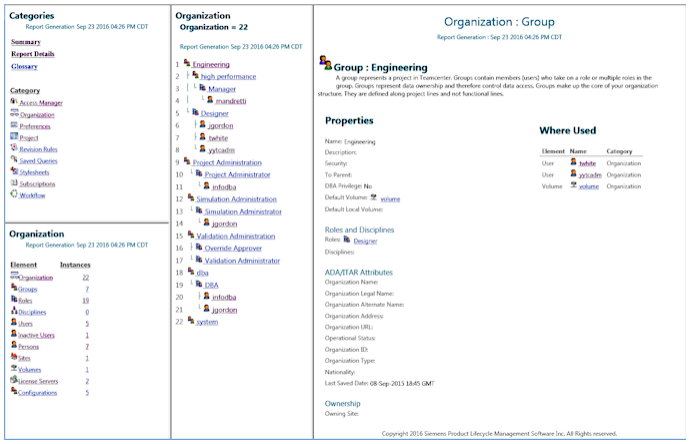
For example, to generate the report for your site, you can enter the following command:

```
generate_admin_data_report -u=admin-username  -p=admin-password
     -g=dba -adminDataTypes=all -outputDir=C:\temp\admin_data\siteA
```

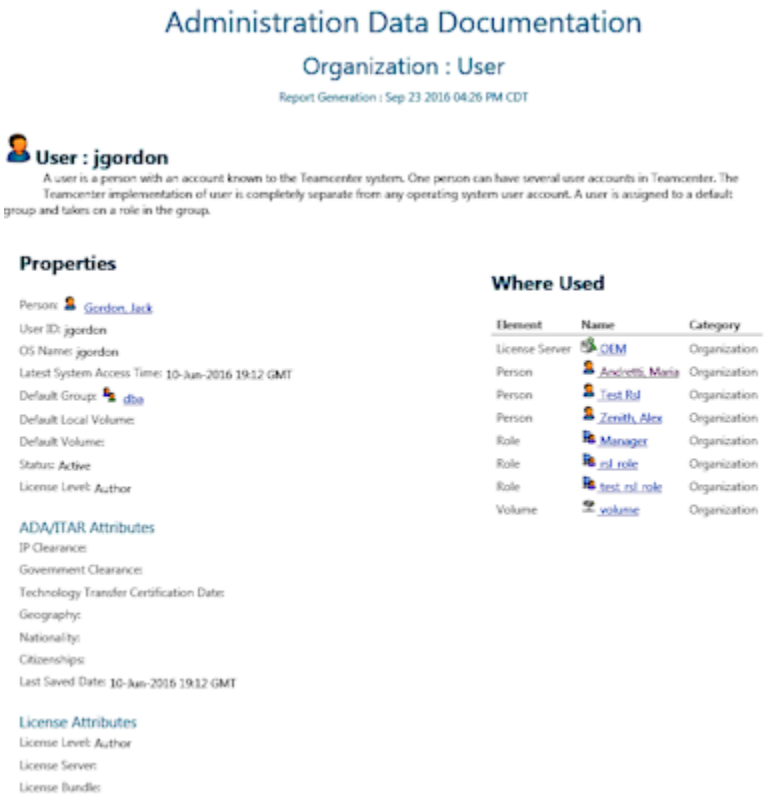
The output looks similar to this:



Click **Organization** in the **Categories** section or the **Organization** tile to display the following details.



The statistics of the organization are shown. For example, there are seven groups containing five users. Also, one inactive user is shown. An *inactive user* is considered a user who never logs on during a calendar month. Also, you can check ADA/ITAR attributes to determine such information as intellectual property (IP) clearance. For example, user **jgordon** does not have IP clearance.



Administration Data Documentation

Organization : User

Report Generation : Sep 23 2016 04:26 PM CDT

User : jgordon

A user is a person with an account known to the Teamcenter system. One person can have several user accounts in Teamcenter. The Teamcenter implementation of user is completely separate from any operating system user account. A user is assigned to a default group and takes on a role in the group.

Properties

Person: Gordon, Jack
User ID: jgordon
OS Name: jgordon
Latest System Access Time: 10-Jun-2016 19:12 GMT
Default Group: dba
Default Local Volume:
Default Volume:
Status: Active
License Level: Author

ADA/ITAR Attributes
IP Clearance:
Government Clearance:
Technology Transfer Certification Date:
Geography:
Nationality:
Citizenships:
Last Saved Date: 10-Jun-2016 19:12 GMT

License Attributes
License Level: Author
License Server:
License Bundle:

Where Used

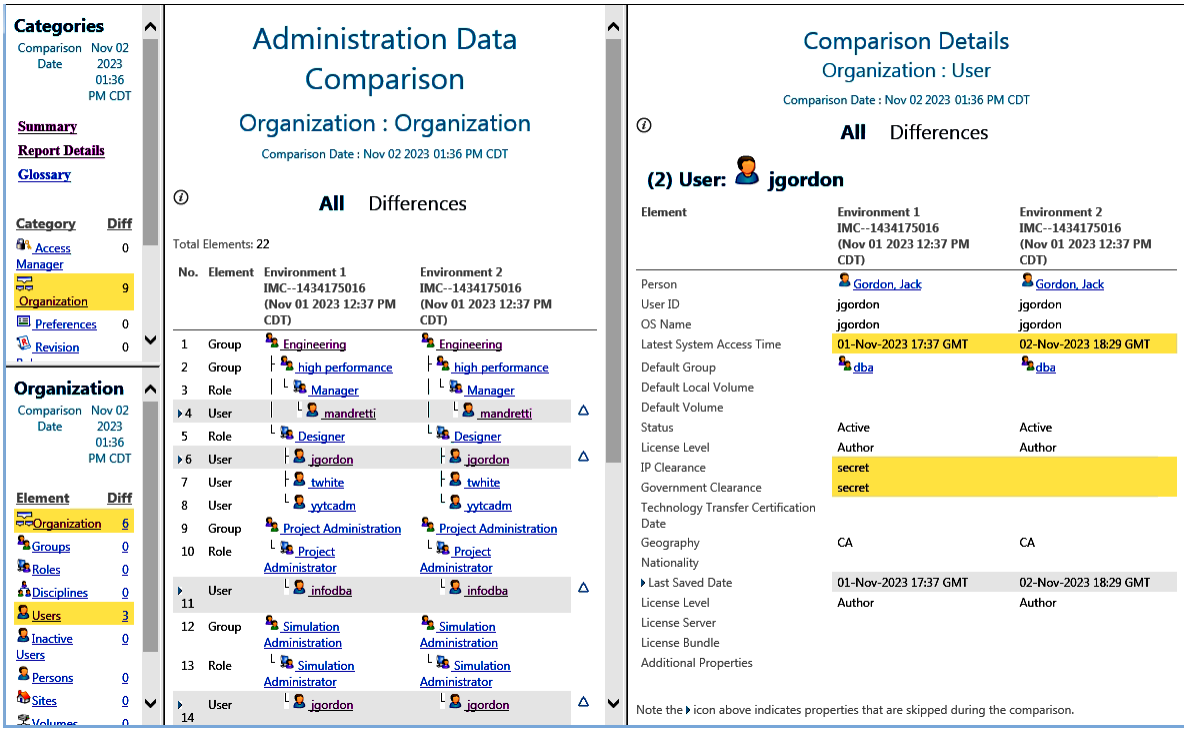
Element	Name	Category
License Server	OEM	Organization
Person	Andretti, Mario	Organization
Person	Test Rd	Organization
Person	Zenith, Alex	Organization
Role	Manager	Organization
Role	rsl_role	Organization
Role	test_rsl_role	Organization
Volume	volume	Organization

Using the administration data comparison report

Use the *administration data comparison report* to compare the differences between the administration data at two sites. It is generated using the **generate_admin_data_compare_report** utility. For example, you can compare your environment at different times to determine what has changed. For example, there may be users who have been granted intellectual property (IP) and government clearance permissions. By comparing your previous environment with your current environment using the administration data comparison report, you can easily see who has been granted IP privileges and if the users still have the privileges granted.

```
generate_admin_data_compare_report -adminDataTypes=all
-sourcePackage=C:\Temp\admin_data\data_export_110116.zip
-targetPackage=C:\Temp\admin_data\data_export_110216.zip
-outputDir=C:\Temp\admin_data\compareTandZ
```

In the following example, the administration data comparison report shows that user **jgordon** had IP clearance and government clearance of secret on November 1. However, on November 2, **jgordon** no longer has the IP clearance and government clearance.



The triangles in the center portion of the report indicate the changed elements when running the comparison. The yellow highlighted areas indicate the latest system access time and what has changed. In this case, the IP clearance and government clearance levels of secret were removed from user **jgordon**.

Exporting administration data

Export administration data when you want to:

- Move administration data out of one environment into another so that both environments are configured the same.
- Move administration data out of a test environment to a production environment.
- Obtain information about an environment so that you can compare it to another environment.
- Move partial administration data from different developers into a source control system (SCM) for compilation into a comprehensive set of administration data.

You can export administration data using the following methods:

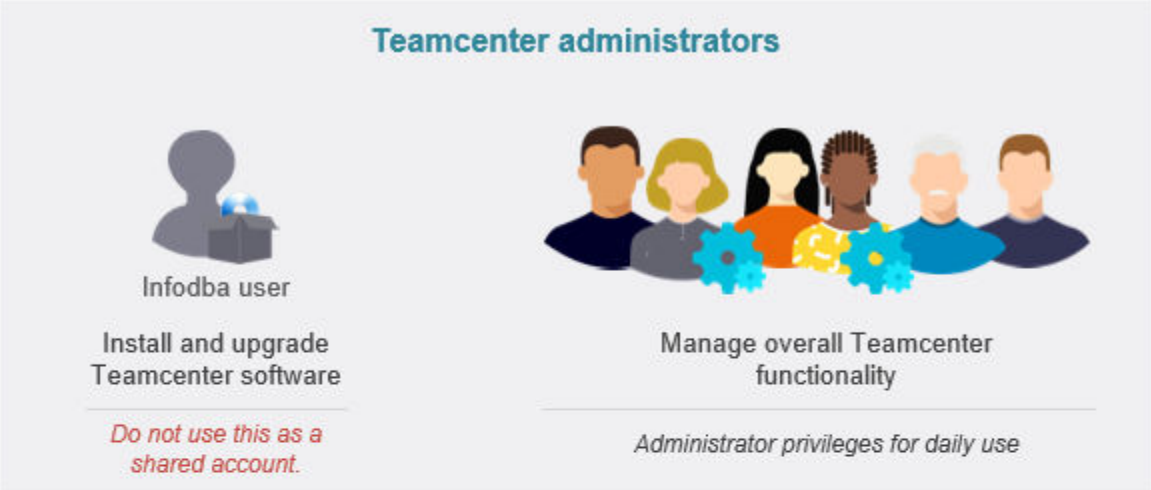
- Export full or partial administration data using the **admin_data_export** utility.
- Export full administration data using Teamcenter Environment Manager (TEM).

- Export partial administration data using TEM.

2. Assigning administrative privileges

Understanding types of administrative users in Teamcenter

Various types of administrative users deal with different kinds of tasks that help keep your site operating well. These tasks range from adding a user to a group to creating a workflow process and upgrading to a new release. There are two levels of administrator privileges in Teamcenter.



Teamcenter administrators

These users have system-wide privileges to manage the Teamcenter software configuration, the environment in which the business users operate.

A Teamcenter administrator is determined at the group level. When a user switches to a group with its **DBA Privilege** property enabled, they become a Teamcenter administrator. When they switch back to a non-privileged group, they return to being a regular business user.

Task examples	Manage security control. Create groups, roles, and users. Run command-line utilities.

The **infodba** user account is a special case of Teamcenter administrator created during the Teamcenter software installation process. It is subsequently used to create the initial Teamcenter administrator accounts and when performing patches and upgrades on the software.

After installation, this account must only be used with Deployment Center (installation or upgrade) or when specifically required.

This account is not associated with a specific person in the real world. Do not use it for daily administration. Instead, use regular user accounts and assign them as Teamcenter administrators or business administrators, as appropriate.

Siemens Digital Industries Software recommends you change your **infodba** user account password. You can change your password from within the Organization application.

Business administrators

There are many types of business administrators, each designed to offload some of the daily management of the business users and their tasks from the Teamcenter administrators.

These user accounts have limited administrative privileges within their scope. Outside of their scope, they are regular business users. This makes it easy for them to switch between being a regular business user and performing their administrative tasks.

Following are some examples of business administrators and their scope:

Role	Responsibilities
Group administrator	**Manage a group's users.** Override preferences for a specific group.
Project administrator	Manage projects and their associated users and data.
Classification administrator	Set up and administer Teamcenter Classification
ADA License administrator	Manage the users and data associated with the licenses. • Create International Trafficking and Arms Regulation (ITAR) licenses. • Create Intellectual Property (IP) licenses.

	• Create *Exclude* licenses.
Qualification administrator	Manage the minimum qualifications required for scheduled tasks.
Workflow administrator	Manage Teamcenter Workflow templates.

Considerations for managing administration accounts

Administrative privileges are required to manage Teamcenter administrative data like organization, access rules, and workflows. Administration accounts have powerful access to data and must be controlled and managed with caution.

When managing administration accounts, consider these key points:

- The out of the box **infodba** group has system-level privileges (**DBA Privilege** is enabled for the group).
- Groups for which **DBA Privilege** is enabled have Teamcenter system-level privileges.

  Users have Teamcenter system-level privileges when they are logged in as a member of a group for which **DBA Privilege** is enabled, and are logged in with role with access privileges equivalent to the out of the box **DBA** role.
- Administrative users can enable the **Administrative** user setting **Bypass** to override access protections and supersede other privileges. By default, **Bypass** is off when the rich client is opened.

  Caution:

  Bypass should be off except when explicitly needed. Enabling **Bypass** allows administrators to make changes that could potentially cause unintended loss of data and have serious repercussions that are normally guarded against by access rules.

  Bypass should be turned off immediately after the need to override privileges is past.

  During a session in which **Bypass** has been enabled, the setting remains enabled even when the group is changed, until **Bypass** is explicitly turned off, even though the **Bypass** setting no longer appears in the user setting dialog box. However, access rules are applied unless the group and role have been granted the bypass privilege.
- For each group that you want to have administrative privileges, designate at least one member of the group to manage roles for the group.

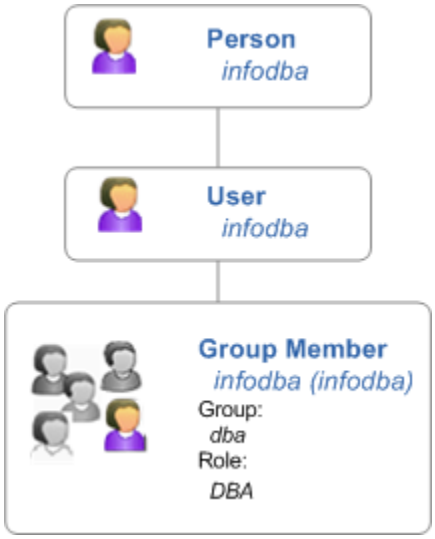
  To do so, add the **DBA** role to the group member.

Note:

The **DBA** role for a user in a non-administrative group has no additional privileges over any other group member.

Characteristics of infodba account

The out of the box account **infodba** comprises a person, user, role, and group named as follows:



The **infodba** account has Teamcenter system-level privileges.

The out of the box **Owning User(infodba)** rule greatly restricts access by users other than **infodba** to content that is created or added using the **infodba** account.

System administration accounts

Settings related system administration include the following:

Setting	Level	Privileges
DBA Privilege	Group	Adds full system administration privileges.
Group Administrator	User	Grants ability to manage roles for the group members.
IP Admin	Role	Manages intellectual property licenses.
ITAR Admin	Role	Manages International Traffic in Arms Regulations licenses.
DBA	Role	Manages roles for that group and can assign the group administrator.

Setting	Level	Privileges
Logged in as member of the **system** group with the **DBA** role		Special access privileges for archive and restore.
Bypass	User	Overrides access protections and supersedes other privileges. By default, **Bypass** is off when the rich client is opened. Caution: **Bypass** should be off except when explicitly needed. Enabling **Bypass** allows administrators to make changes that could potentially cause unintended loss of data and have serious repercussions that are normally guarded against by access rules. **Bypass** should be turned off immediately after the need to override privileges is past. During a session in which **Bypass** has been enabled, the setting remains enabled even when the group is changed, until **Bypass** is explicitly turned off, even though the **Bypass** setting no longer appears in the user setting dialog box. However, access rules are applied unless the group and role have been granted the bypass privilege.

3. Viewing your organization

Browse your Organization structure

Organization provides you with two methods for browsing and managing your structure: the **Organization** tree and **Organization List** tree.

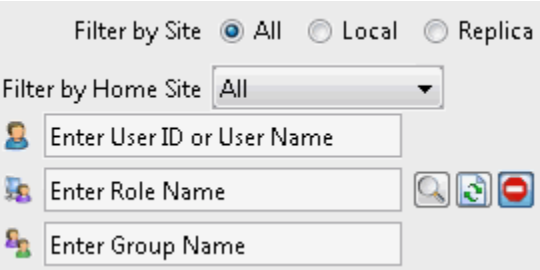
The **Organization** tree enables you to view the structure of your organization at a glance. By expanding and collapsing branches of the tree, you can view and manage the organizational structure. Selecting a node starts Organization wizards used to create groups, subgroups, roles, disciplines, and users.

The **Organization List** tree enables you to view and manage the components of your organization by listing groups, roles, disciplines, users, and persons. You can also use the **Organization List** tree to manage sites, external applications, volumes, and calendars.

Searching your Organization structure

Finding objects in your Organization structure

If you experience difficulty browsing through the organization hierarchy to find a certain group, role, or user, you can use the Organization find function to locate it.



You can also filter objects by owning location (remote or local). Replicated (remote) objects (user, group, role, and person) have two green dots beside them to designate them as remote objects .

After performing a search, you can reload the **Organization** tree by clicking the **Reload** button . This refreshes the organization in the current session; changes made in different sessions cannot be guaranteed to be updated.

To display new organization objects (groups, subgroups, roles, users, and disciplines) and modified objects in the **Organization** tree, select **View→Refresh Window** in the **Organization** perspective. This action refreshes components loaded in the current session so that changes made in another session are available in the current session. Because this action usually takes a long time, use this when you want your current session to be in sync with the latest change in the database by another session.

To suppress the display of inactive members in a group in the **Organization** tree, use the **Suppress inactive group members** button in the **Organization** pane.

Filtering your Organization search

You can sort your searches using two types of object filtering:

- Filter users by home site

  For example, you can filter for all users by home site or all sites.

- Filter objects by site

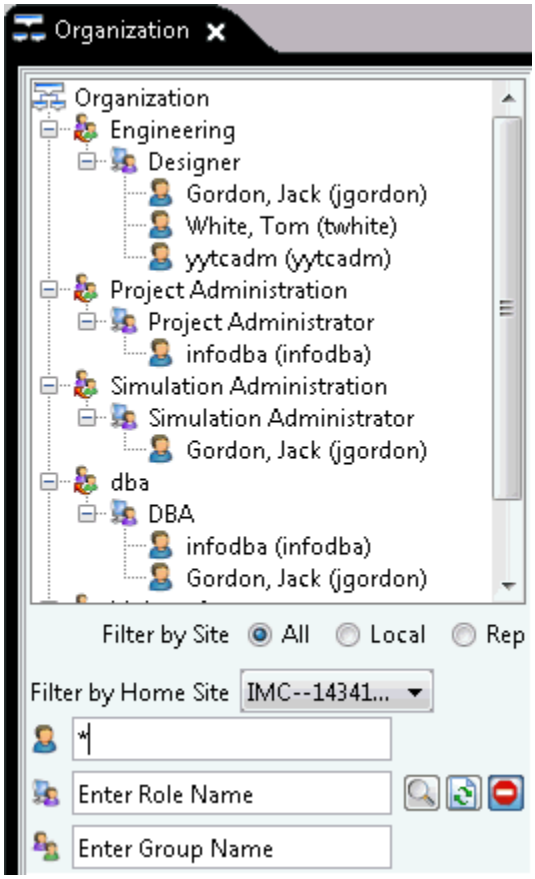
  For example, you can filter for replicated (remote) or local objects by site.

Filter users by home site

1. From the **Filter by Home Site** box, select the home site on which to filter either by selecting **All** or a specific home site.

2. Type the name of the user or the user's ID in the search box, or type an asterisk (*) to display all users, and then press Enter.

For example, the following figure shows the results for a search for all users having the home site **IMC–1434175**.



Filter objects by site

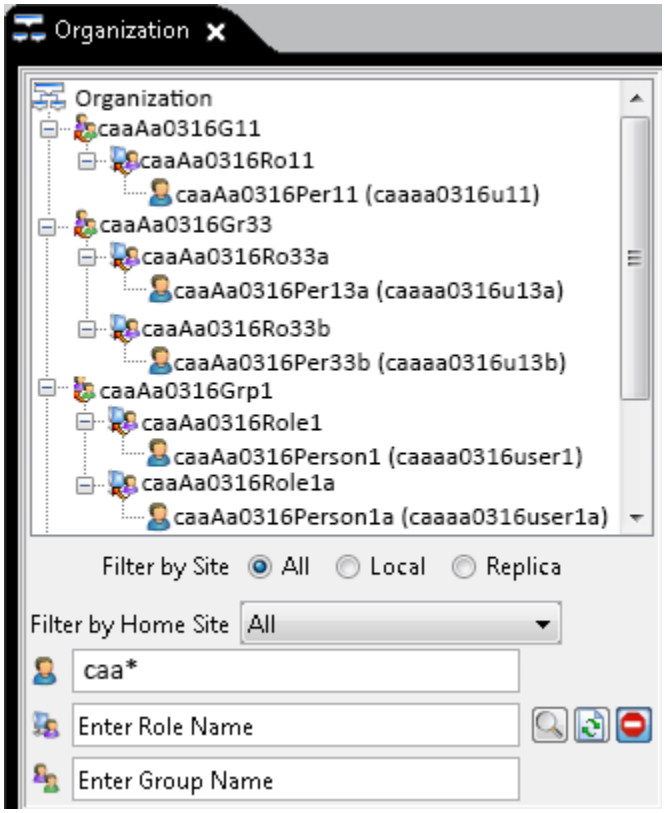
You can use the Organization application to filter objects by site: all objects, local objects, and replicated objects.

1. Select the home site on which to filter either by selecting **All** or a specific home site.

2. Type the text string in the search box mode you want (user, role, and group), and then click 🔍. You can enter the entire text string or a partial string using an asterisk (*).

   > Note:
   >
   > Replicated (remote) objects (user, group, role, and person) have two green dots beside them to designate them as remote objects .

For example, the following results are all replicated users whose name begins with **caa** that are found on all sites.



4. Setting up your organization for the first time

Overview of building an organization

The Organization application supports three methods of building the organization hierarchy:

- Setup Wizard – use when you want to speed up creation by setting up many users using bulk data from an input file. You begin by creating an input file of user data and then use Setup Wizard to map the data. Once this data is mapped to create related elements in Teamcenter, you can add additional associations between users, volumes and groups.

- **Organization** tree – a partially manual process, but automates the creation process by moving between steps for creating the different elements (groups and subgroups, users, roles, and persons)

- **Organization** list tree – a fully manual process used when you want to move from the user definition and on up. This is used most often for maintenance of your organization.

Establishing sites for each database that is used

What is a site?

A *site* describes an individual installation of Teamcenter and comprises a single database, all users accessing that database, and any additional non-Teamcenter resources such as hardware, networking capabilities, and third-party software applications (tools) required to implement Teamcenter at the site.

Site definitions are comprised of an ID and name. Both the site name and ID must be unique. When Teamcenter objects are exported, the site ID is used internally by each Teamcenter site to identify itself to other sites. The site name is also used internally and is stored in the database as a user-defined character string. To share data among sites, each Teamcenter database must store a definition of all of the sites in your enterprise.

Site names are generated automatically at the time of installation but should be modified so that they are descriptive of the function or location of the site. For example, if the site is in Albany and all users working at that site share the same database, Albany may be a suitable name for the site. But if this site is known as the ABC Design Center, a name such as the ABC Design Center may be better.

Every site must have its own unique name and ID. The site ID is generated automatically when the database is installed.

Caution:

Never change the site ID of a database after it is established. The site ID is used to generate internal identifiers for Teamcenter objects that must be unique throughout your enterprise. Never reuse a site ID when creating a new database. For this reason, never use the database's import and export functions to replicate a database; always use Teamcenter import and export capabilities.

As a user with **DBA** privileges, you use the Organization application to create, modify, and delete site definitions.

Create a site

The following procedure instructs you on creating a site using the Teamcenter rich client. You can also define a site from the command line by using the **site_util** utility.

1. Select the top-level **Sites** node  from the **Organization List** tree.

   The **Sites** pane appears.

2. Type a descriptive name for the site in the **Site Name** box.

   Caution:

   To support export of Teamcenter objects among multiple sites, site IDs must agree. Consider two sites: site **A** and site **B**. To export objects to one another, each site must be defined at both sites using exactly the same site ID in each definition. This is especially important if you are using Multi-Site Collaboration.

3. Type a unique site ID in the **Site ID** box. The unique site ID must be an integer.

4. (Optional) Type the site node identifier in the **Site Node/URL** box. If you are using Multi-Site Collaboration, and this site is configured to provide object directory services (ODS), select the **Provide Object Directory Services** check box. Otherwise, select the **Is A Hub** check box.

5. (Optional) Type the service-oriented architecture (SOA) URL in the **SOA URL** box. This URL is used for SOA calls to this site. The URL is used for HTTP-based Multi-Site Collaboration.

6. (Optional) Type the Platform Extensibility Configuration URL in the **TcGS URL** box.

7. Select the license server.

   By default, a local license server is available.

8. (Optional) Type the geographical location of the site in the **Geography** box. Appropriate values are two-character codes from ISO 3166. This information is used for authorized data access.

The following fields are related to the geographical location of the site:

- If this is an object directory services (ODS) site, select the **Provide Object Directory Services** check box. The ODS site maintains a record of each object in an entire Multi-Site Collaboration network.
- If this site is a hub, select the **Is A Hub** check box.
- If this site is enabled for Multi-Site Collaboration, select the **HTTP Enabled Multisite** check box.
- If this site uses TC XML payload instead of an object manager, select the **Uses TC XML Payload** check box.
- If this site has no network connection to the local site, select the **Is Offline** check box.
- For Teamcenter sites, the site ID must be the site ID of the site.

  Sites that manage product data in a file system outside of Teamcenter are considered unmanaged sites. You must allocate a unique number for an unmanaged site.

  If this site is unmanaged, check **Is Unmanaged**. This check box is enabled only when **Is Offline** is checked.
- If this site is enabled for **Is A Test Environment**, then bulk loaded data from a briefcase file is allowed. This feature can only be enabled during installation, or with the install utility.
- Select **Allow deletion of replicated master objects to this site** to allow replicated master objects to this site.
- If this site is enabled for Multi-Site Collaboration archiving and restoring, **Archive enabled Multi-Site** is checked. This feature is enabled during installation or with the **site_util** utility.

9. Click **Create**.

The site is saved and displays in the **Organization List** tree.

Defining the structure of your organization

Defining license servers for your site

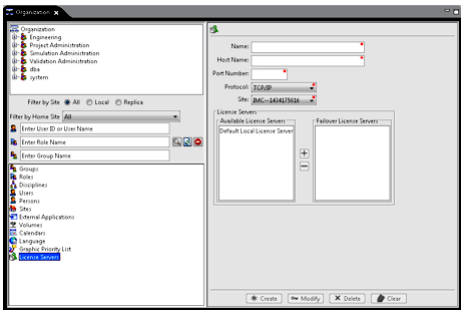
What is a license server?

A *license server* is a process dedicated to tracking license usage by users. It runs on a host machine and port that you specify. As an administrator, you can set up multiple license servers. You can assign a different set of users to each license server. This allows load balancing of license requests so that no one license server is overused.

Create a reference to a license server

1. Select the top-level **License Servers** node from the **Organization List** tree.

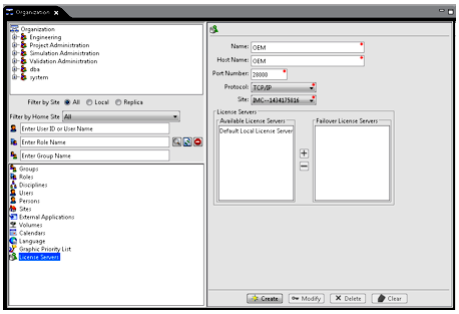
   The Default Local License Server (DLLS) is a special license server definition that is created when you install Teamcenter.



2. Type a descriptive name for the license server in the **Name** box.
3. Type the name of the host in the **Host Name** box.
4. Type the port number in the **Port Number** box.
5. Select the protocol type, **TCP/IP**.

   > Note:
   >
   > Currently, only **TCP/IP** protocol is supported.

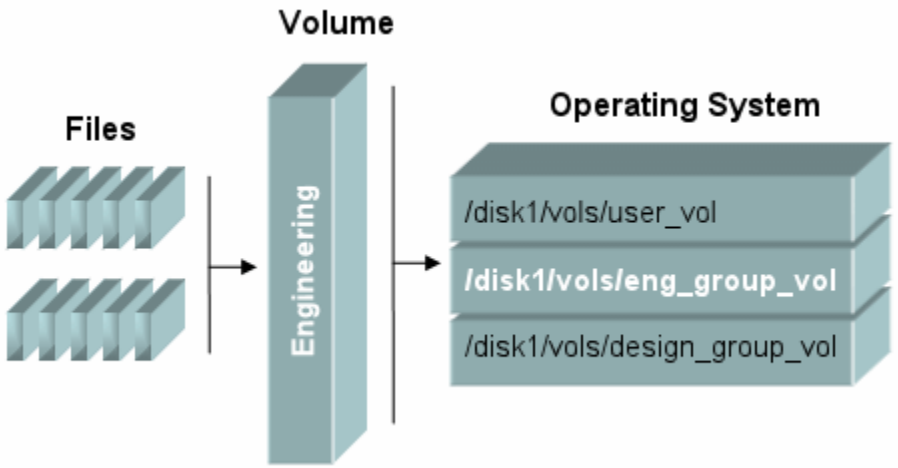
6. Select the site from the drop-down list.
7. Click **Create**.



Defining volumes for your site

What is a volume?

A *volume* is a location where files are stored. A volume equates to a directory on the operating system. Files stored in volumes are created by CAD applications or other third-party applications.



- Teamcenter retains the volume location (directory) and the file name.
- Users should always access files in volumes through Teamcenter.

Assign volumes to groups and users and define file locations for your organization structure. As a user with **DBA** privileges, you use the Organization application to:

- Create and delete volumes.
- Modify volume location and properties.
- Control volume access.

You can control the number of files stored in subdirectories within a volume. Additionally, you can distribute existing Teamcenter volume files to reduce the number of files in subdirectories within a volume. This is beneficial because a volume may contain thousands of files from users and groups assigned to the volume, where the subdirectories in the volume could grow beyond a certain limit and the file storage may not be scalable. The capabilities allow you to:

- Specify the maximum number of files allowed in a subdirectory within a volume with the **TC_Volume_Max_Files_Per_Dir** preference. Enhance performance when **TC_Volume_Max_Files_Per_Dir** is set by adding an index with the **install** command *-add_index* argument as follows:

```
install -add_index -u=<user> -p=<password>|-pf=<pwfile> -g=<group>
<index_name> 0 ImanFile sd_path_name
```

For example:

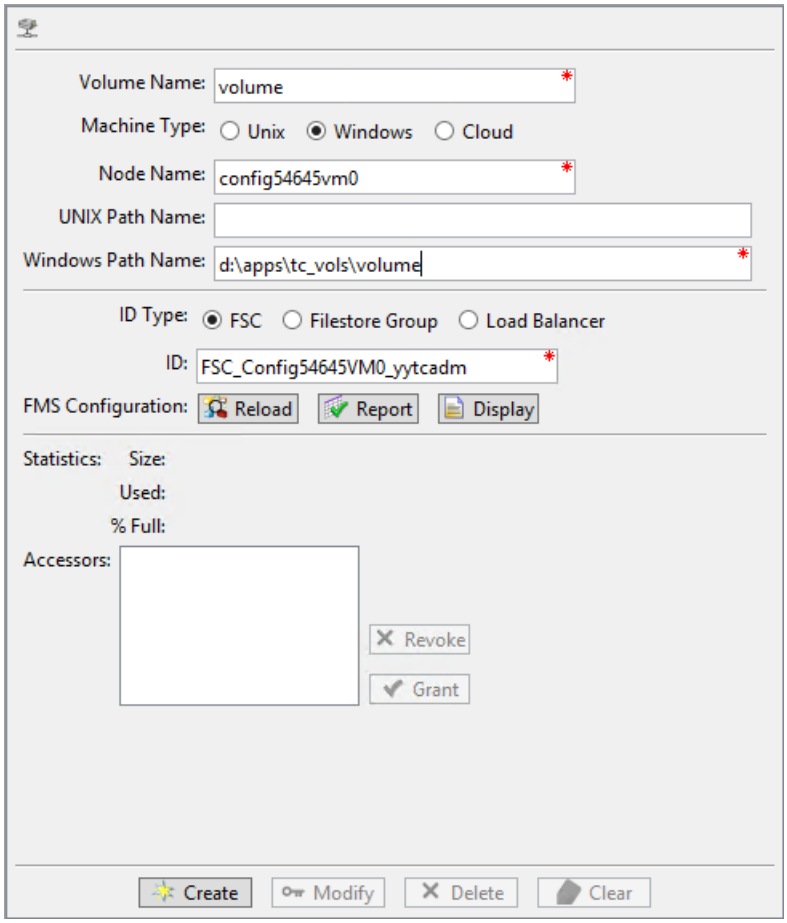
```
install -add_index -u=Tc-admin-user -p=password -g=dba FilePathNameIdx 0
ImanFile sd_path_name
```

where *sd_path_name* is the subdirectory name in the volume root directory.

- Specify the interval to check the volume subdirectory for its maximum file limit with the **TC_Volume_FilesPerDir_Check_Interval** preference.
- Distribute existing Teamcenter volume files with the **move_volume_files** utility when the volume subdirectory file count exceeds the limit.

Create a volume

Because of limitations and restrictions in NTFS file systems, Siemens Digital Industries Software recommends creating the volume on the machine where the disk physically resides. It is important to choose a location that is constantly accessible to all users. Windows services do not support mapped drives. Siemens Digital Industries Software recommends using a UNC path or a path that is local to the machine.



1. Select the top-level **Volumes** node from the **Organization List** tree. Teamcenter displays the **Volumes** pane.

2. Type a unique descriptive character string in the **Volume Name** box.

3. Select the machine type on which the volume will reside: **Linux**, **Windows**, or **Cloud**.

4. Type the name of the network node that physically contains the new volume in the **Node Name** box.

5. Depending on the (non-cloud) machine type, type the full Linux or Windows path of the new volume in either the **Linux Path Name** box or the **Windows Path Name** box.

6. Select the ID type (**FSC**, **Filestore Group**, **Load Balancer**) to indicate the element in the FMS primary configuration to which the new volume element is to be added and type the ID in the **ID** box.

   The value you enter into the **ID** box varies depending upon where the new volume is to be added in the FMS primary configuration. That location in the configuration is determined by the ID type selection.

Following are examples of each ID type:

- **FSC**:

```
<fscGroup id=”fscGroup1”
     <fsc id=”fsc1” address=”http://csun17.ugs.com:4444”>
          <volume id=”vol1” root=”/data/vol1”/>
     </fsc>
     <fsc id=”fsc2” address=”http://csun18.ugs.com:4444”>
          <volume id=”vol2” root=”/data/vol2”/>
     </fsc>
     <clientmap subnet=”146.0.0.1” mask=”255.0.0.0”>
          <assignedfsc fscid=”fsc1”/>
     </clientmap>
</fscGroup>
```

  To add a volume served by the **fsc1** FSC, click the **ID** button for **FSC** and then type **fsc1** in the **ID** box.

- **Filestore Group**:

```
<fscGroup id=”fscGroup1”
     <filestoregroup id=”fsgroup1”>
          <volume id=”vol1” root=”/data/vol1”/>
          <volume id=”vol2” root=”/data/vol2”/>
     </filestoregroup>
     <filestoregroup id=”fsgroup2”>
          <volume id=”vol3” root=”/data/vol3”/>
     </filestoregroup>
     ...
</fscGroup>
```

  In this case, to add a volume to the second filestore group, click the **ID** button for **Filestore Group** and type **fsgroup2** in the **ID** box.

- **Load Balancer**:

```
<fscGroup id=”fscGroup1”
     <loadbalancer id=”loadBal1” address=”http://lb1.ugs.com:4454”>
          <volume id=”vol1” root=”/data/vol1”/>
     </loadbalancer>
     ...
</fscGroup>
```

  In this case, click the **ID** button for **Load Balancer** and type **loadBal1** in the **ID** box.

When the new volume is created, you must specify where in the FMS primary configuration the definition of this volume should be placed: the **FSC element** section, the **filestore group** section, or the **load balancer** section.

Use the following FMS-related buttons as needed:

- **Reload** 

  Makes an FMS configuration the current and active configuration. This is useful for updating the configuration with any manual changes that are made.

- **Report** 

  Displays the primary and secondary FSCs currently configured and the status of each.

- **Display** 

  Displays the contents of the FMS primary configuration file. It can be useful for determining what to add to a volume, for example, an FSC ID or filestore group.

7. Grant users or groups access to the volume, as described in *Grant volume access*.

8. Click **Create**.

Controlling volume access

Granting volume access

Users inherently have read access to newly created volumes. However, you must explicitly grant write access to the volume. To grant access, you must be logged on to the operating system as the root user and logged on to Teamcenter as a member of the **dba** group.

When you grant users access to volumes, the system generates a subdirectory identified by the user's name. Ownership of the subdirectory is assigned to the user.

When you grant access to a group, the system generates a subdirectory identified by the group name. The system does not generate subdirectories for subgroups, regardless of whether access inheritance is enabled. Subgroups share the directory of the original group.

Granting volume access to a group does not implicitly grant access to all subgroups unless specified by the **TC_allow_inherited_group_volume_access** preference. The default value of this preference is **0**, indicating that subgroups do not inherit write access to the volume by default. Change the preference value to any nonzero number to allow inherited access.

- Inherited access applies to all volumes including default local volumes, also known as *store and forward volumes*.
- Access modes are granted accordingly: groups access mode = 777, users access mode = 755.

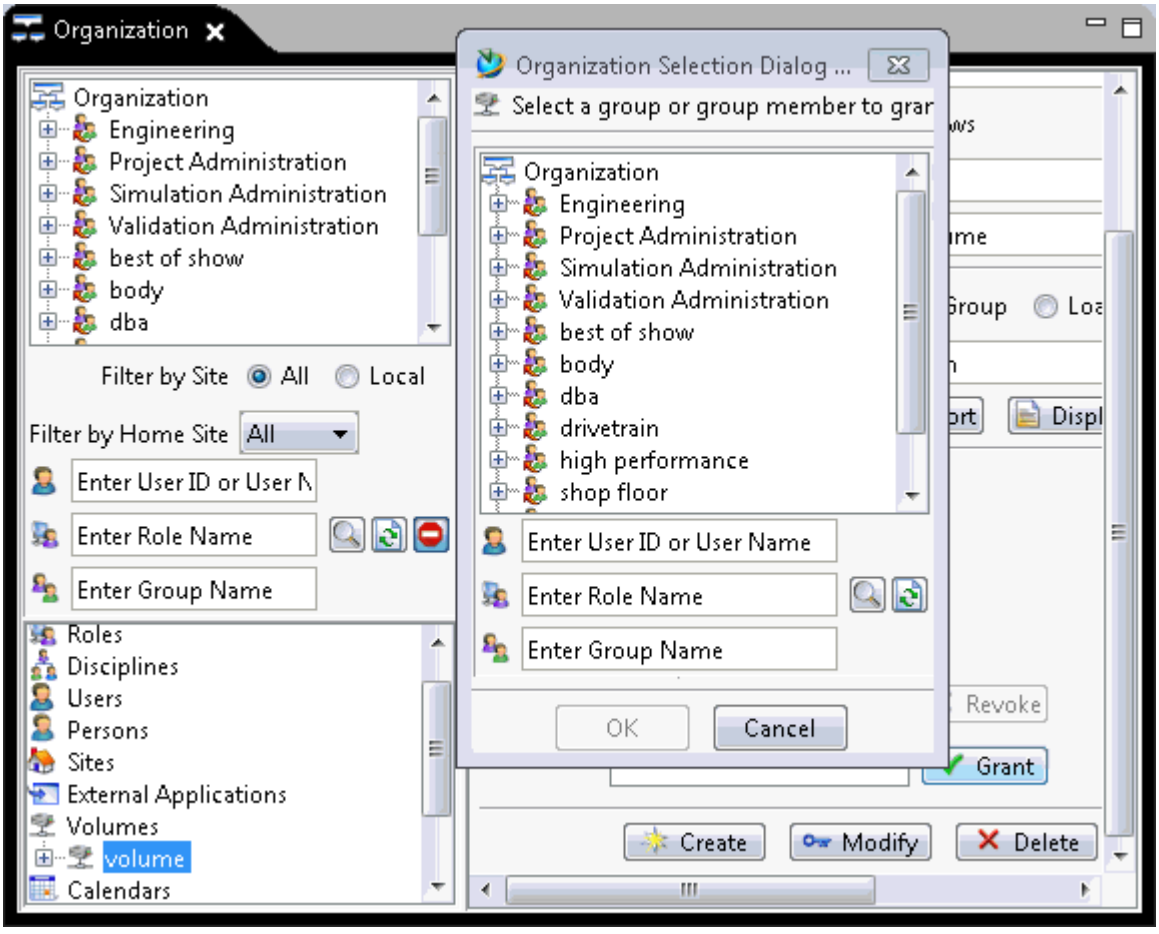
Grant volume access

1. In the **Organization List** tree, select the volume to which you want to grant access.

   Teamcenter displays the properties of the volume definition, including the list of users and groups with access to the volume, in the **Volumes** pane.

2. Click **Grant**.

   The system displays the **Organization Selection** dialog box.



   Use any of the following buttons in the search pane:

   - Search by group

- Search by role 
- Search by user 
- Reload the **Organization** tree 

The search works in an identical way for each mode. To perform a search, type the search text into the box and click the appropriate button. Note that the wildcard (*) character is accepted. The **Organization** tree is reloaded with the results of your search. If there are no matches, a message informing you of this.

3. Select the groups, subgroups, and users to be granted access to the volume.

> Note:
>
> Multiple accessors can be selected by holding the control key and clicking the group, subgroup, and user in the tree.

4. Click **OK** to grant access to the selected groups, subgroups, and users.

   Teamcenter closes the **Organization Selection** dialog box and the new accessors are displayed in the **Accessors** list of the **Volumes** pane.

Revoke volume access

1. Select the volume from which you want to revoke access.

   Teamcenter displays the properties of the volume definition, including the list of users and groups with access to the volume in the **Volumes** pane.

2. From the **Accessors** list, select the group or user from whom volume access is to be revoked.

3. Click **Revoke**.

The group or user is removed from the **Accessors** list and can no longer write data to the volume.

Assigning roles to users

What is a role?

A *role* is an object that models the type of work a user is expected to perform in a group.

- A role can be assigned to multiple groups.

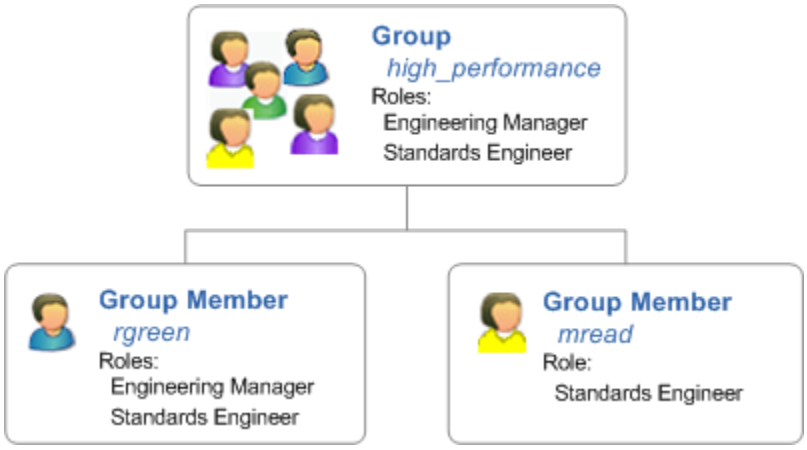
- Roles add another layer of data access control.
- Roles are created along functional lines.

> Tip:
>
> Use real-world descriptions, skills, and/or responsibilities.

Roles refine the group definitions of your organization structure. As a user with **DBA** privileges, you use the Organization application to:

- Create, modify, and delete role definitions.
- Add existing roles to the **Organization** tree.
- Add new roles to the **Organization** tree.
- Assign a default rule within a group.

Example



Robert Green is an Engineering Manager. In addition to his responsibilities as Engineering Manager, Robert must also perform standards work. Therefore, user **rgreen** has been assigned two roles in the **high_performance** group: **Engineering Manager** and **Standards Engineer**.

Create a role

You create roles to reflect the skills and responsibilities of the users in your organization. Roles can be created using the **Organization List** method described or you can create and add a role to the **Organization** tree using the Organization Role wizard.

1. Select the top-level **Roles** node from the **Organization List** tree.

The **Roles** pane appears.

2. Type the following information:

   - A new role in the **Role** box.
   - Optionally, a descriptive character string in the **Description** box.

3. Click **Create**.

The new role is saved in the database and displayed in the **Organization List** tree.

Defining groups

What is a group?

A *group* represents a project in Teamcenter. Groups contain members (users) who take on a role or multiple roles in the group. Groups represent data ownership and therefore control data access. Two groups are provided with Teamcenter: **dba** and **system**.

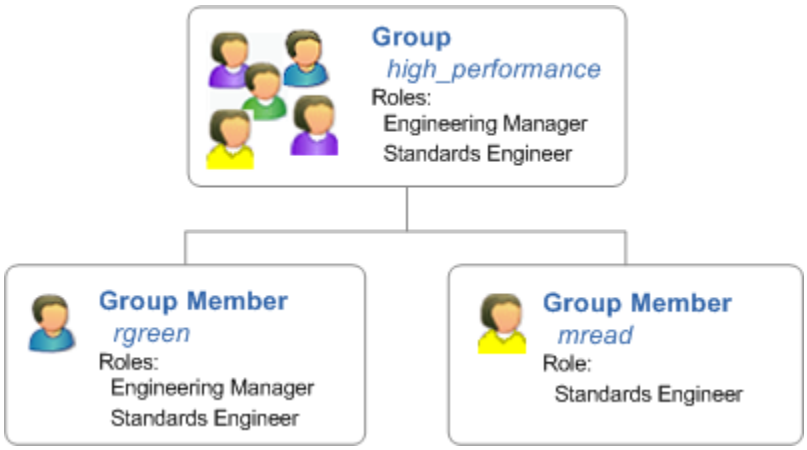
> Warning:
>
> Do not delete the **system** group provided with Teamcenter. It is required for the product to function properly.

- Groups are defined along project lines, not functional lines, but can define third-party organizations such as suppliers.
- A group member can be a member of many groups. For example, Robert Green can belong to the **high_performance** and **standards** groups.

Groups make up the core of your organization structure. As a user with **DBA** privileges, you use the Organization application to:

- Create, modify, and delete groups.
- Manage subgroups within the **Organization** tree.
- Assign default volumes to a group.
- Assign authorized data access privileges to a group.

Example



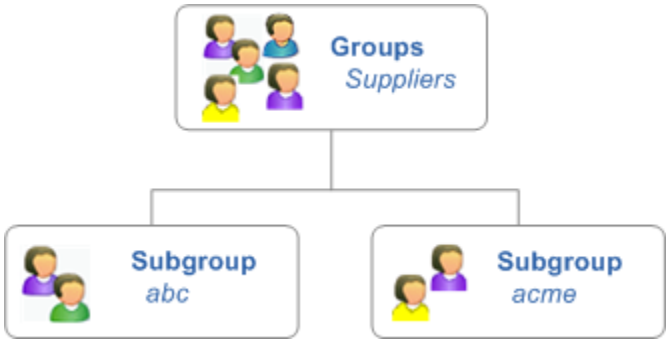
What is a subgroup?

A *subgroup* is a group with another group designated as its parent. A subgroup can also be designated as a parent group itself. The position of subgroups within the Organization hierarchy can be managed by parenting and reparenting groups.

- Subgroups are an excellent way to organize your users.
- Subgroups inherit access permissions, volumes, and preferences from their parent.

Volumes are a location where files are stored. Volumes will be discussed in more detail later.

Example



Group terms and concepts

Term/Concept	Description
Groups and subgroups	Groups and subgroups are project-oriented clusters of users. Each group has exactly one parent group (unless it is at the top, or root,

Term/Concept	Description
	of the hierarchy, when it has no parent) and may have one or more child groups (subgroups).
Default group	When a user belongs to more than one group, one of them is designated as the default group. A default group must be designated for each user so that Teamcenter can store project files in a central location (for example, in the group volume). The user's default group is used at logon unless another group is specified. When Teamcenter Security Services is installed and the **TC_SSO_SERVICE** environment variable is set in the **tc_profilevars** file, logon uses the default Teamcenter group.
Parent group	A parent group is used to organize a configuration of related subgroups.
System administration group	A Teamcenter administrator, also referred to as database administrator (DBA) or user with **DBA** privileges, is any member of a special system administration group and is the primary person responsible for maintaining the Teamcenter software, data volumes, and user accounts. Teamcenter creates one system administration group (**dba**) during installation. You can create others as needed.
system group	Teamcenter provides a special **system** group that is used for performing specialized tasks in an overall system administration strategy. Currently, members of the **system** group are primarily responsible for archiving and restoring objects. Although any Teamcenter user can mark an object for archive or restore, only members of the **system** group can perform the actual object archive and restore operations. This restriction also applies to members of a system administration group; they cannot perform archive and restore operations either. Warning: Do not delete the **system** group from the database under any circumstances. Teamcenter does not function properly without this group. Although a user could belong to both the **system** group and a system administration group, members of the **system** group do not inherently have the privileges required to perform all Teamcenter administrative tasks.
Group administrator	A group administrator is a group member who can add, modify, or remove group members.

Term/Concept	Description
	Group administrators must be members of the group they are administering and these privileges are only valid within that group.
Group names	A group is identified uniquely by the combination of its name and its parent. Two groups with different parents may have the same name, but two groups with the same parent may not. To distinguish between different groups with the same name, note the placement of the group within the **Organization** tree.

Group hierarchies

Groups are organized into one or more trees or hierarchies. Each group has exactly one parent group (unless it is at the top or root of the hierarchy, when it has no parent) and can have one or more subgroups.

The following list indicates the functional areas in Teamcenter that use group hierarchies.

Functional area	Group hierarchy use
Access Manager	A group can inherit access permissions from its parent.
Authorization	Authorization rules are inherited within the group hierarchy.
Volumes	Groups can inherit access to a volume from parent groups; therefore, you must consider volume access when modifying or moving hierarchical groups.
Preferences	Group preferences can be inherited from the parent group.
Mail	Mail can be sent to members of a group's subgroups, subgroups of subgroups, and so on, as well as to the named group only.
Workflow	Signoffs can be assigned to members of a group's subgroups and members of the named group.

Moving groups within the hierarchy and volume access

Moving groups within a hierarchy can affect group member access to data depending on how volumes are assigned.

- Existing files

  Restructuring groups makes no difference; the files continue to be available without any change in behavior.

- New files

  If the group has its own assigned volume, restructuring makes no difference to volume access. Files continue to be saved to the assigned volume. However, if the group does not have its own volume, but instead inherits access to a volume from an ancestor group, there may be a difference after the restructuring. The restructured group now has a different set of ancestor groups; therefore, it either inherits access to a different volume or potentially has no volume access at all.

Creating a group

As a user with **DBA** privileges, you create project-oriented groups to organize clusters of users.

This topic discusses the procedures for creating:

- Parent groups and subgroups using the **Organization List** tree.

  This method presents all the group properties including a parent group property for creating subgroups.

- Parent groups in the **Organization** tree.

  This method presents fewer group properties, but uses wizards instead to add things like **subgroups** and roles.

Groups have several settings to configure access to data owned by the group.

- The internal/external **Security** setting allows or restricts access to data. For example, members of external groups can only access data in their group.

- The **DBA Privilege** setting, when selected, allows system administration privileges to members of the group.

- The authorized data access (ADA) and International Traffic in Arms Regulations (ITAR) setting allows or restricts access to data based on clearance levels and data classification.

Add existing group as subgroup using the Organization Group wizard

There are two ways to add an existing **group** as a subgroup to the **Organization** tree. You can assign a parent group to the subgroup definition or you can use the Organization Group wizard to add an existing group to a parent group.

1. Select a group or subgroup from the **Organization** tree. The selected group serves as the parent group for the subgroup you add.

   The **Groups** pane appears.

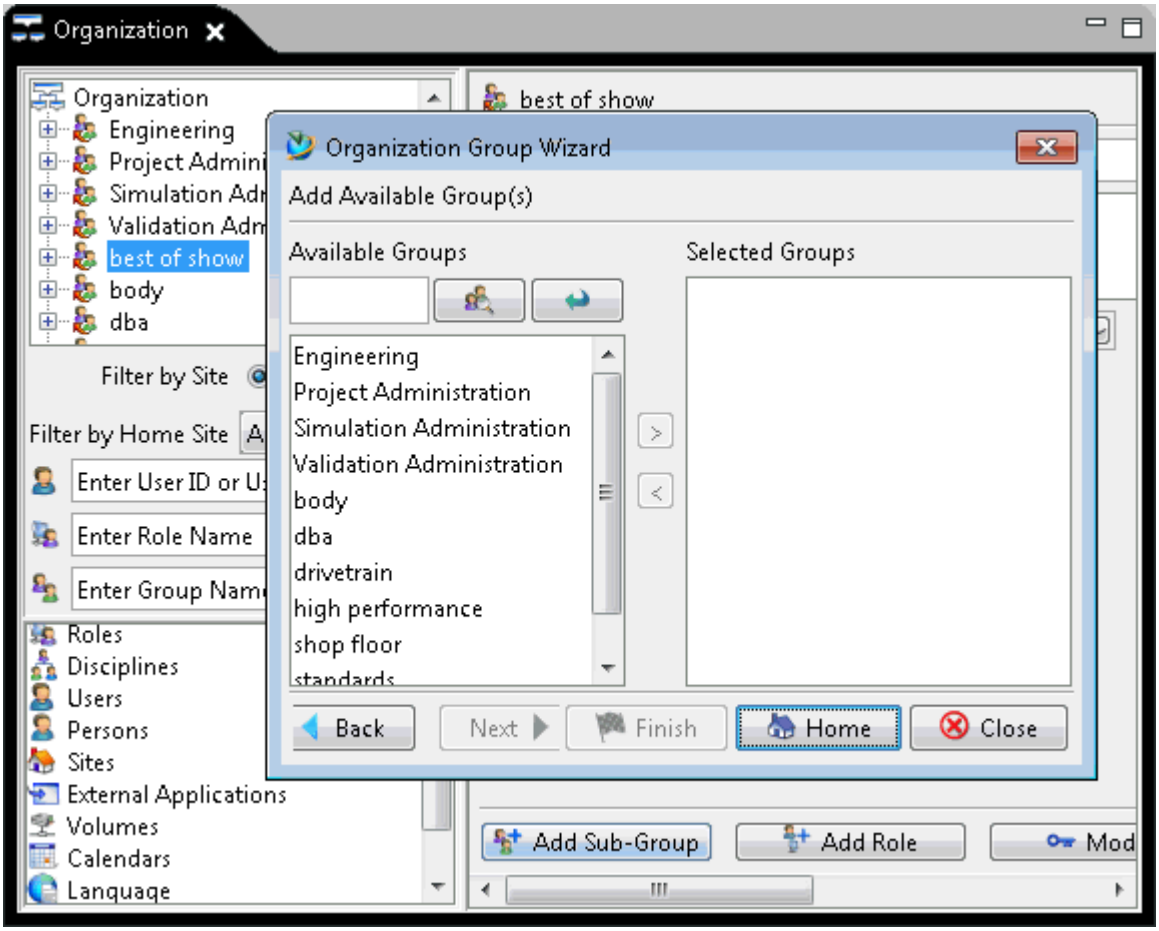
2. Click **Add Sub-Group**.

   The Organization Group wizard appears.

3. Select **Add existing group as sub-group** and click **Next**.

> Caution:
>
> Subgroups can be associated with one parent group. Therefore, selecting a group that is currently associated as a subgroup of another parent group breaks that parent-child relationship. Changing existing group names or structure (for example, reparenting a group) can drastically impact Workflow functionality. Workflow processes do not complete if the group names are changed after the process is started. Therefore, all Workflow processes, including Cascade Release (CR) and Change Management (CM) processes, must be modified to reflect any changes in group names or structure *before* they are started or else they fail. Additionally, all current (started) EPM jobs affected by group name or structure changes must be terminated and new jobs must be started from updated procedure templates.

4. Select the subgroups to add from the **Available Groups** list.



You can also use either of the following buttons in the search pane:

- Find group
- Reload all available groups

To perform a search, type the search text into the box and click the **Search by Group** button. Note that the wildcard (*) character is accepted.

You can move items between the **Available Groups** and **Selected Groups** lists by double-clicking a group or selecting a group and clicking the right arrow (▶) or left arrow (◀) buttons. After you select all of the subgroups, click **Next** or **Finish**.

5. Click **Yes** to add the selected groups.

   The **Group(s) added** dialog box appears.

6. Click **OK**.

   The Organization Group wizard displays the next step.

7. Perform one of the following actions:

   - Select the **What is next?** option from the wizard. You can choose to add another subgroup or add a role to the selected group.
   - Click **Home** to return to step 1 of the Organization Group wizard.
   - Click **Close** to dismiss the wizard.

The subgroup appears in the **Organization** tree.

Add new subgroups using the Organization Group wizard

You can create new subgroups and add them to the **Organization** tree using the **Organization List** method.

1. Select a group or subgroup from the **Organization** tree. The selected group serves as the parent group for new subgroup.

   The **Groups** pane appears.

2. Click **Add Sub-Group**.

   The Organization Group wizard appears.

3. Select **Add new group as sub-group** and click **Next**.

4. Complete the following information:

   a. Type a group name in the **Name** box.

      A group is identified uniquely by the combination of its name and its parent. Two groups with different parents may have the same name, but two groups with the same parent may not have the same name. Additionally, subgroups may not have the same name as a parent group.

      Siemens Digital Industries Software recommends the group name can include the following special characters: spaces, periods, hyphens, and underscores. Other special characters, such as ampersand (&), are not recommended.

   b. (Optional) Type a description of the group in the **Description** box. Doing so is important for future reference.

   c. (Optional) Choose whether this group is subject to **Internal** or **External** project-level security rules. You can also leave this field blank, in which case project-level security rules are not applied.

   d. (Optional) If the group is to have system administration privileges, check **DBA Privilege**. Otherwise, leave **DBA Privilege** unchecked.

   e. Click **Default Local Volume** to display the **List of Defined Volumes** and select, by double-clicking, a default local volume for the group.

      > Caution:
      >
      > If you create a group without assigning a default volume, group members cannot save datasets. Therefore, Siemens Digital Industries Software recommends that you assign a default volume for the group.

   f. Click **Default Local Volume** to display the **List of Defined Volumes** and select, by double-clicking, a default local volume for the group.

      Use this temporary storage to upload a file into FMS volume storage. This temporary local volume allows the file to be stored locally before it is automatically transferred to the final destination in the background. Once the file is stored in the default local volume, the user can continue working without having to wait for the upload to take place.

      > Note:
      >
      > The **Default Local Volume** value must be different than the value of **Default Volume**.

5. When you are finished adding the information, click **Finish** to continue or **Close** to dismiss the wizard.

6. If you clicked **Finish**, perform one of the following actions:

   - Select the **What is next?** option from the wizard. You can choose to add another subgroup or add a **role** to the selected group.
   - Click **Home** to return to step 1 of the Organization Group wizard.
   - Click **Close** to dismiss the wizard.

   The new subgroup is saved in the database and displayed in the **Organization** and **Organization List** trees.

Creating persons and user accounts

What is a person?

Persons are individuals who work at your site. A person has properties such as **Name**, **Address**, and **Employee Number**.

- Consider creating all persons at your site using the following naming convention:

  last-name, first-name, middle-initial

- Person definitions that are referenced by a **User** object cannot be deleted.

You must define a person for each Teamcenter user. As a user with **DBA** or group administrator privileges, you use the Organization application to:

- Create person definitions.
- Modify person definitions.
- Delete person definitions.

Example

Create a person

Person definitions contain real-world information about individual Teamcenter users.

Person definitions can be created:

- Simultaneously with the user definition when using the **Organization User wizard**.
- Manually using the **Organization List** tree and corresponding pane.

These optional **Person** properties have resulting behavior:

- **E-Mail Address** is required for workflow notification.
- **Locale** specifies the user's locale, for example, **en_US** indicates English as spoken in the United States.
- **Time Zone** specifies the user's time zone, for example, **America/Chicago** represents the Central time zone.
- **User Image** allows a graphic to be added for the person. You can add a picture of the person that when a **Person** object is selected.

Often, the real-world information is similar for users residing in the same physical location. In such cases, you can minimize the amount of data entry required by selecting the node of a person definition (from the **Organization List** tree) that possesses similar attributes to the person you want to create. To begin a definition from scratch with a blank **Persons** pane, select the top-level **Persons** node from the **Organization List** tree.

1. Select a node from the **Persons** list in the **Organization List** tree. If you do not see nodes under the **Persons** list, double-click the top-level **Persons** node to display them.

   The **Persons** pane displays the properties of the person definition.

2. Type a unique name in the **Name** box. All other boxes are optional.

   The entry in the **Name** box must be unique. You cannot create two persons with the same name.

3. Click **Create**.

   The new person definition is saved in the database and displays in the **Organization List** tree.

The new person definition is saved in the database and displays in the **Organization List** tree.

What is a user?

A *user* is a person with an account known to the Teamcenter system. One person can have several user accounts in Teamcenter. The Teamcenter implementation of user is completely separate from any operating system user account.

A user is assigned to a default group and takes on a role in the group. As a user with **DBA** privileges, you use the Organization application to:

- Create, modify, and delete user accounts.
- Maintain user password restrictions.
- Deactivate or activate user accounts.
- Assign group administrator privileges.
- Assign intellectual property and government clearances to data stored in Teamcenter for user accounts, along with defining multiple citizenships.
- Assign a license bundle to a user.

Example

Create a user

You create user accounts to identify each individual who interacts with Teamcenter.

User definitions can be created:

- From a role in the **Organization** tree using the **Organization User wizard**.

- Manually using the **Organization List** tree and corresponding pane.

These optional **User** properties have resulting behavior:

1. Select the top-level **Users** node  from the **Organization List** tree.

   The **Users** pane appears.

2. Complete the following system information:

   > Note:
   >
   > - Do not use the delimiters defined in the **TC_user_delimiters** preference when entering user information in either the **Person Name** box or the **User ID** box. (If the **TC_user_delimiters** preference is not set, parentheses **( )** are the default delimiters.) Otherwise, the user name and user ID display incorrectly in the **Organization List** tree.
   > - If you inadvertently use the characters set in the **TC_user_delimiters** preference when you create a user or a person, use the **make_user** utility to correct the user ID and person name delimiters.

   a. Click  to the right of **Person Name** to display the **List of Defined Persons** list and select, by double-clicking, a person name from the list.

   > Caution:
   >
   > If autologon is used at the site, the operating system user name must be the same as the Teamcenter user ID and the password must be valid for both accounts or autologon does not work.

   b. Type a unique user name in the **User ID** field.

      The following naming restrictions apply when creating a unique user name:

      - Do not exceed 32 characters.
      - Do not use the following characters:

        ! # @ $ % = & ' " ^ : ; . _ < > ( ) { }

   c. Type the user's OS name in the **OS Name** field.

      Teamcenter uses the user’s OS name as a backup email address if no email address is set in the **Person** object. This allows the user to receive notifications and subscriptions.

d. **Password** must conform to **password restrictions**.

If a user attempts to log on to Teamcenter without entering a password, a logon failure occurs.

e. Complete the **Latest System Access Time**.

(Optional) **Latest System Access Time** displays the last time this user logged onto Teamcenter. This helps to determine when a user is deactivated according to the **TC_days_non_login_timeout** preference. The default setting for this preference is set to 0, allowing users to always log on. When deactivation does occur, **Reset** activates the user.

f. Click **Default Group** to display the **List of Defined Groups** list and select a group from the list by double-clicking.

Default Group specifies the group the user will be placed in the organization and the default group assigned on logon.

g. (Optional) Click **Default Volume** to display the **List of Defined Volumes** list and select a volume from the list by double-clicking.

Siemens Digital Industries Software recommends that you *do not* define a default volume for each user. If the default volume is not specified, the group's default volume information is used.

h. (Optional) Click **Default Local Volume** to display the **List of Defined Volumes** and select, by double-clicking, a default local volume for the group.

Use this temporary storage to upload a file into FMS volume storage. This temporary local volume allows the file to be stored locally before it is automatically transferred to the final destination in the background. Once the file is stored in the default local volume, the user can continue working without having to wait for the upload to take place.

> Note:
>
> The **Default Local Volume** value must be different than the value of **Default Volume**. Also, either value, **Default Volume** or **Default Local Volume**, can be set without the other being set.

i. Select **User Status**, either **Active** or **Inactive**. The default setting is **Active**.

j. (Optional) Select **Change Ownership** to reassign database objects from a deactivated user to an active user. You may want to change ownership for a short time (maternity leave) or permanently (user left company).

3. You can assign authorized data access (ADA) and International Traffic in Arms Regulations (ITAR) attributes to a user using the boxes in the **ADA/ITAR Attributes** section.

- (Optional) **IP clearance**

  Specifies the intellectual property (IP) clearance level, which is the level of access the user has to sensitive (classified) information. This box is optional.

- (Optional) **Government clearance**

  Specifies the level of clearance that users have to classified data. This box is optional.

- (Optional) **TTC date**

  Specifies the technology transfer certification (TTC) date, which is the date when the user's qualification for viewing exporting data marked as government classified lapses. Teamcenter revokes the user's access rights after the TTC date expires unless renewed. As administrator, you can manually cancel a user's TTC date at any time. This box is optional.

- (Optional) **Geography**

  Specifies the geographical location of the user. Appropriate values are two-character codes from ISO 3166. If not specified, the user is assumed to be at the same location as the database. This box is optional.

- (Optional) **User Declared Geography**

  Specifies the geographical location of the user that is set by the user on the post logon dialog screen. Appropriate values are two-character codes from ISO 3166. If not specified, the user is assumed to be at the same location as the database. This box is optional.

- (Optional) **Nationality**

  Specifies the nationality of the user, which you can set using the LOV containing two-character codes from ISO 3166. This box is optional.

- (Optional) **Citizenships**

  Specifies the citizenships of the user. The user can have multiple citizenships. Setting this value is optional.

  To add a citizenship to the **Citizenships** list, enter a two-letter country code in the text field and click  . To add additional citizenships, click **Edit**  to toggle this field to edit mode, enter the two-letter country code, and click .

  To sort the list of multiple citizenships alphabetically, use **Sort**  .

To remove citizenship entries from the **Citizenship** list, select a citizenship in the **Citizenship** list and click —.

- Citizenship is a two-letter country code from ISO 3166, for example, **US** (United States) and **GB** (Great Britain).
- If a country code LOV is attached to the **fnd()citizenships** property of the **User** business object, a combination box is displayed to allow the selection of a citizenship from the country code list.

4. Set the licensing level to the appropriate level for the tasks the user performs.

   License levels are used to enable usage by time or by features; see your license agreement document for descriptions of available license levels.

   The Teamcenter administrator can change the licensing level of a user during the month. But, once the user logs on, that user's license is considered reserved for the remainder of the calendar month, even if the user's license level is changed after that date. A single user could thereby unintentionally reserve multiple licenses. For example, a single user could reserve three licenses during a calendar month (Author, Consumer, Occasional Author license levels) if they have logged on with each license level.

   Users are always able to log on to their home site.

   If your administrator has set up additional custom properties, you can click the **Add Additional Properties** link to add searchable custom properties on the user profile.

   a. Set the licensing level to the appropriate level for the tasks the user performs.

      License levels are used to enable usage by time or by features; see your license agreement document for descriptions of available license levels.

   b. (Optional) Select the appropriate license server from the **License Server** list. This is a process dedicated to tracking license usage by users.

   c. Select the appropriate license bundle from the **License Bundle** list. As an administrator, you can assign a license bundle to a user.

      If the selected license bundle has a base license level, the **License Level** box is updated with this value and is made noneditable.

5. Set the following site information:

   a. (Optional) **Owning Site**

   b. Select the home site from the **Home Site** list. This is the site from which the user is physically present and works.

c. (Optional) **Deny Login At Sites**.

6. Click **Create**.

   The new user definition is saved in the database and a default role, as defined by the default group, is associated with the user definition.

   Repeat steps 2 and 6 to create additional users.

Specifying password restrictions

Teamcenter enables companies to specify restrictions for passwords when creating user accounts. These password restrictions are controlled through preference settings and take effect upon password creation. Existing passwords are not affected.

Companies can set the following restrictions:

- Minimum length required (**PASSWORD_minimum_characters**)

  Set this preference to a positive integer whose value does not exceed the maximum storage space allocated to a password in your database. The default value is **0**, indicating no minimum password length is required.

- Mixed case required (**PASSWORD_mixed_case_required**)

  Set this preference to **true** if mixed case is required in a password. The default value is **false**, indicating mixed case is not required in a password.

- Minimum number of alpha or numeric characters required (**PASSWORD_minimum_alpha** and **PASSWORD_minimum_digits**)

  Set the **PASSWORD_minimum_alpha** preference to a positive integer whose value, combined with other minimum password length values, does not exceed the maximum storage space allocated to a password in your database. The default value of **0** indicates no minimum is required.

  Set the **PASSWORD_minimum_digits** preference to a positive integer whose value, combined with other minimum password length values, does not exceed the maximum storage space allocated to a password in your database. The default value of **0** indicates no minimum is required.

- Minimum special characters (**PASSWORD_minimum_special_chars**)

  Set this preference to the minimum number of special characters required in a password. Set this preference to a positive integer whose value, combined with other minimum password length values, does not exceed the maximum storage space allocated to a password in your database. The default value is **0**, indicating no minimum is required.

Caution:

Never deploy Teamcenter with default passwords. Default passwords are too well known.

Use high-entropy (strong) passwords for all accounts, especially for **infodba**, **dcproxy**, operating system user values used for installation, and the **DB_CONNECT_STRING** value. For example, **oiunr0i##++9dE** is stronger than **mypassword**.

The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab.

In addition, the password must not contain any of the following characters:

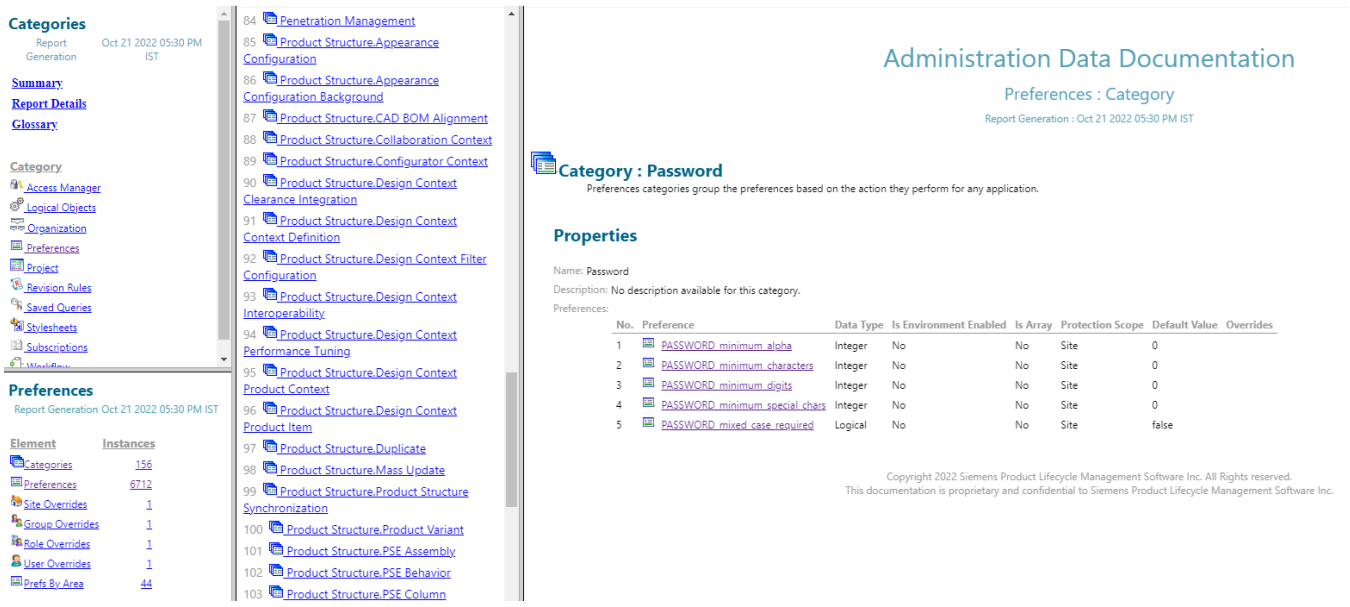
! # @ $ % = & ' " ^ : ; . _ < > ( ) { }

Protect all files containing passwords with OS permissions. Encrypted or not, the read access to these files must be guarded because hackers cannot break the encryption if they can't read the contents.

Once you have set up your organization, you can run the **administration data documentation report** to verify these password preferences settings by running the **generate_admin_data_report** utility as follows:

```
generate_admin_data_report -u=admin-username -p=admin-password
        -g=dba -adminDataTypes=all -outputDir=C:\temp\admin_data\siteA
```

From the administration data documentation report, select **Preferences→Preference Categories→Password** to display the password preferences.



Examples

```
PASSWORD_mixed_case_required=false

PASSWORD_minimum_alpha=0

PASSWORD_minimum_digits=0

PASSWORD_minimum_special_chars=0
```

Note:

If a user attempts to log on to Teamcenter without entering a password, a logon failure occurs.

Configuring ADA for ITAR support

When creating users, you can define the following ADA/ITAR attributes for each user in the **ADA/ITAR Attributes** section of the **Users** pane:

- IP clearance

  Intellectual property (IP) clearance applies to a specific user and specifies the level of access the user has to sensitive (classified) information.

- Government clearance and TTC date

  Government clearance status and technology transfer certification (TTC) date track the user's level of clearance for viewing data marked as government classified. Teamcenter revokes the user's access rights after the TTC date expires unless renewed. As an administrator, you may manually cancel a TTC at any time.

- Geography, nationality, and citizenship

  Use nationality, citizenship (one or more), and geography (physical location) attributes to determine if the user is a foreign (non-U.S.) national for ITAR purposes or a U.S. national located outside the U.S. If the user views classified material, this material is considered an ADA export and requires a license granting the user rights to export

  Geography, nationality, and citizenship information is private and viewing is restricted as follows:

  - Users can view their own information.
  - Users with system administration privileges can view everyone's information.

Use the following preferences to access ADA/ITAR attributes information.

- **Hide_User_Privacy_Information** set to **TRUE** hides geography, nationality and citizenship information.

- **Hide_User_Clearance_Information** set to **TRUE** hides IP clearance, government clearance, TTC date information.

Add an existing user to a role/group using the Organization User wizard

The Organization User wizard can be used to add an existing user to a group during the process of creating a group/role combination in the **Organization** tree.

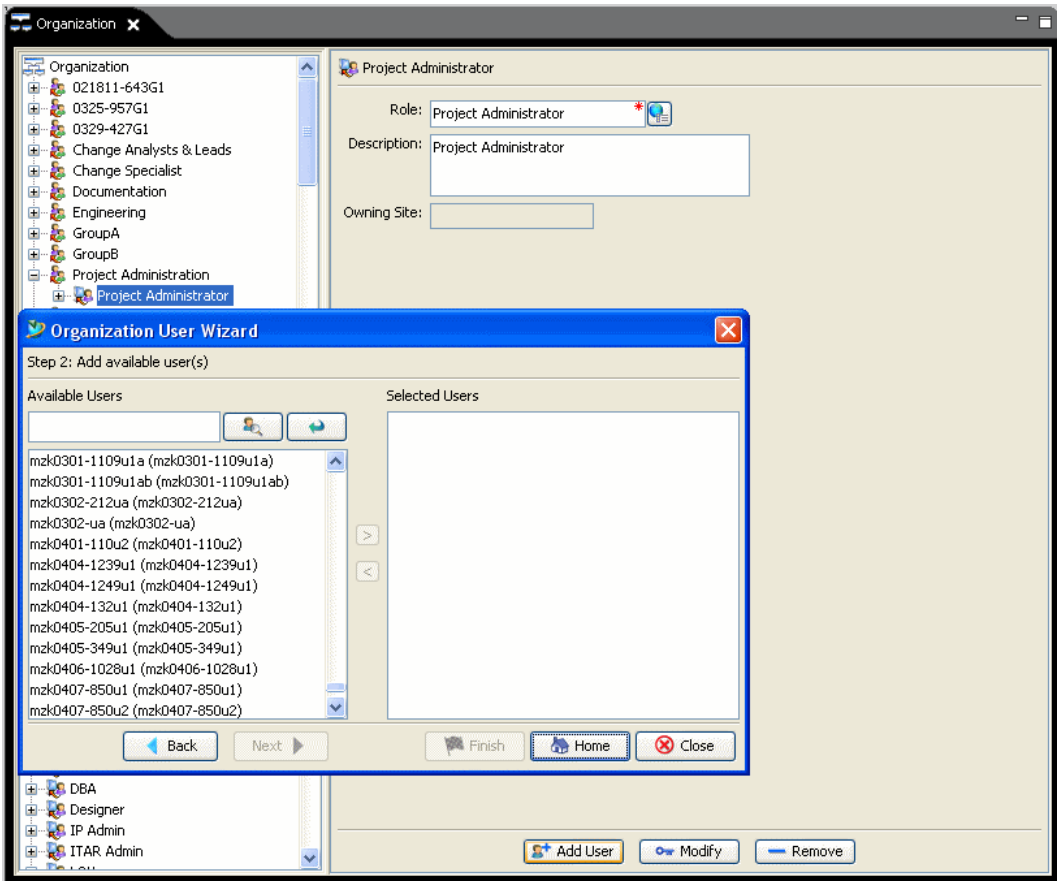
Existing users can also be added to existing group/role combinations within the **Organization** tree. The procedure for using the Organization User wizard to add an existing user is the same, regardless of the activity being performed when the wizard is invoked.

1. Select a role node from the **Organization** tree.

2. Click **Add User**.

3. Select **Add existing user to the group/role** and click **Next**.

4. Select the users to add from the **Available Users** list.



You can also use either of the following buttons in the search pane:

- Find users
- Reload all available users

You can move items between the **Available Users** and **Selected Users** lists by double-clicking a user or selecting a user and clicking the right arrow (▶) or left arrow (◀) buttons. After you select all the users to be added, click **Finish** to continue or **Close** to dismiss the wizard.

5. If you clicked **Finish**, a message appears asking if you want to add the selected users. Click **Yes**.

6. Click **OK**.

   The **User(s) added** dialog box closes and you are returned to step 1 on the Organization User wizard.

   The user appears in the **Organization** tree as a child of the selected role.

7. Click **Close** or repeat steps 1 through 6 to add additional users to the same role/group combination.

Add a new user to a group/role using the Organization User wizard

You can add a new user to the **Organization** tree as part of the process of creating the group/role hierarchy.

You can also add a new user to an existing group/role combination in the **Organization** tree. The procedure for using the Organization User wizard to add a new user is the same, regardless of the activity being performed when the wizard is invoked.

1. Select a role node from the **Organization** tree.

   The **Roles** pane appears.

2. Click **Add User**.

   The Organization User wizard appears.

3. Select **Add new user to the group/role** and click **Next**.

4. Create the user by performing the following substeps:

   a. Define the person to be associated with this user. If the person definition already exists, click **Person Name** to display the **List of Defined Persons** list and select, by double-clicking, a person name from the list. If a person definition does not yet exist, type the name of the individual in the **Person Name** box.

   b. Type a unique user name in the **User ID** box.

   c. Optionally, type a password. **Default Group** and **Roles** are already filled in for you.

   d. Click **Default Volume** to display the **List of Defined Volumes** list and select, by double-clicking, a default volume for the group.

      > Caution:
      >
      > If you create a group without assigning a default volume, group members cannot save datasets. Therefore, Siemens Digital Industries Software recommends that you assign a default volume for the group.

   e. Click **Default Local Volume** to display the **List of Defined Volumes** list and select, by double-clicking, a default local volume for the group.

> Note:
>
> The **Default Local Volume** value must be different from the value in the **Default Volume** box.

f. Set the licensing level to the appropriate level for the tasks the user performs.

License levels are used to enable usage by time or by features.

For descriptions of the available license levels, see your license agreement documentation.

g. Select the appropriate license server from the **License Server** list. As an administrator, you can assign a license server to a user.

h. Select the appropriate Teamcenter license bundle from the **License Bundle** list. As an administrator, you can assign a license bundle to a user.

If the selected license bundle has a base license level, the **License Level** box is updated with this value and is made non-editable.

i. When all required input is complete, click **Next** or **Finish**.

j. Click **Yes** to create the new user.

If you created a new person definition while creating the new user, go to step 5. If you did not create a new person definition, go to step 6.

5. The **Create Person** dialog box appears. Click **Yes** to confirm that you want to create the new person.

6. The **User(s) added** dialog box appears. Click **OK**.

The **User(s) added** dialog box is dismissed and you are returned to step 1 of the Organization User wizard.

The new user appears as a child of the selected role in the **Organization** tree. Additionally, the new user and person (if applicable) are displayed in the **Organization List** tree.

> Note:
>
> Persons are not displayed in the **Organization** tree.

7. Click **Close** to dismiss the Organization User wizard or repeat steps 3 through 6 of this section to add additional users to the same role/group combination.

Managing external user constructs in Teamcenter

You can organize and manage your user base on a corporate LDAP directory server that is also used as a central user authentication repository for applications, such as Teamcenter, using either external or internal user constructs.

What is the difference between externally managed and internally managed user constructs?

User construct type	Description
Externally managed	User data (users, groups, and roles) is replicated and synchronized to your Teamcenter database using the **make_user** utility.
Internally managed	User data (users, groups, and roles) is created and maintained in Teamcenter.

The **make_user** utility helps you manage the entire life cycle of the user by:

- Supporting user, role and group creation.
- Handling all related management activities, such as setting security context, license level, activation, deactivation, and so on.
- Providing a batch processing mode with an input file using special syntax, where every line is a single entry that describes a single operation, such as creating, adding, and removing and users.

Example of using the make_user utility

To feed the user construct from your corporate LDAP directory to Teamcenter, you can extract the user data using a script and transform the data into an input file for the **make_user** utility. Then, execute the utility to create the user, group, and role artifacts in Teamcenter.

Similarly, to handle changes in the user data in LDAP, you can follow the same process to create an input file and run the **make_user** utility in update mode.

Mapping and synchronization considerations

The synchronization process affects only user data that is new, or has been removed, deactivated, or updated. Certain attributes have special handling during the synchronization process, as follows:

- Externally managed passwords are never synchronized with Teamcenter.

  The passwords of externally managed users are set to the same value as the user ID. This is merely a placeholder, because sites using external synchronization must also have external authentication configured; therefore, user passwords are authenticated against the LDAP directory.

- User status should not be mapped from an LDAP attribute. User status, active or inactive, is synchronized with Teamcenter based on the following conditions:

  - If the user exists in the LDAP server but not in Teamcenter, the user is created in Teamcenter using the mapped attributes from LDAP. The user is configured to be externally managed and the user's status in Teamcenter is set to active.

  - If the user exists in both the LDAP server and Teamcenter and the user is configured to be externally managed, the user's mapped attributes are synchronized from LDAP to Teamcenter. The user's status in Teamcenter is set to active.

  - If the user exists in Teamcenter but not in the LDAP server and the user is configured to be externally managed, the user's status in Teamcenter is set to inactive.

    The status field acts as an emergency override for the Teamcenter administrator to disable externally managed user accounts without updating the external directory and running the synchronization process.

Define your organization using Setup Wizard and data from an input file

What is Setup Wizard?

Administrators use Setup Wizard to create a Teamcenter virtual organization. The wizard enables administrators to map the contents of an input file, such as an output file generated from Microsoft Exchange, a text editor or the **etc/passwd** file on a Linux system, to the fields required to create user/person definitions in the database. This mapping eliminates the need to individually create these definitions. After the input file is mapped, administrators can create volume associations and assign a group/role to each user.

> Note:
>
> While Setup Wizard is a convenient tool for adding bulk user data to your database, it is intended to supplement, not replace, the functionality of the Teamcenter Organization application.

When you use Setup Wizard, you must decide whether or not to create a **Volume** definition. If created, this volume is assigned to any and all groups that you associate with users in **Step 7: Select group/role for users**. Although groups can be created without assigning a default volume, the group members cannot save datasets until a default volume is assigned. Therefore, Siemens Digital Industries Software recommends that you assign a default volume.

Setup Wizard prompts you through a series of steps to create person and user definitions.

At any time while using Setup Wizard, you can click **Back** to return to the previous step or **Home** to return to step 1. To exit Setup Wizard, choose **File→Close**.

When performing the following Setup Wizard steps, every field displaying a red asterisk is a required field. Fields without a red asterisk are optional.

Loading data from an input file using Setup Wizard

Using Setup Wizard

At any time while using Setup Wizard, you can click **Back** to return to the previous step or **Home** to return to step 1. To exit Setup Wizard, choose **File→Close**.

When performing the following Setup Wizard steps, every field displaying a red asterisk is a required field. Fields without a red asterisk are optional.

Step 1: Start Setup Wizard

1. Start Setup Wizard by clicking **Setup Wizard**  in the navigation pane.

   Teamcenter displays the Setup Wizard welcome window.

2. Click **Next**.

Step 2: Enter input file and delimiter

Select the input file to use in order to populate the person/user information in your Teamcenter organization. The following are examples of possible input files:

- **etc/passwd** file on Linux machines
- Output files generated from Microsoft Exchange or standard security information on Microsoft Windows-based platforms

The information contained in the input file must be delimited by at least one single character delimiter (primary delimiter) to enable accurate mapping of the file data to the database fields. Setup Wizard accepts a primary and a secondary input file delimiter. For example, consider the following Linux **etc/passwd** file:

```
userName:passwd:usedId:groupId:UserDetails:user_home_dir:user_default_she
ll
```

In this example, a colon character (**:**) is the primary delimiter separating the complete line in the **etc/passwd** file into different fields. A comma character (**,**) is the secondary delimiter separating **User Details** into **Person Name**, **Address**, and **City**.

1. Enter the input file name, including path, in the **Select Input File** box or click **Browse** to choose a file from the OS directory.

2. Type the primary and secondary delimiters used in the input file. You can only use single-character delimiters.

3. Click **Next**.

Step 3: Provide mapping information of the input file

1. Map the input file information to the **Person/User** definition fields by selecting a value from the list for each field.

Field	Description
User ID	User IDs must be unique. This field is mandatory.
Person Name	Person names must be unique. This field is mandatory.
Address	(Optional)
City	(Optional)
State	(Optional)
ZIP Code	(Optional)
Country	(Optional)
Organization	(Optional)
Employee Number	(Optional)
Internal Mail Code	(Optional)
EMail	(Optional)
Telephone	(Optional)

2. When you complete mapping the file, click **Next**.

Step 4: Select groups/roles to use while creating users

Select groups and roles that are later assigned to the user definitions being created from the input file. You can select existing groups/roles or add new groups/roles. **Step 7: Select group/role for users** guides you through the process of assigning these groups/roles to users.

You must select at least one group or group/role combination.

1. To add a new group/role:

   You can create a new group or a new group/role combination. However, you cannot use Setup Wizard to create a role without an associated group.

a. Type a name for the new group in the left-hand box in the **New Group Role** box.

b. (Optional) Type a name for the new role in the right-hand box in the **New Group Role** box.

c. Click **Add Group/Role**.

The new group or group/role combination appears in the **Selected Group/Role** list.

2. To select an existing group/role:

> Note:
>
> The **Existing Group/Role** list displays the group/role combinations that are currently defined in the database.
>
> If you are using Setup Wizard to populate a new postinstallation database, **dba/DBA** and **system** are the only entries in the **Existing Group/Role** list.

a. Select a group or group/role combination from the **Existing Group/Role** list and click  . The group/role appears in the **Selected Group/Role** list.

To remove a selection from the **Selected Group/Role** list, click  .

b. Repeat the previous step to select additional group/roles.

3. After you complete adding or selecting groups/roles, click **Next**.

Step 5: Create a volume

You can create a volume association for any groups you assign in **Step 7: Select group/role for users**. Siemens Digital Industries Software recommends that you create a default volume for these groups.

1. Click **Yes** or **No** to respond to the following question:

```
Do you want to create Volume?
```

2. Click **Next**. If you choose to create a volume, proceed to **Step 6: Enter volume details**; if you choose not to create a volume, proceed to **Step 7: Select group/role for users**.

Step 6: Enter volume details

1. Type a unique and descriptive character string in the **Volume Name** box.

2. Select the machine type on which the volume will reside: **Linux**, **Windows**, or **Cloud**.

Currently, Teamcenter supports Linux and Microsoft Windows volumes in homogeneous and heterogeneous environments.

3. Type the name of the node where the Teamcenter File Services process is running in the **Node Name** box.

4. Depending on the (non-cloud) machine type selection made in the previous step, type either the full Linux path of the new volume in the **Linux Path Name** box or the Microsoft Windows path of the new volume in the **Windows Path Name** box.

5. Select the ID type to indicate the element in the FMS master configuration to which the new volume element is to be added.

> Note:
>
> When a new volume is created, the user must specify where in the FMS master configuration the definition of this volume should be placed: the FSC element section, the filestore group section, or the load balancer section.

6. Type the ID of the element identified in the previous step in the **ID** box.

   Click **Next**.

Step 7: Select group/role for users

1. To assign all users to the same group/role combination, select the **Same Group for all Users** check box. If you do not want to assign the same group/role to all users, clear the check box.

2. Double-click in the group cell that corresponds to the user to whom you want to assign a group/role. The list of selected groups/roles appears. For additional information on adding groups/roles to the selection list, see step 4.

3. Select the group/role that you want to assign to the user. Selecting **Same Group for all Users** assigns this group/role to all users.

4. If assigning groups/roles to users individually, repeat steps 2 and 3 until all users are assigned a group/role.

5. Click **Next** or **Finish**.

Step 8: Create objects in Teamcenter

1. Click **Yes** to create objects in the Teamcenter database.

   Setup Wizard displays a list of processes to be completed.

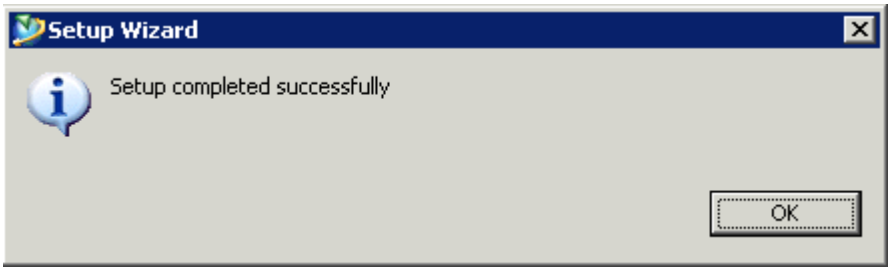
The content of the list of processes depends on the choices made while performing each Setup Wizard step. You can generate any or all of the following processes:

- **Creating Person**
- **Creating User**
- **Creating Group**
- **Creating Role**
- **Creating Volume**
- **Adding Role to Group**

As the objects are created, check marks appear in the boxes next to the processes to indicate that they have been completed. The mark to the right of the process indicates successful or unsuccessful completion.

If an error occurs during a process, an button appears to the right of the process. Click to display information about the error.

When all processes are successfully completed, the following message appears:



2. Click **OK**.

Setup Wizard is now complete. The users, groups/roles, and volumes defined using Setup Wizard are added to the database and are displayed in the Teamcenter **Organization** tree.

5. Optional organizational setup tasks

Defining disciplines

What is a discipline?

A *discipline* is a set of users who have a common behavior, for example, developers that have expertise in Linux.

You have the option to define a discipline for each Teamcenter user. As a user with **DBA** or group administrator privileges, you can use the Organization application to:

- Create disciplines.
- Modify disciplines.
- Delete disciplines.
- Add disciplines to a group.
- Remove disciplines from a group.

Create a discipline

1. Select the top-level **Disciplines** node from the **Organization List** tree.

   The **Disciplines** pane appears.

2. Complete the following information:

   a. Type a unique name in the **Name** box.

   b. (Optional) Type a description in the **Description** box.

   c. Type a default rate in the **Default Rate** box, or accept the default value.

   d. Select the currency type from the **Default Currency** list, for example, **USD**, which denotes United States dollars.

   e. Select users from the **List of Users** list. Add one or more users to the list by selecting a user from the **List of Users** and either double-clicking the user name or clicking the plus button to move them to the **List of Associated Users** list. You can remove users from the **List**

of Associated Users list by double-clicking a user or selecting a user and clicking the minus button —.

3. Click **Create** .

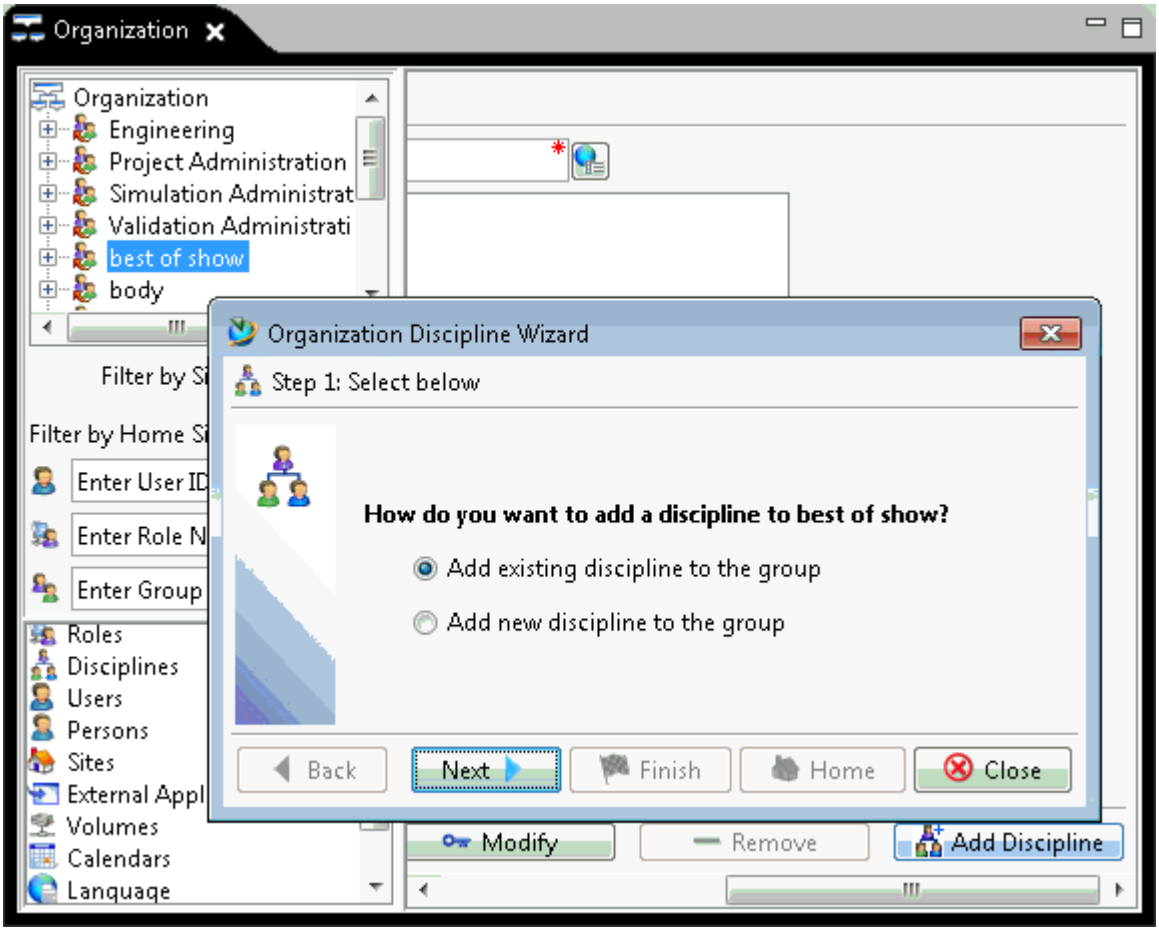
Add a discipline to a group

1. Select a group from the upper-left corner of the **Organization** tree.

   The associated group pane appears.

2. Click **Add Discipline**.

   The **Organization Discipline Wizard** appears.



3. Click **Next**.

4. Select the discipline to add to the group, click the plus button + to add the discipline to the **Selected Disciplines** list.

5. Click **Next**.
6. Click **Yes** to add the selected discipline.
7. Click **Close**.

The selected discipline is added to the group.

Maintaining disciplines

Modify a discipline

1. From the **Organization List** tree, double-click **Disciplines** to display the existing disciplines.
2. Select the discipline to be modified.

   The **Disciplines** pane displays the discipline definition.
3. Modify any information in the **Disciplines** pane by typing over the existing information.
4. Click **Modify**.

The system saves the changes to the discipline definition.

Delete a discipline

1. From the **Organization List** tree, double-click **Disciplines** to display the existing disciplines.
2. Select the discipline to be deleted.

   The **Disciplines** pane displays the discipline definition.
3. Click **Delete**.

   The **Delete Confirmation** dialog box appears.

The **Disciplines** pane clears and the discipline is deleted from the database.

Remove a discipline from a group

1. Select a group from the upper-left corner of the **Organization** tree.

   The associated group pane appears.

2. Select the discipline to remove.

3. Click **Remove** —.

The selected discipline is removed from the group.

Defining calendars

Selecting which calendar type to use

Teamcenter allows you to create four types of calendars that allow you to consider things like work days, work hours, holidays, and vacations when developing schedules for your projects.

- The *base calendar*, which is installed by default with Teamcenter, is used as the master calendar when creating schedules. It shows which days are workdays, hours in a workday, holidays, and days off. As an administrator, you can modify the base calendar using Organization.

  Teamcenter provides the following three default base calendars:

  - Standard
  - Night shift
  - 24 hours

  A site can have several base calendars.

- The *user calendar* allows you to set days off, holidays, and hours in a day for the current user. You can create it using either My Teamcenter or Organization.

- The *schedule calendar* allows you to set days off, holidays, and hours in a day for the current schedule.

- The *schedule user calendar* allows you to set days off, holidays, and hours in a day for an individual resource (person or discipline).

As a user with **DBA** or group administrator privileges, use the Organization application to modify the base calendar and create and modify the user calendar.

Create a user calendar

When creating new calendars, Teamcenter determines the default time zone as follows:

1. Teamcenter checks the **Time Zone** property on the default calendar. If this property is set, its value is used.

2. If that property is not set, Teamcenter checks the **SiteTimeZone** preference. If this preference is set, its value is used.

3. If neither of these are set, Teamcenter uses GMT as the time zone.

If Teamcenter is using GMT and that is not the correct time zone for your site, you may encounter unexpected behavior. Therefore, Siemens Digital Industries Software recommends that you set both the Time Zone property on the default calendar and the **SiteTimeZone** preference.

1. Double-click the **Users** node  from the **Organization List** tree to display a list of users.

   The **Users** pane appears.

2. Select a user from the **Organization List** tree.

3. Right-click the user and choose **Calendar→Create Calendar**.

   A calendar is added to the **Calendars** node for the user.

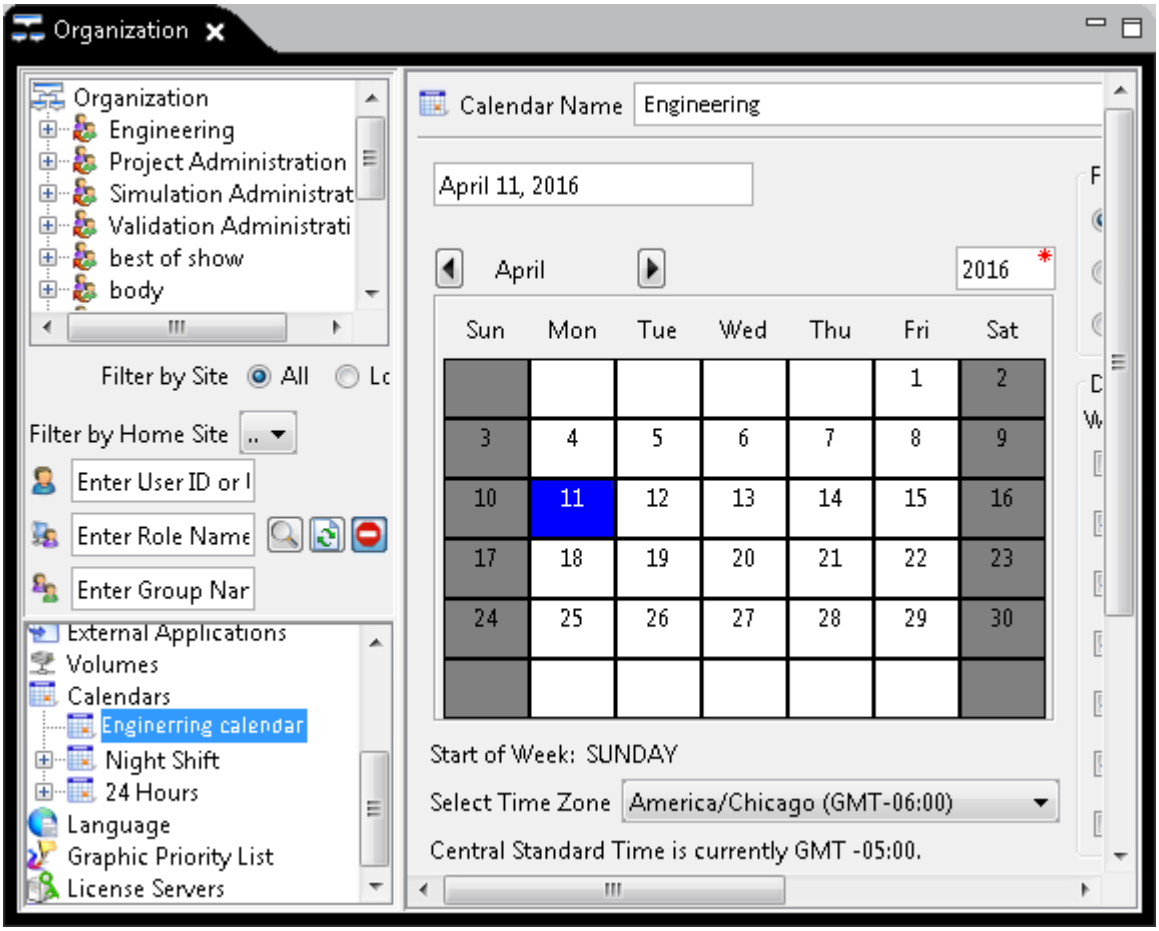
   The **Create User Calendar** dialog box appears. Click **Yes** to verify you want to create a user calendar.

Maintaining calendars

Modify the base calendar

1. Select a calendar to modify, for example, **Engineering calendar**, from the **Calendars** node  in the **Organization List** tree.

   The calendar to be modified appears in the calendar pane.



2. Edit the calendar information for your desired implementation.

   a. Select the month and year by either:

      - Clicking the right arrow (▶) or left arrow (◀) buttons.
      - Entering the desired date in the date field.

   b. Select the items from the **For Selected Dates** list.

   c. Select the working hours from the **Daily Defaults** list.

3. Click **Modify** .

The system saves the changes to the calendar definition.

Modify a user calendar

1. Select the **Calendars** node from the **Organization List** tree.

The tree expands to show all existing users who have calendars on the system.

2. Select a calendar from the **Organization List** tree.

   You can now edit the calendar.

3. Click **Modify** to save the changes to the user's calendar.

Creating external applications

External applications are part libraries that are based on site objects.

In the Organization application, you can create, modify, and delete external applications.

1. Select the top-level **External Applications** node from the **Organization List** tree.

   The **External Applications** pane appears.

2. Complete the following information:

   a. Type a unique application name in the **Application Name** box using any combination of alphanumeric characters. You can use the hyphen (-) and underscore (_) special characters.

   b. Type a unique application ID in the **Application ID** box. The application ID must be any valid positive integer.

      To automatically generate a unique application ID, click the **Assign** button.

   c. Select the application type from the **Application Type** list.

   d. Select **Allow deletion of replicated master items to this site** to allow the deletion of replicated master items.

      The **Uses TCXML Payload** check box is only for information purposes and cannot be modified.

3. Click **Create**.

Maintaining part libraries

Modify an external application

1. From the **Organization List** tree, double-click the **External Applications** node to display the existing external applications.

2. Select the external application to be modified.

   The **External Applications** pane displays the properties of the external application definition.

3. Modify any information contained in the **External Applications** pane by typing over the existing information.

4. Click **Modify**.

The modified external application definition is saved in the database.

Delete external applications

1. From the **Organization List** tree, double-click the **External Applications** node to display the existing external applications.

2. Select the external application to be deleted.

3. Click **Delete**.

   The **Delete Confirmation** dialog box appears.

4. Verify that the correct external application is selected.

5. If the correct external application is displayed, click **Yes**.

The **External Applications** pane clears, and the external application definition is deleted from the database.

6. Maintaining your organization

Maintaining sites

Modify a site

> Caution:
>
> Never change the site ID of a database after it is established. The site ID is used to generate internal identifiers for Teamcenter objects that must be unique throughout your enterprise. Never reuse a site ID when creating a new database.

1. Select the node of the site definition to modify from the **Organization List** tree.

   The **Sites** pane displays the properties of the site definition.

2. Modify the **Site Name** box.

   > Warning:
   >
   > Ensure that the proper site ID is entered. Failure to do so may compromise data integrity.

   If you are using Multi-Site Collaboration and this site is configured to provide object directory services (ODS), perform step 3. Otherwise, go to step 4.

3. Select **Provide Object Directory Services**.

4. Optionally, modify the **Site Node/URL** box.

5. Optionally, select **Is A Hub**.

6. Click **Modify**.

The system saves the changes to the site definition.

Delete a site

1. Select the node of the site definition to delete from the **Organization List** tree.

   The **Sites** pane displays the properties of the site definition.

2. Verify that the correct site is selected.

3. Click **Delete**.

The **Delete Confirmation** dialog box appears.

4. Click **Yes** to delete the site.

The **Sites** pane clears and the site is deleted from the database.

Maintaining license servers

Modify a license server

1. From the **Organization List** tree, double-click **License Servers** to display the existing license servers.

2. Select the license server to be modified.

   The **License Servers** pane displays the license server definition.

3. Modify any information in the **License Servers** pane by typing over the existing information.

4. Click **Modify**.

Delete a license server

1. From the **Organization List** tree, double-click **License Servers** to display the existing license servers.

2. Select the license server to be deleted.

   The **License Servers** pane displays the license server definition.

3. Click **Delete**.

   The **Delete Confirmation** dialog box appears.

The **License Servers** pane clears and the license server is deleted from the database.

Maintaining volumes

Modify volume location

You can use Organization to move a volume from one location to another on the *same* host. Moving volumes involves copying the volume and its contents to a new location and deleting the old volume.

Note:

Moving a volume is different than merely modifying the path name attribute of the volume. Simply modifying the path name leaves the volume data in the original location. Teamcenter looks for the data in the new path name location and cannot find it, rendering the data inaccessible to users.

A situation in which you use Organization to modify the path name attribute is after moving a volume to a *different* host, for example, after using operating system copy tools to move a volume from one host to another host within the same enterprise. In this situation, after moving the volume, use Organization to modify the path name attribute of the volume as described in step 6 of the following procedure.

Warning:

To ensure data integrity, volumes must be moved only when there are no users logged on to Teamcenter.

1. Ensure that all users are logged off Teamcenter.

2. Select the volume to be moved from the **Volumes** list in the **Organization List** tree.

3. Type the path name of the new volume location in the **Path Name** box.

4. Type the ID in the **ID** box because this value is not persisted in the database.

5. Click **Modify**.

   Teamcenter displays the **Move Volume** dialog box, prompting you to confirm whether you want to move the selected volume.

   Note:

   Moving a volume can take an extended period of time. The exact time required depends on system, network bandwidth, and the amount of data being moved.

6. Perform one of the following steps:

   - Click **Yes** to move the volume.

     The selected volume and all existing data within the volume are moved to the new location.

   - Click **No** to change the volume location without moving the volume data.

     Teamcenter displays the **Modify volume** dialog box, informing you that the data will be lost due to modification and prompting you to confirm whether to continue.

Note:

Modifying the volume location does not delete the data. However, the data is inaccessible once the volume location is modified.

Modifying volume properties

Warning:

To ensure data integrity, modify volume properties only when no users are logged on to Teamcenter. When modifying the path name, the new path must be a valid operating system directory. Changing the path to an invalid directory results in loss of data.

1. Ensure that all users are logged off Teamcenter.
2. Select the volume to be modified from the **Organization List** tree.

   Teamcenter displays the properties of the volume in the **Volumes** pane.
3. Modify information in the **Volume Name**, **Node Name**, **Machine Type** or **Path Name** boxes.
4. Click **Modify**.

The system saves the changes to the volume definition.

Delete a volume

The following are important restrictions you should note when deleting a volume.

- An existing volume can be deleted only if there are no database references to the volume.
- A volume to be deleted must not be designated as the default volume of any group or user.
- Users must not have access to the volume. If objects were created that placed files in the volume, the objects must be deleted or moved to a different volume using a customized ITK program.

1. Select the volume to be deleted from the **Organization List** tree. Teamcenter displays the properties of the selected volume definition in the **Volumes** pane.
2. Verify that the correct volume has been selected.
3. Click **Delete**.

   The **Delete Confirmation** dialog box appears.

4. Click **Yes** to delete the volume.

The volume is deleted from the database.

Managing volumes

Reallocating volume data

As an administrator, you can reallocate volume data by defining volume storage criteria based on business data using volume reallocation rules. These rules are defined in an XML file and managed with the **-rulesfile** and **-outrulesfile** arguments of the **move_volume_files** utility.

For example, consider a site using both CAD and JT files. Because JT files are volatile and can be recovered from the CAD file if lost, they are on a different backup schedule. The administrator wants all JT files stored in a different volume than the CAD files. Rules can be written in the XML file specifying different target volumes for the JT and CAD files. Each time the utility is run, JT and CAD files not already stored in the respective target volume are moved to the appropriate destination. You can run the utility manually or as a **cron** job.

> Note:
>
> The volume reallocation rules do not affect any existing default volume settings or default local volume settings.

Using the move_volume_files utility

The **move_volume_files** utility moves files from one volume to another by copying the files from source volume to destination volume, commits the database changes, and rolls back the copied files from the source volume. You can list the files that are candidates to be moved and move the files based on the following:

- Last access data
- File size
- User-supplied input file list
- Volume selection rules and criteria supplied by an XML file.

The **move_volume_files** utility moves files within the same volume from the current volume subdirectory structure to the new subdirectory structure that has a controlled maximum number of files.

Managing volume failover behavior

You can manage volume failover behavior by using the following preferences:

- **TC_Volume_Failover_Trigger**

  Specifies the percentage full of a volume at which the file import is sent to the failover volume. The default value is **90**.

  Siemens Digital Industries Software recommends setting this preference between **80** and **95**. Setting this value too low triggers failover behavior too often. Setting this value too high prevents failover behavior from initiating.

- **TC_Volume_Failover_Volume_Name**

  Specifies the volume to use in a failover situation. **TC_Volume_Failover_Volume_Name** accepts a single string as a value; the string must be a valid volume name. When set, the system checks the original target volume before import. If the target volume is filled beyond the capacity specified by the **TC_Volume_Failover_Trigger** preference, the imported file is directed to the failover volume specified by **TC_Volume_Failover_Volume_Name**.

- **TC_Volume_Status_Resync_Interval**

  Specifies the minimum amount of time (in seconds) that can pass before the percent full value of a volume is retrieved from File Management System. The percentage full values are cached to prevent excessive FSC requests.

  The system checks for this cached value only during file import, and only when volume failover during file import behavior is enabled by setting the **TC_Volume_Failover_Volume_Name** preference.

  The default value is **600** seconds. Siemens Digital Industries Software recommends keeping this setting similar to the default value. Setting this value too high causes the cached percentage full value to be out of date. Setting this value too low generates excessive FSC requests.

Display the volume path in the rich client

Display the full path of Teamcenter volume files in rich client applications by setting the **IMF_display_full_path** preference to **TRUE**. Doing so causes, as an example, the full path to the Teamcenter volume in which the dataset is stored to be shown when clicking **Print** in the **Dataset Properties** dialog box.

By default, this site preference is not listed in the **preferences.xml** file and must be added before setting as described in Creating preferences from within the rich client.

Maintaining roles

Modify a role

1. Perform one of the following substeps:

- Select a role definition from the **Organization List** tree.
- Select a role definition from the **Organization** tree.

The **Roles** pane appears.

2. Modify any information contained in the **Roles** pane boxes by typing over existing information.
3. Click **Modify**.

The modified role definition is saved in the database.

Delete a role

As your organization evolves, you may want to permanently remove a role from the database. Roles can only be deleted by accessing the **Roles** pane from the **Organization List** tree.

> Caution:
>
> Do not delete any default roles, for example, the **Project Administrator** role. Doing so can cause issues with the rule tree or other processing that depends on them. Siemens Digital Industries Software recommends you leave all default roles in place, even if you are not using the functionality related to these roles.

You cannot delete a role that is referenced by another organization object.

1. Select the role node to be deleted from the **Organization List** tree.

   The **Roles** pane appears.

2. Verify that the correct role is selected.
3. Click **Delete**.

   The **Delete Confirmation** dialog box appears.

4. Click **Yes** to delete the role.

The **Roles** pane clears and the role is deleted from the database.

Add an existing role to a group using the Organization Role wizard

The Organization Role wizard can add an existing role to a group or subgroup in the **Organization** tree. Existing roles can also be added to existing groups in the **Organization** tree. The procedure for using the Organization Role wizard to add an existing role is the same, regardless of the activity being performed when the wizard is invoked.

1. Select the group node in the **Organization** tree to which you want to add the role.

   The **Groups** pane appears.

2. Click **Add Role**.

   The Organization Role wizard appears.

3. Select **Add existing role to the group** and click **Next**.

   > Note:
   >
   > The first role added to a group becomes the default role for that group.

4. Select the roles to be added to the group from the **Existing Roles** list. You can move items between the **Existing Roles** and **Selected Roles** lists by double-clicking a role or selecting a role and clicking the plus (+) or minus (—) buttons. When you select all the roles to add, click **Finish** to continue or **Close** to dismiss the wizard.

5. If you clicked **Finish**, perform one of the following actions:

   - Select a **What is next?** option from the wizard. You can **add another role** to the selected group or **add a user to the role** you just added.
   - Click **Home** to return to step 1 of the Organization Role wizard.
   - Click **Close** to dismiss the wizard.

The role is added to the **Organization** tree.

Add a new role to a group using the Organization Role wizard

You can use the Organization Role wizard to add a new role to a group during the process of creating the group or subgroup in the **Organization** tree.

New roles can also be added to existing groups or subgroups in the **Organization** tree. The procedure for using the Organization Role wizard to add a new role is the same, regardless of the activity being performed when the wizard is invoked.

1. Select the group node in the **Organization** tree to which you want to add the role.

   The **Groups** pane appears.

2. Click **Add Role**.

   The Organization Role wizard appears.

3. Select **Add new role to the group** and click **Next**.

> Note:
>
> The first role added to a group becomes the default role for that group.

4. Type the following information and click **Close** to create the new role or click **Finish** to perform another action:

   - A new role in the **Role** box.
   - Optionally, a descriptive character string in the **Description** box.

5. If you clicked **Finish**, perform one of the following actions:

   - Select a **What is next?** option from the wizard. **You can add another role to the selected group** or **add a user to the role you just added.**
   - Click **Home** to return to step 1 of the Organization Role wizard.
   - Click **Close** to dismiss the wizard.

The role appears in the **Organization** and **Organization List** trees.

Assign a default role within a group

1. In the **Organization** tree, expand the group and role structure corresponding to the role that you want to set as the default.

   Teamcenter displays the users assigned to this role.

2. Select the user node.

   Teamcenter displays the user information.

3. In the **Group Member Settings** section, select the **Default Role** check box.

4. Click **Modify**.

Maintaining groups

Modify a group

You can modify group definitions using the **Organization List** tree or the **Organization** tree.

1. Perform one of the following steps:

   - Select the group to be modified from the **Organization List** tree.
   - Select the group to be modified from the **Organization** tree.

   The **Groups** pane displays the group definition.

   Caution:

   Changing existing group names or structure (for example, reparenting a group) can drastically impact Workflow functionality. Workflow processes do not complete if the group names are changed after the process is started. Therefore, all Workflow processes, including Cascade Release (CR) and Change Management (CM) processes, must be modified *before* they are started to reflect any changes in group names or structure, or they fail. Additionally, all current (started) EPM jobs affected by group name or structure changes must be terminated and new jobs must be started from updated procedure templates.

   Because the group name is used in the directory structure to store and locate information, changing the group name does not change the path to existing datasets.

2. Modify any information in the **Groups** pane by either typing over the existing information or selecting a different option from the defined lists.

   To select a different option from a defined list, you must first click **Clear** in the list dialog box and then select another item from the list by double-clicking.

3. Click **Modify**.

The system saves the changes to the group definition.

Delete a group

Warning:

Do not delete the **system** group from the database under any circumstances. Teamcenter does not function properly without this group.

Caution:

Do not delete any default groups, for example, the **Project Administration** group. Doing so can cause issues with the rule tree or other processing that depends on them. Siemens Digital Industries Software recommends you leave all default groups in place, even if you are not using the functionality related to these groups.

Note:

You cannot delete group definitions that are referenced by another Organization object. You must first delete users and roles referenced by the group.

1. Select a group from the **Groups** list.

   The **Delete Confirmation** dialog box appears.

2. Verify that the correct group is selected.

3. Click **Delete**.

   The **Delete Confirmation** dialog box appears.

4. If the correct group appears, click **Yes**.

The **Groups** pane clears and the group is deleted from the database.

Maintaining group members

Managing group members

As your real-world organization evolves and changes, your Teamcenter virtual organization also changes. Implementing new projects, promoting personnel, and restructuring your organization are all examples of real-world events that would necessitate changes involving group members.

Remove a member from a group

Note:

You cannot remove the last instance of a user from the **Organization** tree if the group from which you are removing the user is the user's default group.

1. Select the user (group member) you want to remove from a group or subgroup in the **Organization** tree.

   Teamcenter displays the user's information.

2. Click **Remove**.

   The system displays the **Remove User Confirmation** dialog box.

3. Click **Yes** to remove the user from the group.

Activate a group member

1. Select the user (group member) you want to activate in a group or subgroup in the **Organization** tree.

   Teamcenter displays the user's information.

2. In the **Group Member Settings** section, select the **Active** option.

3. Click **Modify**.

Deactivate a group member

When a user leaves the organization or changes groups or roles within the organization, you can deactivate their membership within a group. This prevents them from logging on to the system as a member of the group and denies them access to information related to their previous group and role. Since a user can have multiple group member instances in a group, it is important to deactivate all of the user's group member instances within the group.

- Only an administrator or a user designated as a group administrator can change a group member's status from active to inactive.

  Database objects are owned by individual users; therefore, object ownership does not change when a group member is deactivated.

- You cannot deactivate a group member if they have any pending workflow tasks. You must first delegate these tasks to another group member and then deactivate the user. You can use the **global_transfer** utility to transfer one user's tasks to another user.

  You can also reassign the user's tasks from the My Teamcenter inbox.

- Before you deactivate users referenced in a workflow process assignment list, reassign their roles to another user with the **Replace Group Member** wizard.

1. Select the user (group member) you want to deactivate from a group or subgroup in the **Organization** tree.

   Teamcenter displays the user's information.

2. In the **Group Member Settings** section, select the **Inactive** option.

3. Click **Modify**.

Repeat this process for each user's group member instance you want to deactivate within the group or subgroup.

Suppress the display of inactive group members in the Organization tree

1. Expand the group in the **Organization** tree to display the roles and users within the group.

2. Click **Suppress Inactive Group Members/Show Inactive Group Members** .

   Teamcenter filters the display to suppress group members who have been designated as inactive within a group or groups.

> Note:
>
> This feature suppresses the display of active and inactive users who are designated as inactive group members. However, users can be designated as inactive but not be designated as inactive group members. In this case, the users are still displayed as group members when the **Suppress Inactive Group Member** filter is applied.

You can restore the display of inactive group members in the tree by clicking the button again.

Maintaining persons and users

Modify a person

As the real-world information associated with a Teamcenter user changes, it may be necessary to update the person definition.

1. Select the node of the person definition to be modified from the **Organization List** tree.

   The **Persons** pane displays the properties of the person definition.

2. Modify any information contained in the **Persons** pane boxes by typing over the existing information.

3. Click **Modify**.

The modified definition is saved in the database.

Delete a person

As your organization changes, it may become necessary to delete a person definition from the database.

Note:

Person definitions that are referenced by another organization object cannot be deleted. You must eliminate the reference before deleting.

1. Select the node of the person definition to be deleted from the **Persons** list in the **Organization List** tree.

   The **Persons** pane displays the properties of the person definition.

2. Click **Delete**.

   The **Delete Confirmation** dialog box appears.

3. Verify that the correct person is selected.

4. If the correct person appears, click **Yes**.

The **Persons** pane clears, and the person definition is deleted from the database.

Modify a user

You can modify user definitions from within the **Organization List** tree or the **Organization** tree. However, the assignment of group administrator privileges can only be performed by accessing the **Users** pane from the **Organization** tree.

1. Perform one of the following substeps:

   - Select a user definition from the **Organization List** tree.
   - Select a user definition from the **Organization** tree.

   The **Users** pane displays the user definition.

2. Modify any information contained in the **Users** pane by either typing over the existing information or selecting a different option from the defined lists.

   To remove entries in the **Citizenship** list, select the citizenship in the list to be removed and click the minus button −. To add additional citizenships to the list, enter the two-letter country code in the text and click the plus button + or select a country code from the country code list.

> Note:
>
> To select a different option from a defined list, you must first click **Clear** in the list dialog box and then select an item from the list.

3. Click **Modify**.

The changes to the user definition are saved in the database.

Deleting users

As your organization changes, it may become necessary to delete a user from the database. This is important because database objects are owned by users, and a determination must be made about what to do with any objects owned by the user before deleting the user from the database.

Siemens Digital Industries Software recommends that you first deactivate an obsolete user account in the database, then delete it when all references to the account have ceased.

Because the names of inactive users do not display in the LOVs throughout the rich client, inactive accounts cannot continue to be referenced by other users. Inactive user accounts cannot be logged on to the database, yet account records remain in the database so that an audit trail can continue to reference the data.

Once all references to objects owned by the deactivated account are cleared from the database, and an audit trail of the account's actions is no longer required, the account can safely and easily be deleted.

When you are ready to delete a user account, there are two options:

- Delete all objects owned by the user.
- Change ownership of all objects owned by the user. However, you cannot reassign objects owned by a replicated user.

> Note:
>
> If deleting all objects owned by the user, the delete procedure fails if any of these objects are referenced by another object. If this occurs, change ownership of the referenced objects to a different user.

Delete a user

1. Select the user definition to be deleted from the **Users** list in the **Organization List** tree.

   The **Users** pane displays the properties of the user definition.

2. Click **Delete**.

   The **Delete User** dialog box appears.

3. Confirm that the correct user definition is selected for deletion.

4. Perform one of the following substeps:

   - If deleting all database objects owned by the user, go to step 7.
   - If changing ownership of all database objects owned by the user, go to step 5.

5. Select the **Change Object Ownership** check box and click **New Objects Owner**.

   The **List of Values** list displays the users eligible to be the new owner.

6. Select a new object owner from the **New Objects Owner** list by double-clicking the name of the new owner on the **New Objects Owner** button.

7. Click **Delete**.

The user definition is permanently removed from the database.

Modifying user status

Changing user status

Siemens Digital Industries Software recommends that you first deactivate an obsolete user account in the Teamcenter database, then delete it when all references to the account cease.

Because the names of inactive users do not display in the list of values (LOVs) throughout the rich client, inactive accounts cannot continue to be referenced by other users. Inactive user accounts cannot be logged on to the database, yet account records remain in the database so that an audit trail can continue to reference the data.

An account can be deleted when all references to objects owned by the deactivated account are cleared from the database, and an audit trail of the account's actions is no longer required.

> Note:
>
> A replicated (remote) user is designated by having two green dots beside the user symbol to designate it as a remote object  . As an administrator, you cannot modify the associated data. However, you can remove remote users from your local organization structure.

Inactivate a user account

1. Perform one of the following substeps:

   - Select a user definition from the **Organization List** tree.
   - Select a user definition from the **Organization** tree.

   The **Users** pane displays the properties of the user definition.

   > Note:
   >
   > Because database objects are owned by users, you must decide what to do with any objects owned by the user being deactivated. You can either change ownership of these objects to another user or allow ownership to be retained by the inactive user.

2. Click **Inactive**.

   The **Change Ownership** button becomes available.

3. Perform one of the following substeps:

   - If you want to change the ownership of the user's database objects, go to step 4.
   - If you want ownership of the database objects to be retained by the inactive user, go to step 6.

4. Click **Change Ownership**.

5. Select a new owner for the database objects from the **List of Defined Users** list (double-click a user).

   The name of the new owner displays on the **Change Ownership** button.

6. Click **Modify**.

7. If the **Inactivate All Members** dialog box appears and you want to set the user's **Group Member Status** to **Inactive** for all groups that the user belongs to, click **Yes**. If you want to keep the user's **Group Member Status** set as they currently are for all groups, click **No**.

The user account is deactivated.

Activate a user account

1. Perform one of the following substeps:

- Select a user definition from the **Organization List** tree.
- Select a user definition from the **Organization** tree.

2. Click **Active**.
3. Click **Modify**.

The user account is activated.

7. Setup required by Content Management application

Defining languages

What is a language?

A *language* represents the vocabulary of a country or region. Languages are identified by a unique language name and store such attributes as the ISO language code and ISO country code. In Content Management, languages are associated with content that is translated into specific languages.

As a user with **DBA** privileges, you use the Organization application to:

- Create languages.
- Modify languages.
- Delete languages.

Create a language

1. Select the top-level **Language** node  from the **Organization List** tree.

   The **Language** pane appears.

2. In the **Language Name** box, type the name of the language.

   If you are creating a language for the DITA standard, use the allowed values, which are based on industry standards.

3. (Optional) Select the two-letter code for the language that corresponds to the ISO standard.

4. (Optional) Select the two-letter country code for the language that corresponds to the ISO standard.

5. Type the string appended to the XML unique ID at construction of rendition file names for documents in the **Language File Initials** box.

6. (Optional) Type descriptive text about the language in the **Language Description** box.

7. (Optional) In the **Default Publishing Font** box, type the default font for publishing content in the language to PDF; for example, **Helvetica**.

8. (Optional) In the **Fallback Language** box, select the translated language to be used for publishing if the selected language is not available.

   > Example:
   >
   > If the **Fallback Language** for English (U.K.) is set to English (U.S.), when you choose English (U.K.) when you publish a topic, and no English (U.K) translation is available, but an English (U.S.) translation is available, then the topic is published in English (U.S.).

9. (Optional) Type a description in the **Description** box.

   The following fields are related to the language selection:

   - To enable logon, select the **Login Enabled** check box.
   - To enable metadata, select the **Metadata Enabled** check box.
   - To enable content, select the **Content Enabled** check box.

10. Click **Create**.

Maintaining languages

Modify a language

1. From the **Organization List** tree, select the node of the language to modify.

   The **Language** pane displays the properties of the language definition.

2. Modify any information in the **Language** pane boxes by typing over existing information.

3. Click **Modify**.

   The system saves the changes to the language definition.

Delete a language

> Note:
>
> You cannot delete languages that are referenced by another object.

1. From the **Organization List** tree, select the node of the language to delete.

   The **Language** pane displays the properties of the language definition.

2. Verify that the correct language is selected.

3. Click **Delete**.

   The **Delete Confirmation** dialog box appears.

4. If the correct language appears, click **Yes**.

   The **Language** pane clears and the language is deleted from the database.

Defining graphic priority lists

What is a graphic priority list?

A *graphic priority list* is a list of graphic uses in a specific order, for example: **print**, **view**, and **thumbnail**.

Graphic priority lists are used in Content Management to manage *graphic items* and *graphic options*. A graphic item has no specific file type but serves as a generic parent placeholder for one or more graphic options. A graphic option is a graphic file of a specific type, such as a **.png** file. For example, a graphic item may be named **piston**, and it may have several child graphic options named **piston.eps**, **piston.jpg**, and **piston.png**.

When you import a graphic option to the database, you assign one or more uses to it, which defines the contexts in which the graphic is best suited. For example, the **piston.png** graphic option may have the **view** usage assigned to it.

In Content Management, when an editing or publishing tool editor opens an object that contains a graphic item, the tool uses a graphic priority list to select the appropriate graphic option.

As a user with **DBA** privileges, you use the Organization application to:

- Create graphic priority lists.
- Modify graphic priority lists.
- Delete graphic priority lists.

Create a graphic priority list

1. Select the top-level **Graphic Priority List** node  from the **Organization List** tree.

   The **Graphic Priority List** pane appears.

2. In the **Name** box, type a unique name for the graphic priority list.

3. (Optional) In the **Description** box, type a description for the graphic priority list.

4. For each use you want to add to the priority list, select a use from the **List of Defined Uses** list and either double-click it or click the plus button + to move it to the **List of Selected Uses** list. You can remove items from the **List of Selected Uses** list by double-clicking a use or selecting a use and clicking the minus button −.

   > Note:
   >
   > Keep the uses in the order in which you want them to be selected for a publish or view action.

If the graphic is used for this purpose	Select this graphic use
Icon in published output.	**ICON**
High-resolution graphic in printed output.	**PDF**
Graphic in a resolution appropriate for the printer where it will be printed.	**PRINT**
Small-scale image.	**THUMBNAIL**
Low-resolution image, typically for viewing only.	**VIEW**
Image to appear in a Web browser.	**WEB**

5. In the **Multiple Graphics Publish Max Options** box, do one of the following:

   - For standard publishing, type **1**.
   - To make the graphic option selection dependent on the stylesheet, type a value greater than 1, so that multiple copies of the graphic tag are added to the content during publishing.

     That number of graphic options are selected from the priority list. For example, if you type **3**, the first three graphics in the priority list are selected. This is used for specific cases, such as for dynamic HTML contents, where the graphic resolution changes when a mouse hovers over a graphic.

6. Click **Create**.

Maintaining graphic priority lists

Modify a graphic priority list

1. From the **Organization List** tree, select the node of the graphic priority list to modify.

The **Graphic Priority List** pane displays the properties of the graphic priority list.

2. Modify any information in the **Graphic Priority List** pane by typing over existing information.
3. Use the plus (+) or minus (−) buttons to arrange the uses in the list.
4. Click **Modify**.

Delete a graphic priority list

> Note:
> You cannot delete graphic priority lists that are referenced by another object.

1. From the **Organization List** tree, select the node of the graphic priority list to delete.

   The **Graphic Priority List** pane appears.
2. Verify that the correct graphic priority list is selected.
3. Click **Delete**.

   The **Delete Confirmation** dialog box appears.
4. If the correct graphic priority list displays, click **Yes**.

   The **Graphic Priority List** pane clears, and the graphic priority list is deleted from the database.