TEAMCENTER

Active Workspace Administration

Active Workspace 6.3

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

Logging

Assistant configuration

Subscription configuration

Administration from Active Workspace

Using Active Workspace, you can perform routine tasks to:

- Monitor your site and keep it running efficiently
- Provide an environment in which your users perform their tasks quickly.

Where do I go from here?

 Teamcenter Administrator	
Learn about administration tools available in Active Workspace	**Active Admin workspace**
Control user access to data	**Manage which data your users see**
Share data	**Share data with external locations**
Monitor system logging	**Configure and view log files**
Manage your site's settings and performance	**Manage system settings and performance**

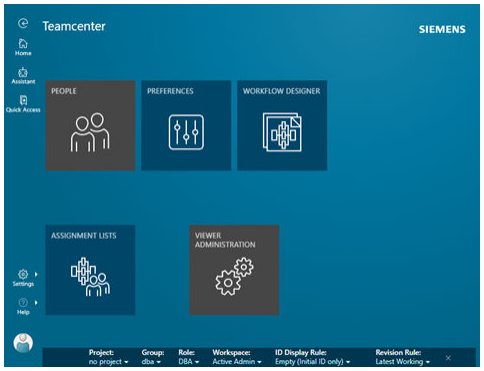
1. Active Admin

The Active Admin workspace

What is the Active Admin workspace?

This workspace is an *exclusive* workspace designed for Active Workspace administrators. Since it is exclusive, there are a limited set of pages and commands that the administrator is allowed to visit. For example, there is no access to initiate a workflow, change management, scheduling, or other end-user functionality.

The workspace provides quick access to the most common administrative functions on the home page tiles.



How do I enable it?

Use Deployment Center or the Teamcenter Environment Manager to install it.

During installation, the workspace definition file, **workspace_TcActiveAdminWorkspace.json**, is added to the **STAGE***src**solution* directory of your Active Workspace development environment, and the workspace is mapped to the dba group.

What applications does it contain?

See the workspace definition file for a complete list of available pages and commands. The following applications are displayed in the **Active Admin** workspace home page by default:

- **People**

  Manage your organization. Create and modify groups, roles, and users. Remove roles and users.

> Note:
>
> You must use the Teamcenter rich client to remove or delete a group or subgroup from the parent group, as this capability is not available using the Active Workspace client.

- **Preferences**

  Manage your Teamcenter preferences from within Active Workspace.

- **Access Manager**

  Control user access to data objects by defining rules and defining access control lists (ACLs).

- Workflow Designer

  Use a graphical editor to view and design workflows and task templates.

- Assignment Lists

  Prepare lists of groups or roles to assist your users when they assign users to workflows.

- Viewer administration

  Help troubleshoot your active visualization installation.

2. Localization configuration

Localization configuration tasks

What is localization?

Localization is the presentation of an application's text in the local language. You can install Active Workspace to be displayed in many different languages.

Why configure localization?

After installing Active Workspace to run on a localized Teamcenter server, additional setup may be required to present text in the local language.

What can I configure?

You can configure the following aspects of localization:

- Configure Active Workspace for additional locales.
- Configure locales for visualization servers.

What do I need to do before configuring?

Before you can configure localization, you must ensure that the server-side of Teamcenter is configured for the locales you want.

Where can I find out more about localization?

See *Localization* in the Teamcenter help.

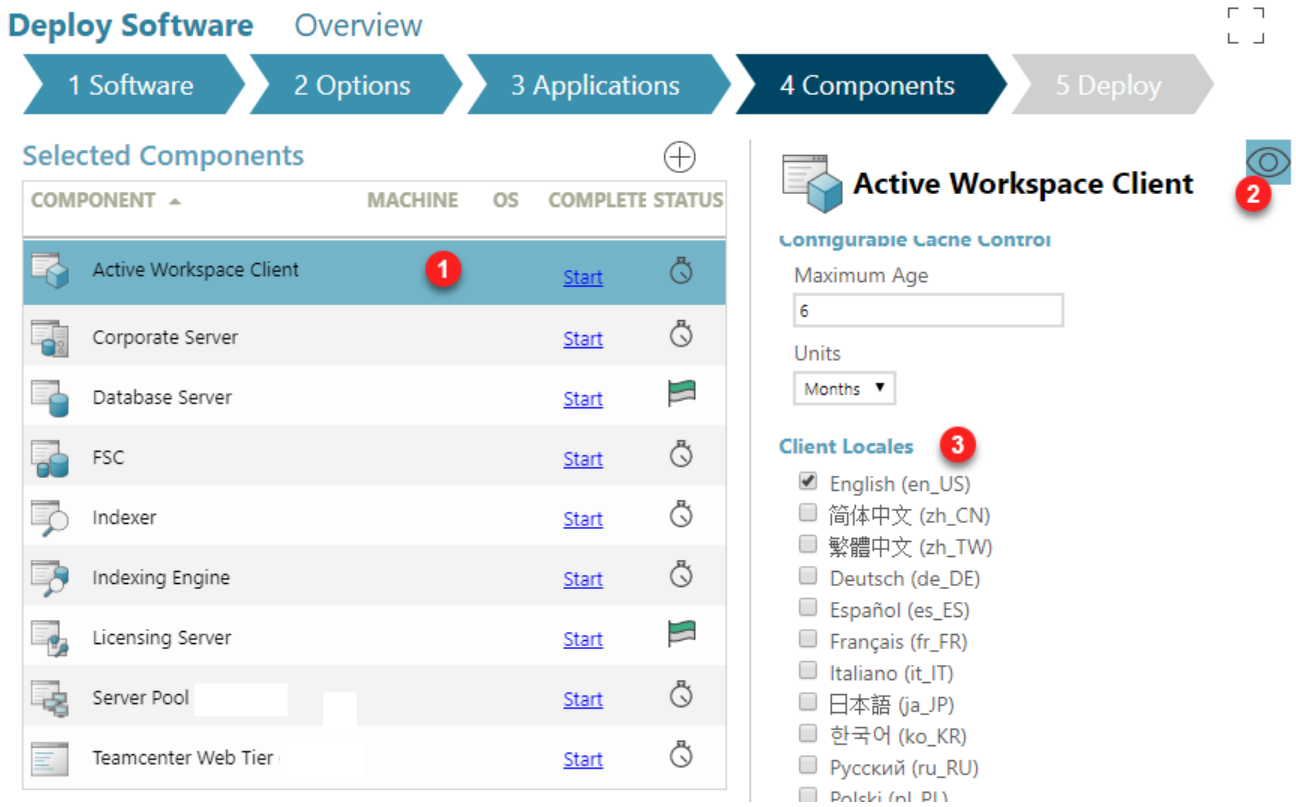
Configuring Active Workspace for other locales

You can configure Active Workspace to support various languages in addition to English. Use the Deployment Center or the Teamcenter Environment Manager to manage your available locales.

> Tip:
>
> When creating custom content, the parenthetical value is post-fixed to the JSON file name in the **i18n** folder of your custom module.

Deployment Center

The list of available locales is not a required parameter in the Deployment Center, so you must show all parameters when choosing locales.

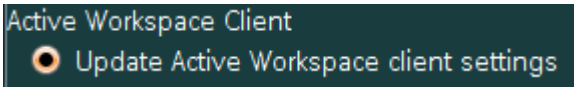


Your list of components may differ.

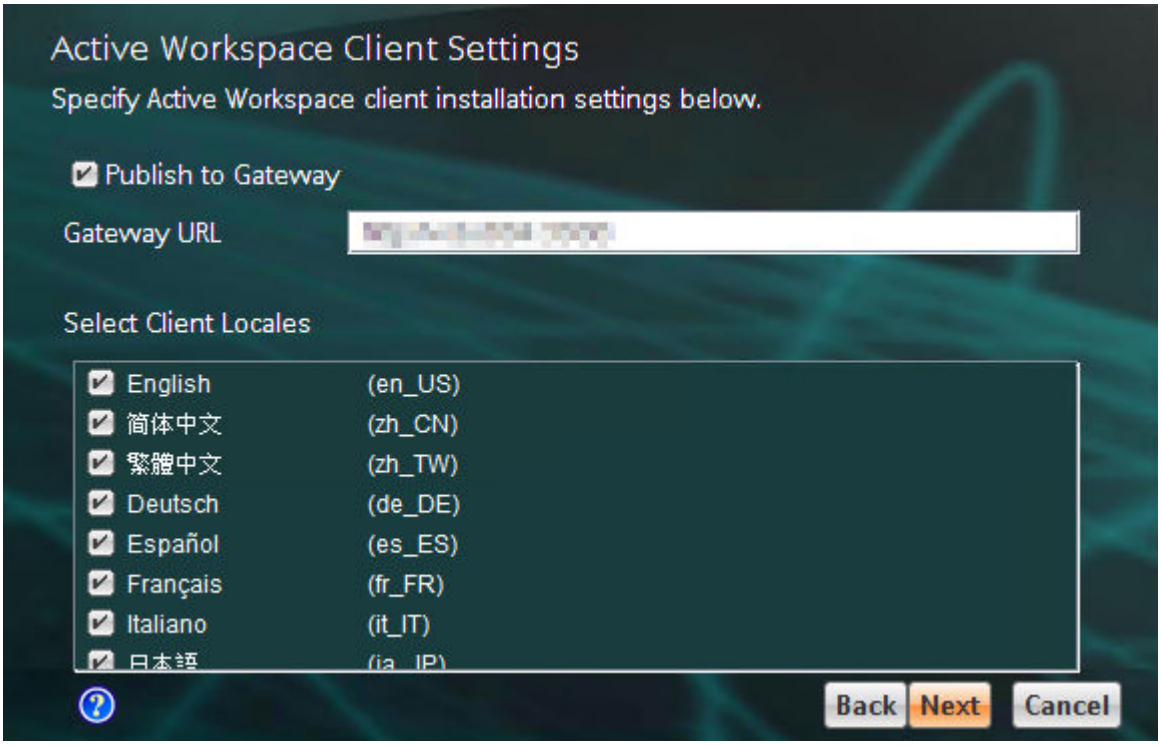
1. Select the **Active Workspace Client** component.
2. Select **Show all parameters**.
3. Choose your additional **Client Locales**.

Teamcenter Environment Manager

The list of available locales is found when you **Update Active Workspace client settings**.

1. 

2.



Locale support by Visualization Server Manager

You can configure the Active Workspace client to display the user interface in any of the supported Teamcenter locales. However, some visualization data, such as Product and Manufacturing Information (PMI), requires a Visualization Server Manager (VSM) configured for the same locale as the information. For visualization data to display correctly in the Active Workspace client, you must have at least one VSM configured to run in each locale for which you have data. With this system in place, visualization processes are then routed to the appropriate server based on locale.

VSMs can be configured to support the following languages:

Brazilian Portuguese	English	Korean
Chinese (Simplified)	French	Polish
Chinese (Traditional)	German	Spanish
Czech	Italian	Russian
French	Japanese	

You can configure a VSM with any one of these languages. If you want to configure a cluster of VSMs to support more than one language, you need at least one VSM per language.

To change the language of a VSM, set Windows to the required language, location, and locale. You can adjust these settings using the Region and Language options found in the Windows Control Panel. You must adjust the **Date and time formats**, the **Current location**, and the **Current language for non-Unicode programs** values. After changing your Windows settings, reboot the system. When the VSM is started again, it inherits the new language configuration of the operating system.

If all VSMs are configured to use the same language, all clients use the available language regardless of browser preferences.

Note:

If you have a VSM system configured for two or more different languages, then Siemens Digital Industries Software highly recommends that at least one VSM be configured for English, even though this may require a minimum of three VSMs.

When the server system is configured with multiple languages, if at least one VSM is configured for English, then the English locale is a default.

The following table shows the VSM system response to a visualization data request from client when the client is not in one of the pre-configured languages.

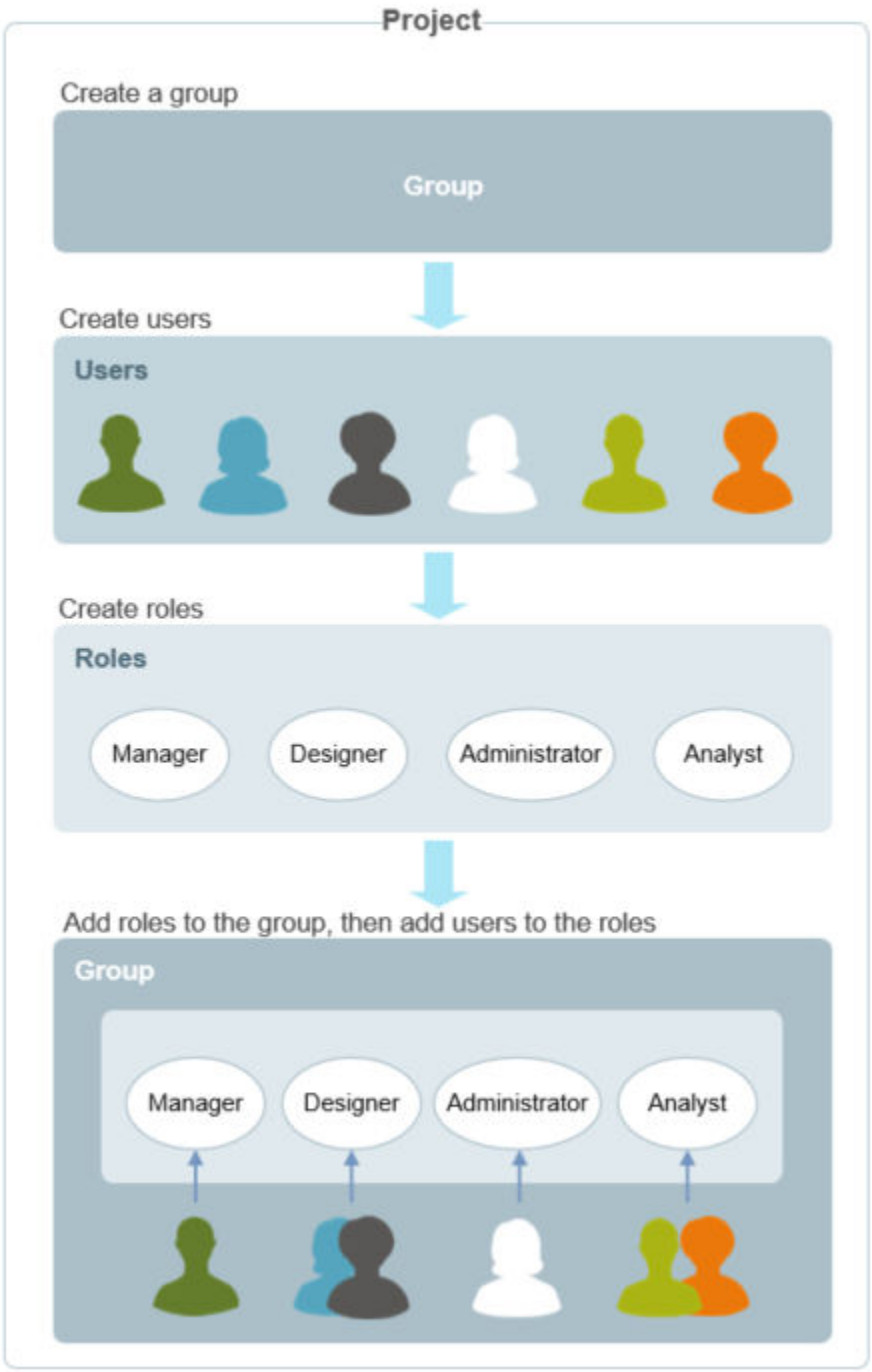
VSM system configured for two or more languages	**Client is not in a pre-configured VSM language**
VSM for English exists	The data request is routed to an English VSM.
No VSM for English	The data request is rejected.

3. Control data access

Creating the organizational structure

By setting up user management you can control the functionality that is available to users who are mapped to a specific role, thereby controlling the access to restricted data. To do this, you can create groups for specific projects, and add users, or roles assigned as team members to the projects.

> Example:
>
> You want to set up the organizational structure for a project that requires an administrator, a project manager, two designers, and two analysts. You first create a project and add a group to the project. You then identify the users or create new users that you require for your project. Next, you search for existing roles or create new roles required for the project. You then add the roles to the group, and add users to the respective roles in the group.



Managing users, groups, and roles

What are groups, roles, and users?

Groups

In Active Workspace, the term *group* refers to a cluster of *users* who take on a *role* or multiple roles in a group. Groups can be created to represent data ownership and to control data access.

Projects are created with specific groups, users, or roles assigned as team members, privileged team members, and team administrators.

Typically, groups are defined along project lines and not functional lines. However, you can also create groups of third-party organizations such as suppliers.

A group member can be a member of multiple groups. Groups make up the core of the organization structure.

As an administrator, you can:

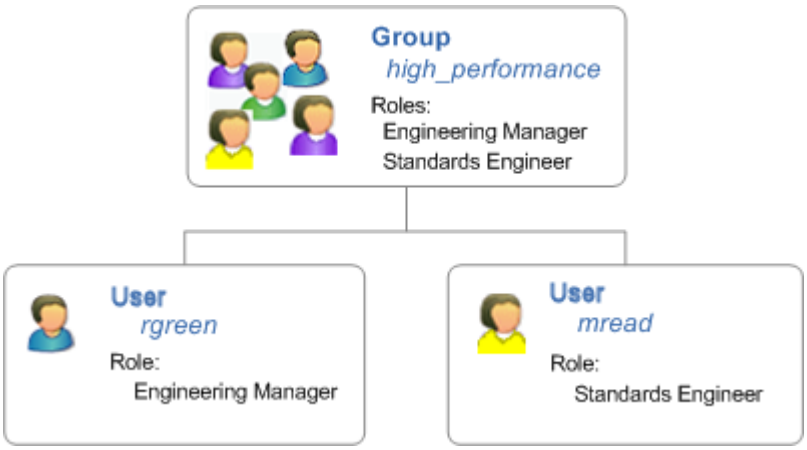
- **Create** and **modify** groups.

  Note:

  You must use the Teamcenter rich client to remove or delete a group or subgroup from the parent group, as this capability is not available using the Active Workspace client.

  Example:

  The **high_performance** group consists of 2 roles, that is, **Engineering Manager** and **Standards Engineer**, and 2 users, namely, **rgreen** and **mread**, who are assigned their respective roles.



- Assign authorized data access privileges to a group.
- Assign default volumes to a group.

  A *volume* is a location where files are stored. A volume corresponds to a directory on the operating system. Files stored in volumes are created by CAD applications or other third-party applications. You can assign volumes to groups and define file locations for your organization structure.

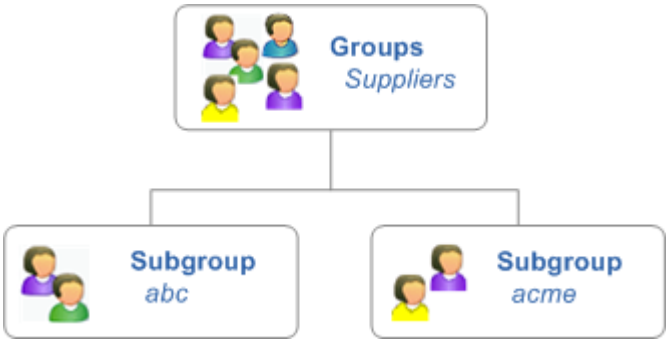
- Manage subgroups within the organization.

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

  Subgroups can be used to organize users. Subgroups inherit access permissions, volumes, and preferences from their parent.

  Example:

  Consider a scenario where you wish to restrict contractors from viewing any content in the employee group. In this case, you can create subgroups **abc** and **acme** within a group such that users from these subgroups will not have access to the content from any groups other than their own.



Roles

A *role* defines the type of work a user is expected to perform in a group. Roles refine the group definitions of your organization structure.

- A role can be assigned to multiple groups.
- Roles add an additional layer of data access control.
- Roles are created along functional lines.

  Tip:

  While creating roles, use real-world descriptions, skills, and responsibilities.

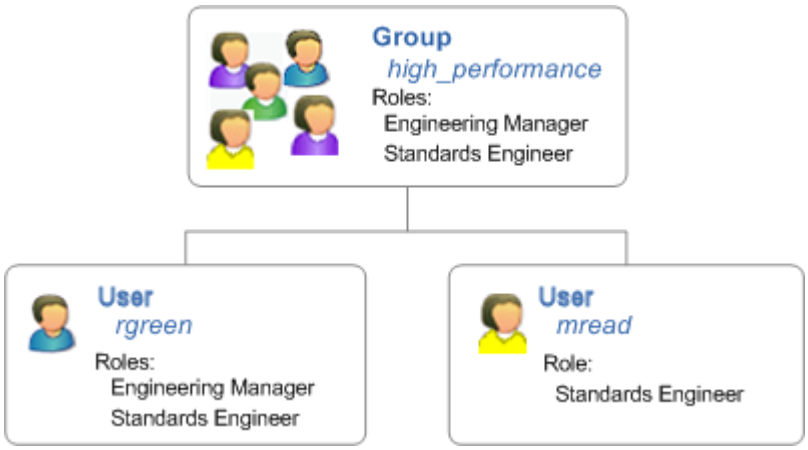
As an administrator, you can:

- **Create**, **modify**, and **delete** role definitions.
- **Add new or existing roles to groups**.

- Assign a default role within a group.

Example:

Robert Green, a user, is assigned the default role of **Engineering Manager**. In addition to his responsibilities as engineering manager, Robert must also perform standards-related work. Therefore, user **rgreen** is assigned two roles in the **high_performance** group: **Engineering Manager** and **Standards Engineer**.



Users

Users are individuals who interact with Active Workspace. A user is assigned to a default group and takes on a role in the group.

As an administrator, you can:

- **Create**, **modify**, **deactivate** user accounts, or **delete users from groups**.
- **Reset user passwords**.
- Assign license bundles, and license servers to a user.

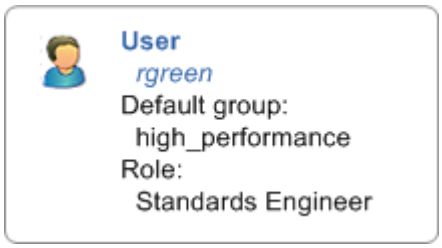
  When you assign a license bundle to a specific user, the user assigned to the bundle is assured the availability of all the features in the bundle. You can use license bundling in conjunction with other licensing schemes. Consider a scenario where a user is assigned a license bundle that does not include the Systems Engineering module. When the user launches Systems Engineering, the system confirms if the feature key exists in the license file outside of the license bundle. If the feature key is found, the application can be used.

  A *license server* is a process dedicated to tracking license usage by users. It runs on a host machine and port specified by an administrator. An administrator can set up multiple license servers. Each license server can have a different set of users assigned to it. This allows the load balancing of license requests so that a single license server is not overused.

Users can be assigned various roles in the organization. A user can also be part of multiple groups in the organization.

Example:

Robert Green, a user, is assigned the default role of **Standards Engineer** and belongs to the default group **high_performance**.



How to manage groups, roles, and users in Active Workspace

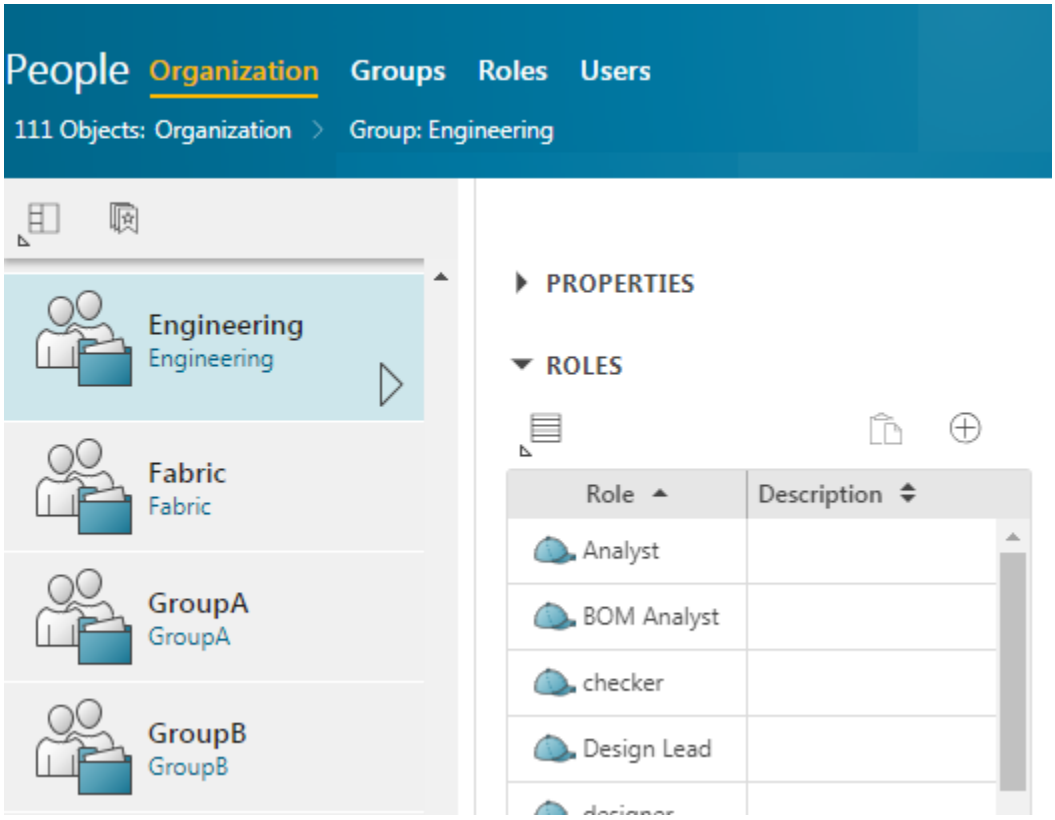
In Active Workspace, you can use the **PEOPLE** tile to create and modify users, roles, and groups and to set up authorized access using login credentials for each user.

Note:

The **PEOPLE** tile is visible in both the **Active Admin** and **Default** workspaces. It *may* be visible in the **General User** workspace.

You can create your own workspace mapped to a special group of non-**dba** group users and add the **PEOPLE** tile to it. This allows users to perform admin work because privileges for **dba** group users are too broad.

As a database administrator, you can create users and user roles specific to your organization. You can then add the users and roles to a specific group to grant them authorized access to the application.



Creating groups, roles, and users

Create a group

1. In the **Groups** tab, click **New** > **Add** ⊕.
2. In the **Add** panel, specify values for the following:
   - **Name**
   - (Optional) **Description**
   - (Optional) **Security**
   - (Optional) **To Parent**

     To create a subgroup for an existing group, select the parent group from the list.
   - (Optional) **DBA Privilege**
   - (Optional) **Default Volume**

- (Optional) **Default Local Volume**

3. Click **Add**.

> Note:
>
> You can also create groups in the **Organization** tab. To do so, in the **Organization** tab, click **New** > **Add**, and follow similar steps to a create a group.

Create a role

1. In the **Roles** tab, click **New** > **Add**.
2. In the **Add** panel, specify values for the **Role** and, optionally, a **Description**.
3. Click **Add**.

Create a user

1. In the **Users** tab, click **New** > **Add**.
2. In the **Add** panel, in **NEW**, enter the following:
   - **Name**
   - **User ID**
   - **OS Name**
   - **Default Group**
   - (Optional) **Default Volume**
   - (Optional) **Default Local Volume**
   - **Status**

     > Note:
     >
     > To create an active user, set **Status** = **0**.

   - **License Level**

> Note:
>
> The types of licenses available depends on your license agreement. For descriptions of the available license levels, see your license agreement documentation.

- (Optional) **License Server**
- (Optional) **License Bundle**
- **Visualization Licensing Level**

  0 (Base)

  1 (Standard)

  2 (Professional)

  3 (Mockup)
- (Optional) **Geography**
- (Optional) **Nationality**
- (Optional) **Citizenships**

In **PERSONAL INFORMATION**, specify the following optional fields:

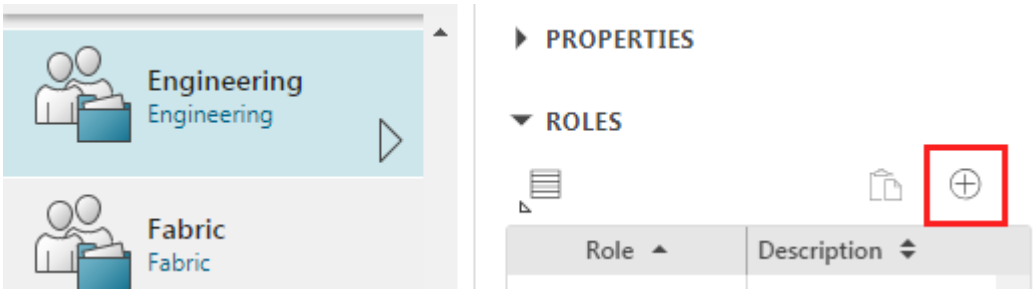
- **Address**
- **City**
- **State**
- **Zip Code**
- **Country**
- **Organization**
- **Employee Number**
- **Internal Mail Code**
- **E-Mail Address**

- **Phone Number**
- **Locale**
- **Time Zone**

3. Click **Add**.

Add roles and users to groups

1. In the **Organization** tab, select the group to which you want to add users.
2. In **ROLES**, click **Add Role** ⊕.



3. In the **Add** panel, do one of the following:
   - In the **New** tab, enter a role and description for the new role.
   - In the **Search** tab, enter the name of an existing role, and select the required role from the search results.
4. Click **Add**.
5. To add users in a group, select the group and click **Navigate**.

6. Select the role to which you want to add users.
7. In **USERS**, click **Add** ⊕.

8. In the **Add** panel, do one of the following:

   - In **New**, enter a name and description for a new user.
   - In **Search**, enter the name of an existing user and select the required user from the search results.

9. Click **Add**.

> Tip:
>
> If you add a role to a group, but do not assign any users to that role, it will not appear in the **Organization** tree.

Managing users

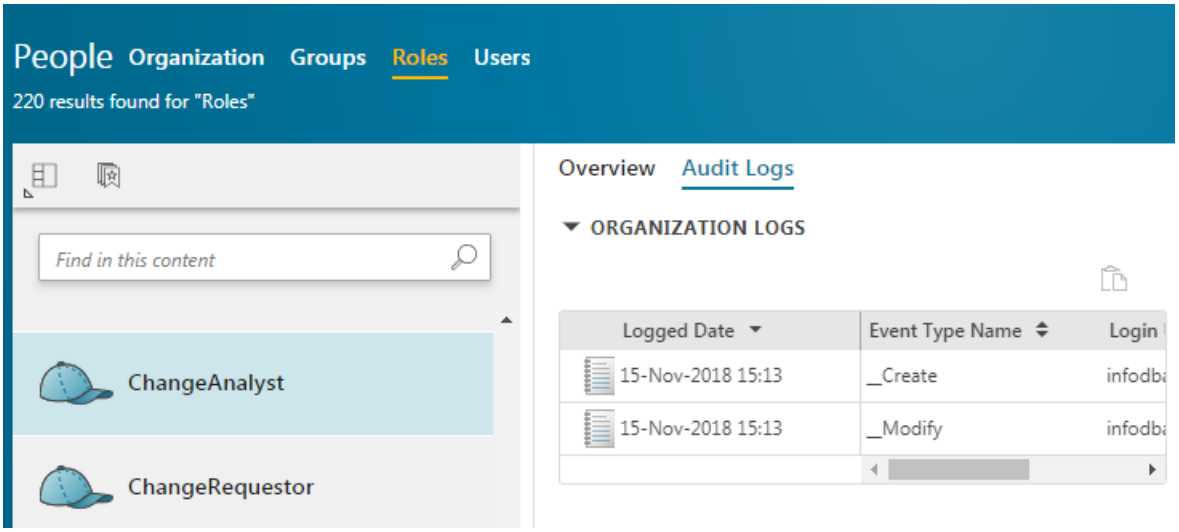
Edit user information

1. Navigate to the **Users** tab and search for an existing user.
2. Select the user.
3. Click **Edit** > **Start Edit**.
4. Modify the user information and click **Edit** > **Save Edits**.

View user activity logs

1. In the **Roles** tab, select the role for which you want to view the user activity logs.
2. Click the **Audit Logs** tab.

   A table that shows the **Logged Date**, the **Event Type Name**, and the **Login User ID** is displayed under **ORGANIZATION LOGS**.



Adding the Access tab to view user access rights

What is the Access tab?

The **Access** tab enables you to view access rights on objects in Active Workspace. As an administrator, it helps you determine if the correct access privileges have been assigned to the selected user. If a user is assigned multiple groups and roles, you can determine access for that user by selecting a particular group/role combination and clicking **Show Access Rights**.

The **Access** tab contains three sections:

- **User, group, and role filters**

  Filters the user, group, and role for the current user session context.

  You can use these filters to select another user, group, and role combination for which you want to view the associated access rights for the currently selected object. Click **Show Access Rights** to apply these changes.

- **ACCESS RIGHTS**

  Lists the operations and privileges granted to the filtered combination of user, group, and role.

- **ASSOCIATED RULES**

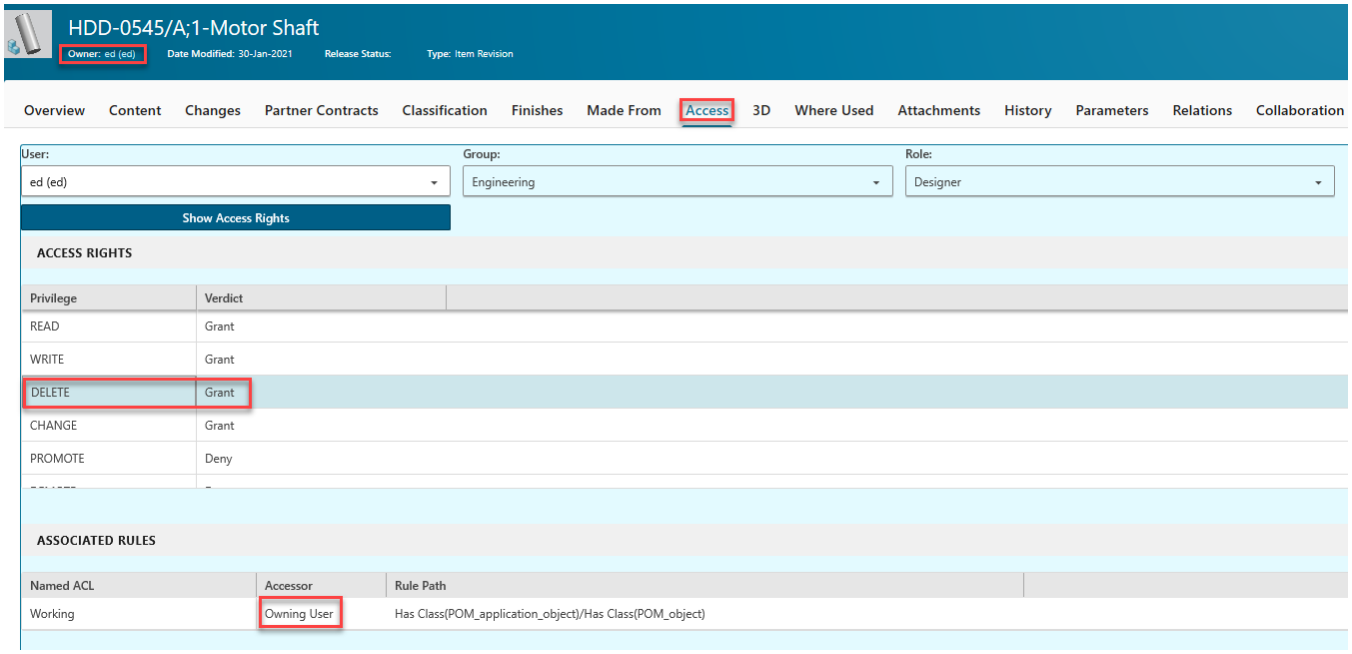
  Lists the rules associated with the given object.

Note:

By default, the **Access** tab is not available. To add the **Access** tab, **edit the style sheet registered to the summary view** for the object type to which you wish to add the **Access** tab.

Example:

Ed, a designer in the engineering group, designed the **Motor Shaft** object. His access rights are shown in the **ACCESS RIGHTS** section. As indicated in the **ASSOCIATED RULES** section, Ed is granted **DELETE** access rights because he is the **Owning User**.



How do I add an Access tab?

1. Open the style sheet registered to the summary view for the type of object to which you wish to add the **Access** tab:

   - **Item revision**

     The default summary style sheet is **Awp0ItemRevSummary**.

   - **Document revision**

     The default summary style sheet is **Awp0IDocumentRevSummary**.

   - **Requirements revision**

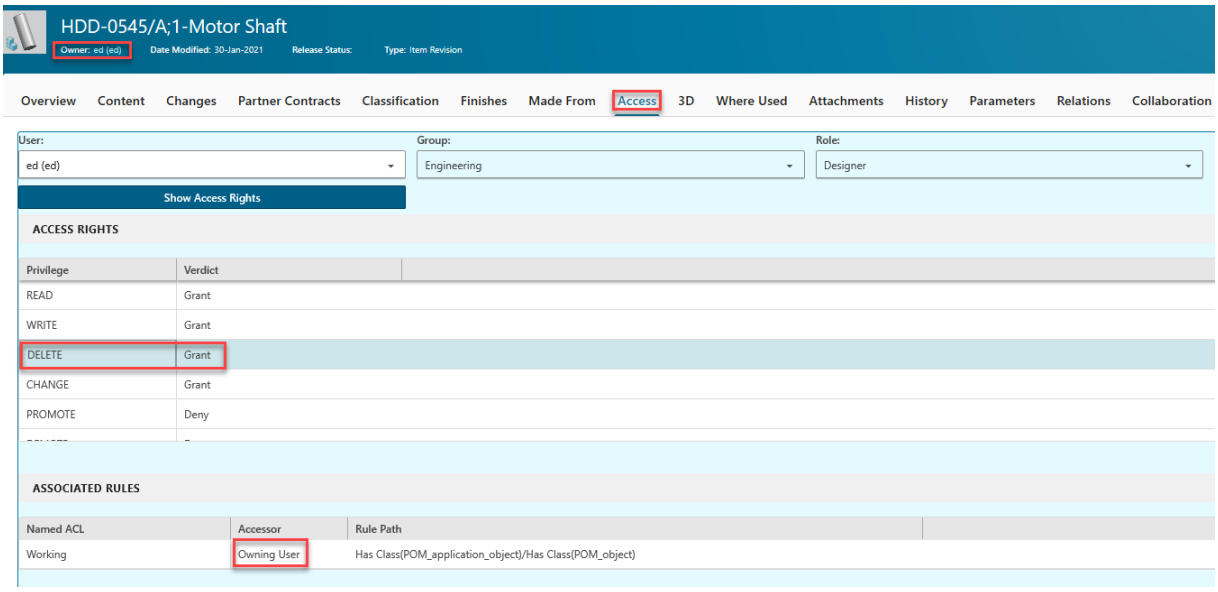
     The default summary style sheet is **Awp0RequirementRevisionSummary**.

2. Add the following line to the appropriate style sheet.

<inject type="dataset" src="Aut0ItemRevSummary" />

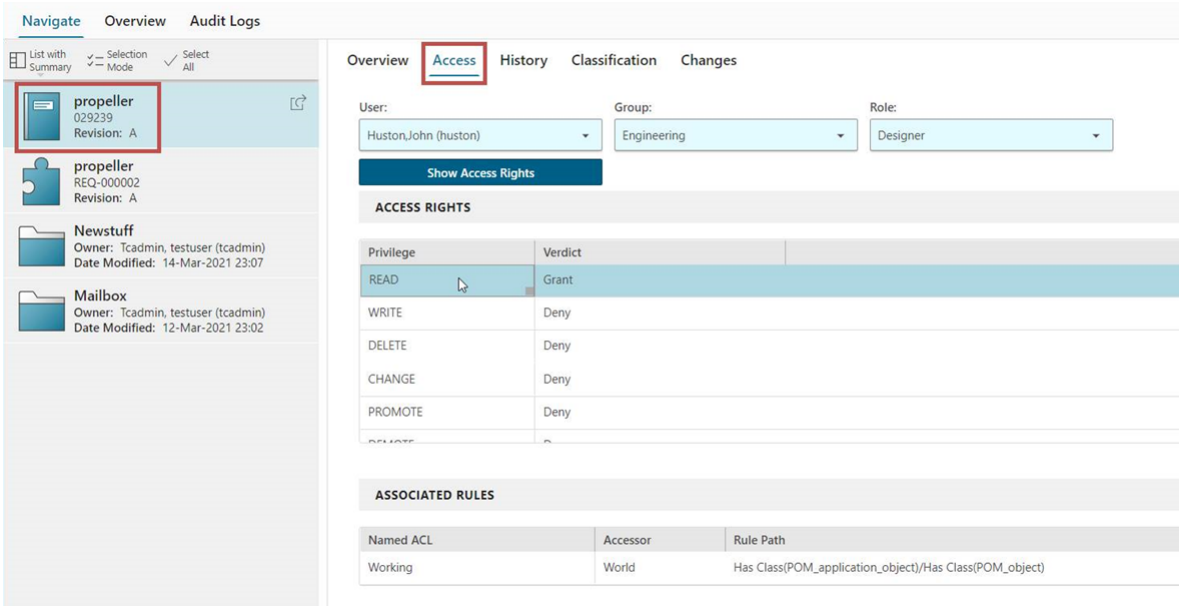
a. For an *item revision*, add the line here in the **Awp0ItemRevSummary** style sheet:

<inject type="dataset" src="Fsh1FinishesSection"/>
<inject type="dataset" src="Ads1NotesSection"/>
<inject type="dataset" src="Vm1PartnerContracts"/>
<inject type="preference" src="ClassificationStylesheetTab"/>
<inject type="dataset" src="Sm1MadeFromSection"/>
<inject type="dataset" src="Aut0ItemRevSummary"/>



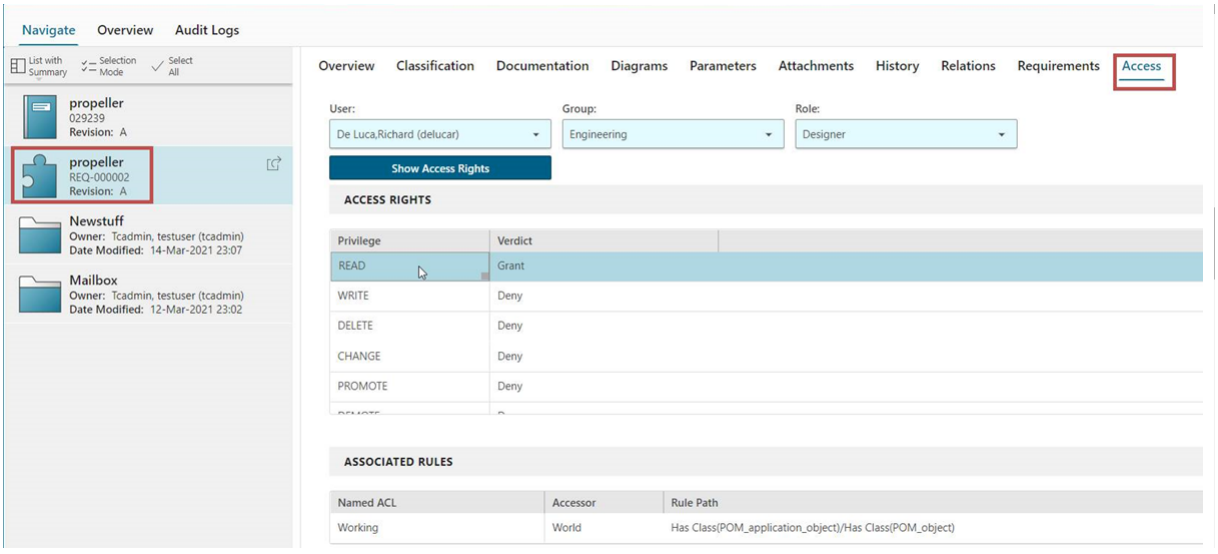
b. For a *document revision*, add the line here in the **Awp0IDocumentRevSummary** style sheet:

<inject type="dataset" src="Fnd0ClassificationSummary"/>
<inject type="dataset" src="ProjectListInfo"/>
<inject type="dataset" src="Aut0ItemRevSummary"/>



c. For a *requirements revision*, add the line here in the **Awp0RequirementRevisionSummary** style sheet:

```
<inject type="dataset" src="WorkflowSummary"/>
<inject type="dataset" src="RelationsSummary"/>
<inject type="dataset" src="Ase0SystemRequirementsSubLocation"/>
<inject type="dataset" src="Aut0ItemRevSummary"/>
```



Add or change a user password

1. In the **Users** tab, select the user whose password you want to add or change.

2. Click **Manage** > **Change Password**.

3. In the **Change Password** panel, enter a password in the **New Password** box.

4. Retype the same password in the **Confirm New Password** box.

5. Click **Change**.

Deactivate users

You can deactivate a specific user ID by modifying the status of the user. This user is retained in the database and can be activated for future use.

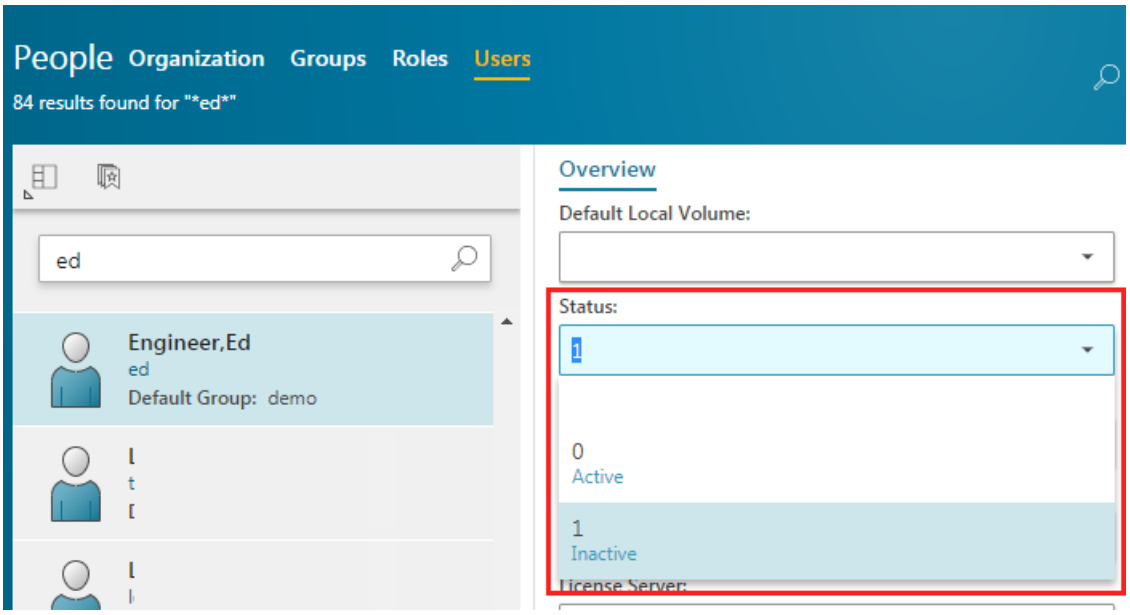
> Example:
>
> Consider a designer who will be going on an extended leave of absence. Instead of deleting the user from the project group, you can temporarily deactivate the user. Once the user is available, you can set the status to active.

1. In the **Users** tab, search for the user whose status you want to modify.

2. Click **Edit** > **Start Edit** .

3. Set the **Status** field of the user to **1 Inactive**.

4. Click **Edit** > **Save Edits** .



Delete a user from a group

1. In the **Organization** tab, search for the group from which you want to delete a user.

2. Click the group to view a summary of the roles and users that are included in the group.
3. In **ROLES**, select the row that displays the user that you want to delete.
4. Click **Remove**.

   The selected user is deleted from the group.

Managing roles

Edit a role

1. Navigate to the **Roles** tab and search for an existing role.

   In the **Roles** tab, search for and open the role that you want to modify.
2. Click **Open**.
3. Click **Edit** > **Start Edit**.
4. Modify the role name and description and click **Edit** > **Save Edits**.

Delete a role

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

1. In the **Organization** tab, search for the group from which you want to delete a role.
2. Click the group to view a summary of the roles that are included in the group.
3. In **ROLES**, select the row that displays the role that you want to delete.
4. Click **Edit** > **Remove**.

Managing projects

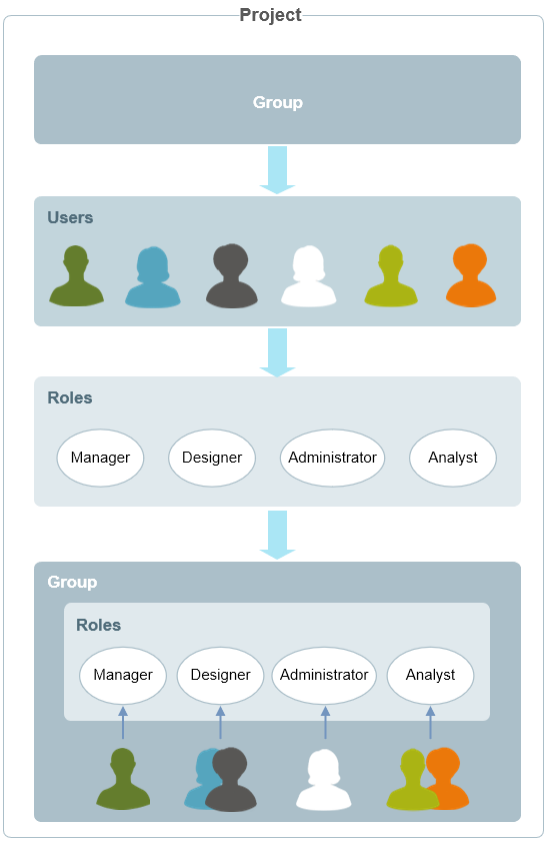
What are projects?

In the Teamcenter rich client, the Project application provides a means to group data and users from different groups, such as Engineering, Supplier, and Customers, and allow configuration of access rules based on this grouping. This is an easy way to organize your data and implement the access control based on a business project or program's security requirements.

Using the Active Workspace client, you can use the **PROJECTS** tile to create projects and programs and manage your project teams by correlating groups of users, potentially at different physical sites, with your product data. However, you must use the rich client to delete projects.

Example of a typical project

A project comprises a group of users each having one or more roles. For example, this project consists of an administrator, a project manager, two designers, and two analysts.



Control access to your project data

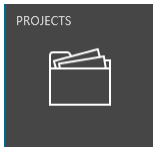
There are several measures you can use to control access to your project data:

- When *creating* a project, you can use the **Project Category** field, which allows you to restrict a user's access to objects based on the category of the project. For example, a user assigned to the **Supplier** project category would be unable to view proprietary information. The default project categories are **Internal**, **Partner**, and **Supplier**.

- Designating team members as *privileged* is one step in the process of granting access to users to allow them to assign data to and remove data from projects and programs.

Understanding project team roles

In Active Workspace, as Project Administrator or Team Administrator, you use the **PROJECTS** tile to manage your project teams. For example, you can add groups, roles, and users to your project by selecting them from your organization.



Depending on your role, you can perform the following project-related tasks in Active Workspace:

Team role	Definition
Project Administrator	Teamcenter user with privileges to administer project teams in Active Workspace. Users in the **Project Administrator** role can: • Modify the properties on the project. • Add and remove team members to projects in which the project administrator is also a member. • Assign **Privileged**, **Non-privileged**, and **Team Administrator** status to any project team member. Note: You can designate multiple team administrators for each project. This is often necessary to balance resource management tasks for large projects.
Team Administrator	Project team member with privileges to add and remove project members. Users in the **Team Administrator** role can: • Add and remove team members to projects in which the team administrator is also a member. • Assign **Privileged**, **Non-privileged**, and **Team Administrator** status to any project team member.

Team role	Definition
	Note: You can designate multiple team administrators for each project. This is often necessary to balance resource management tasks for large projects.
Privileged team members	Project team members with privileges can view their projects and their team members. They can also assign or remove objects to or from their projects.
Non-privileged team members	Project team members without privileges can view their projects and their team members.

Manage project teams

As an administrator of a project team, you can select a project and view your team members. In addition, you can add and remove users, roles, and groups.

Select a project and view your team members

1. As **Project Administrator** or **Team Administrator**, select a project to display the **TEAM MEMBERS** section.

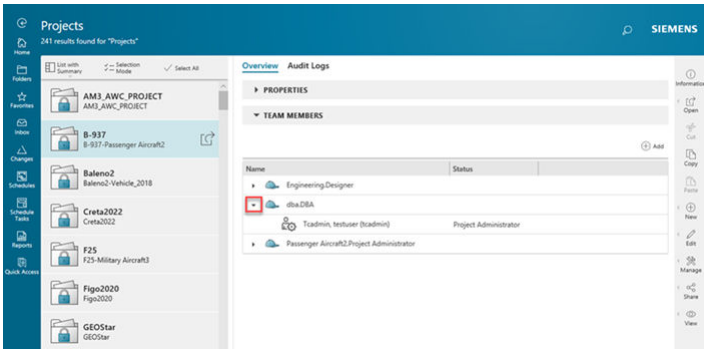
   A team member can have one of four types of status:

   - **Project Administrator**
   - **Team Administrator**
   - **Privileged**
   - **Non-privileged**

2. To view your project's team members, click **Show Children** (**>**).

   Example:

   In this example, when you expand the role, you see the user whose status on the project is **Project Administrator**.



Add a user to a project

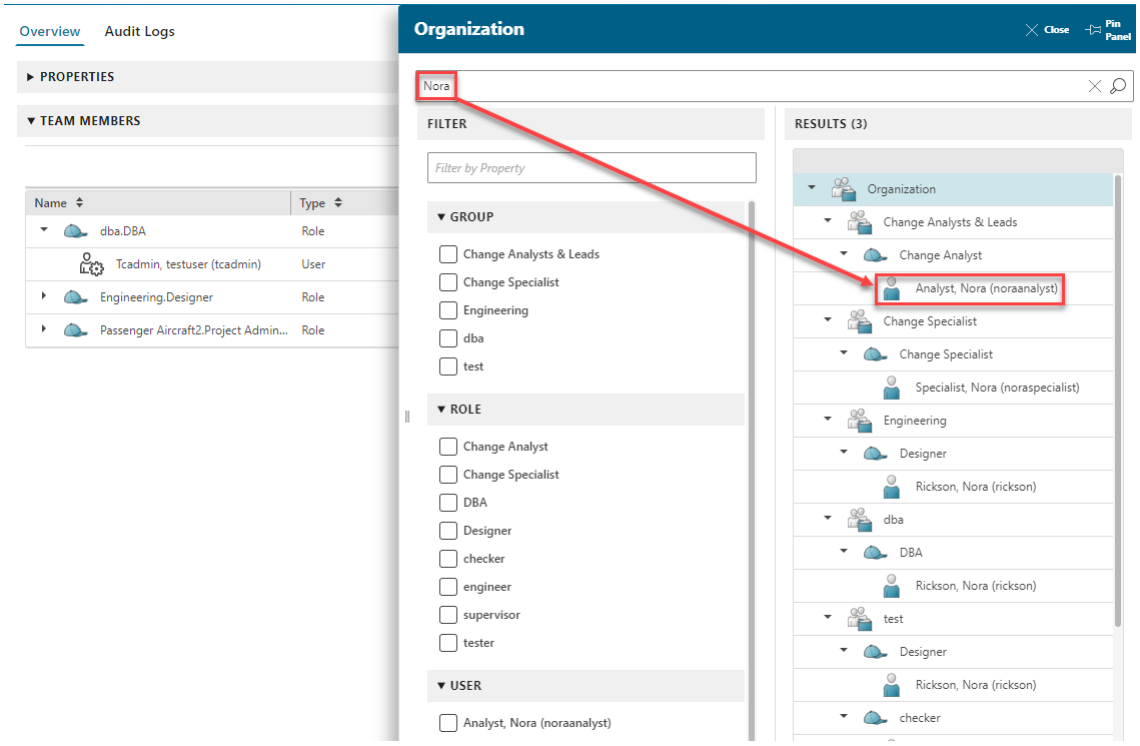
1. Log on as **Project Administrator** or **Team Administrator**.
2. From the **TEAM MEMBERS** section, click **Add** ⊕ to open **Organization** to search for a user
3. Select the user, and click **Add** to add the selected user to your project team.

Note:

To remove a user from the project, select the user and click **Remove** ⊖.

Example:

From **Organization**, filter on **Nora**. Then, select Nora and click **Add**.

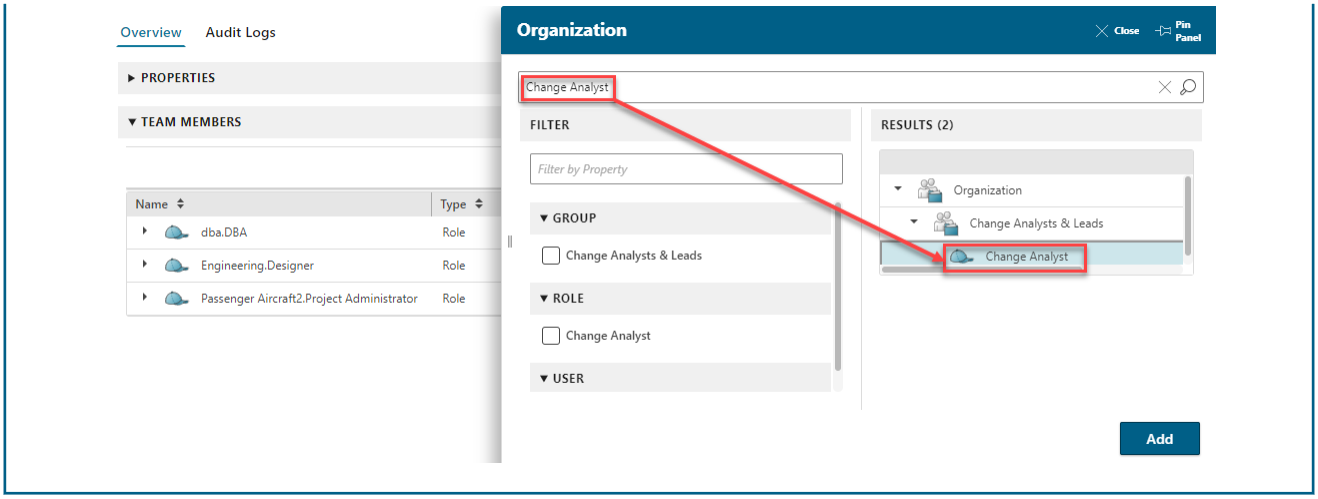


Add a role to a project

1. Log on as **Project Administrator** or **Team Administrator**.
2. From the **TEAM MEMBERS** section, click **Add** ⊕ to open **Organization** to search for a role.
3. Select the role, and click **Add** to add the selected role to your project team.

Example:

From **Organization**, filter on **Change Analyst**. Then, select the role and click **Add**.



Add a group to a project

1. Log on as **Project Administrator** or **Team Administrator**.
2. From the **TEAM MEMBERS** section, click **Add** ⊕ to open **Organization** to search for a group.
3. Select the group, and click **Add**.

As a **Project Administrator** or a **Team Administrator**, from **TEAM MEMBERS**, click **Add** ⊕ to open **Organization** to search for a group, select the group, and click **Add** to add the selected group to your project team.

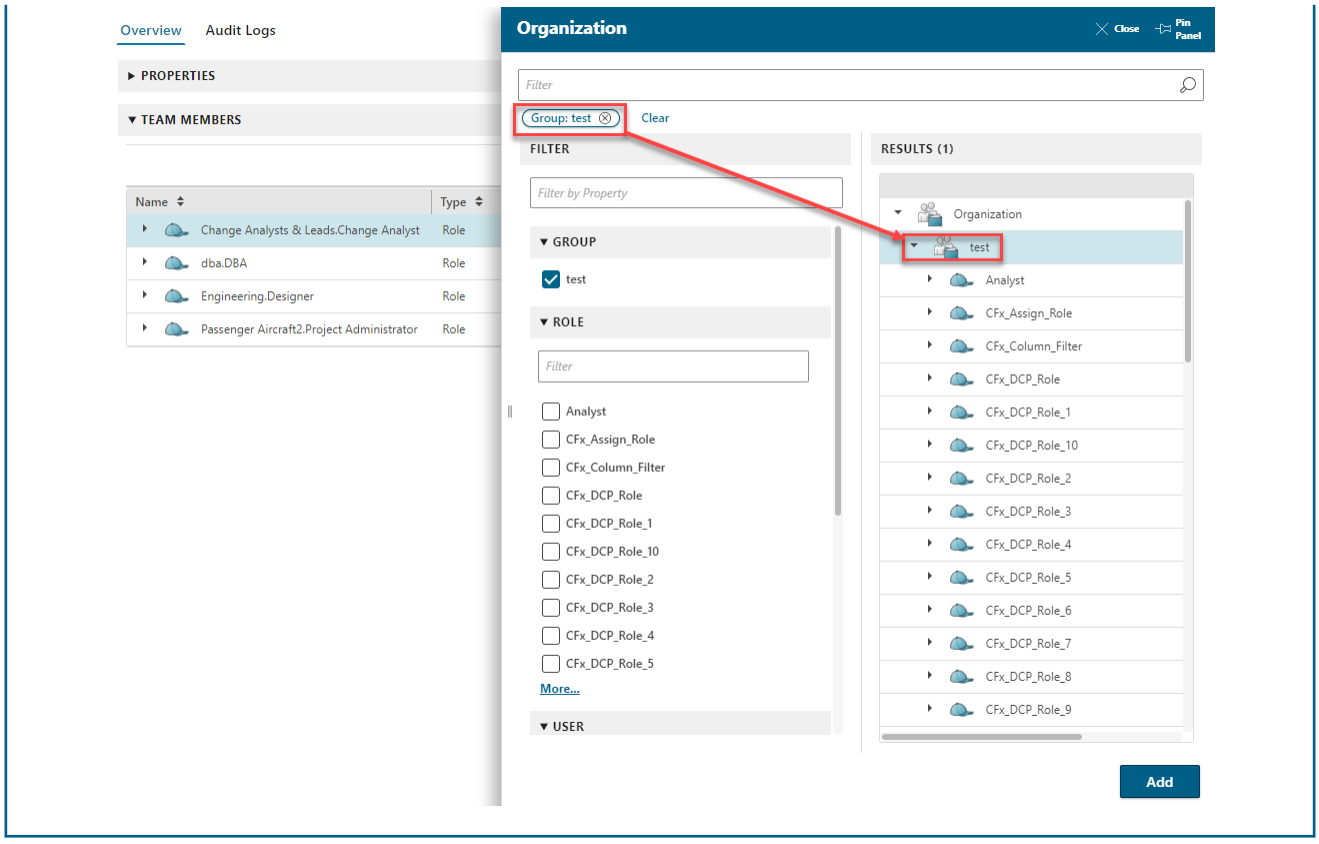
Note:

You cannot remove a role or a user from the group. You can only remove the group.

To remove a group from the project, select the group and click **Remove** ⊖.

Example:

From **Organization**, filter on **Test**. Then, select the group and click **Add**.



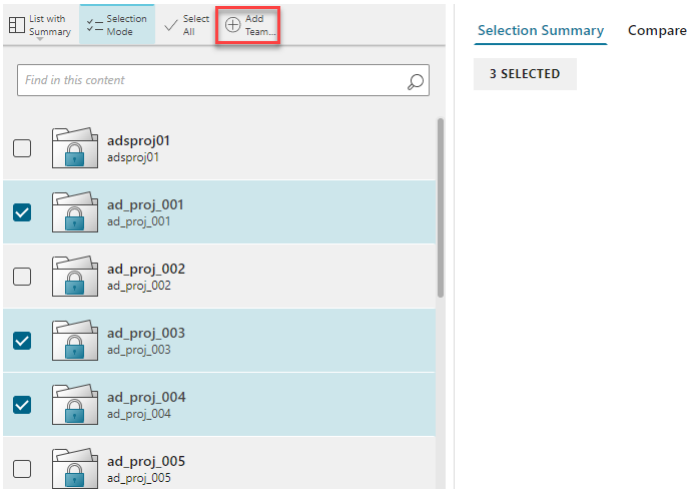
Add a group to multiple projects

1. Log on as **Project Administrator** or **Team Administrator**.

2. Click **Selection Mode** to enable multiple selections.

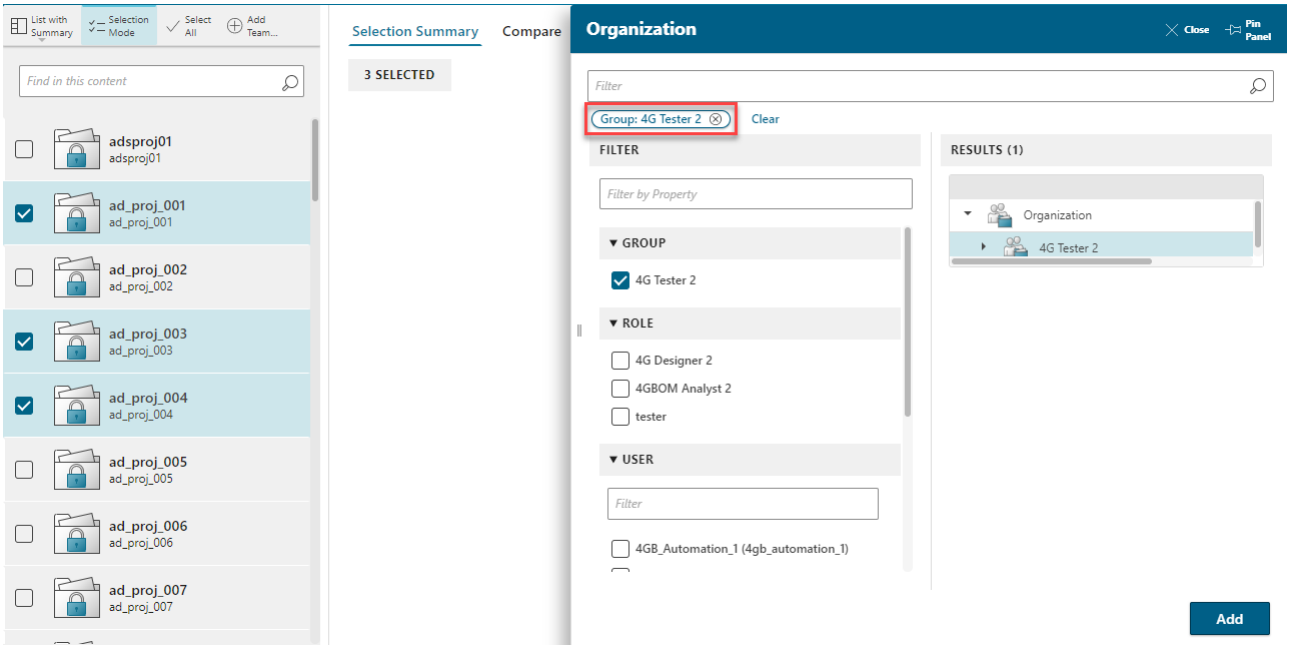
3. Select one or more projects.

   Click **Add Team Members** in the results panel or from the primary toolbar (**Manage** > **Add Team Members**).

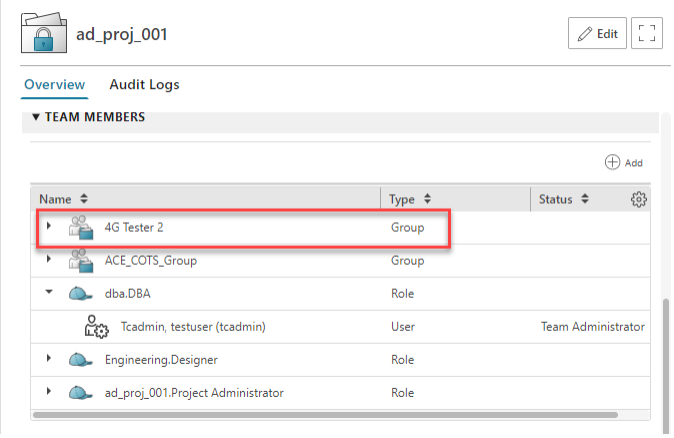


The **Organization** panel appears.

4. Choose a group to add to the selected projects and click **Add**.



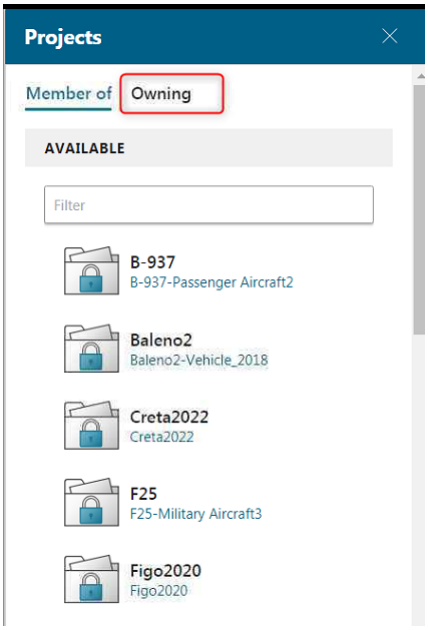
The selected group, **4G Tester 2**, is added to the selected projects.



Configuring owning program

You can set or change an owning program on an object to control access to data. Once you configure owning program, users can set or change owning programs for instances such as:

- No owning program is set on data.
- A user mistakenly assigned data to the wrong program.
- Government policies force data to be tagged with a different owning program.
- Addressing a partner program change request.



To view the **Owning** program tab, you must set the **AWC_Project_showOwningProgramTab** preference to **true**. Owning program can be set on the object only if the **autoAssignToProject** extension is enabled on the object type.

> Note:
>
> If you use the Aerospace and Defense template, the **autoAssignToProject** extension is enabled by default.

For more information on owning program and the **autoAssignToProject** extension, refer to *Project and Program* in the Teamcenter documentation.

Configure project-level security

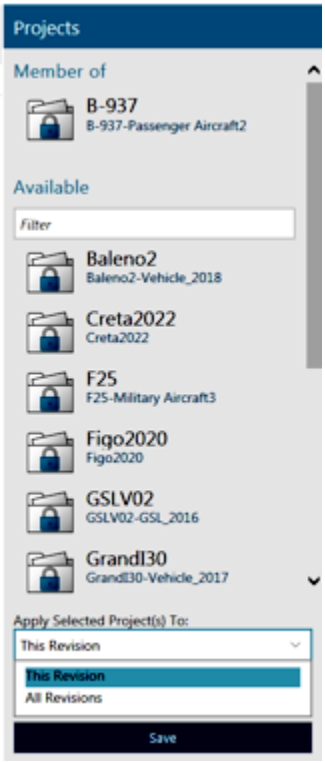
You can configure project-level security for selected objects at the item level and have it available to all revisions under the item. When selecting either **This Revision** or **All Revisions**, the following preferences should be set to the default value to ensure security is applied correctly.

- **TC_Security_Apply_To_Visible**

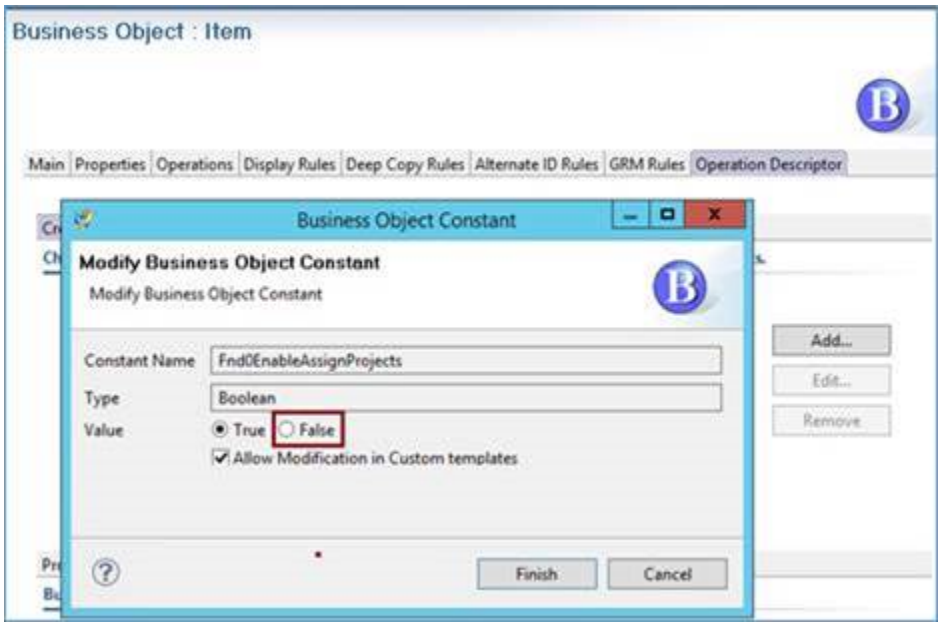
  Activates the visibility of the **Apply To** project option. When set to **true** (default), the **Apply To** project option is available.

- **TC_Security_Apply_To_Item_Revision**

  Controls the behavior of the **Apply To** project option. When set to **true**, security is applied to item revisions. If set to **false** (default), security is applied to items.



Also, you can hide the project section from the **Add** panel for items. To do this, modify your data model configuration in Teamcenter using the Business Modeler IDE and set the **Fnd0EnableAssignProjects** constant to **False**.



For more information about modifying business object constants, see *Configure your business data model in BMIDE*.

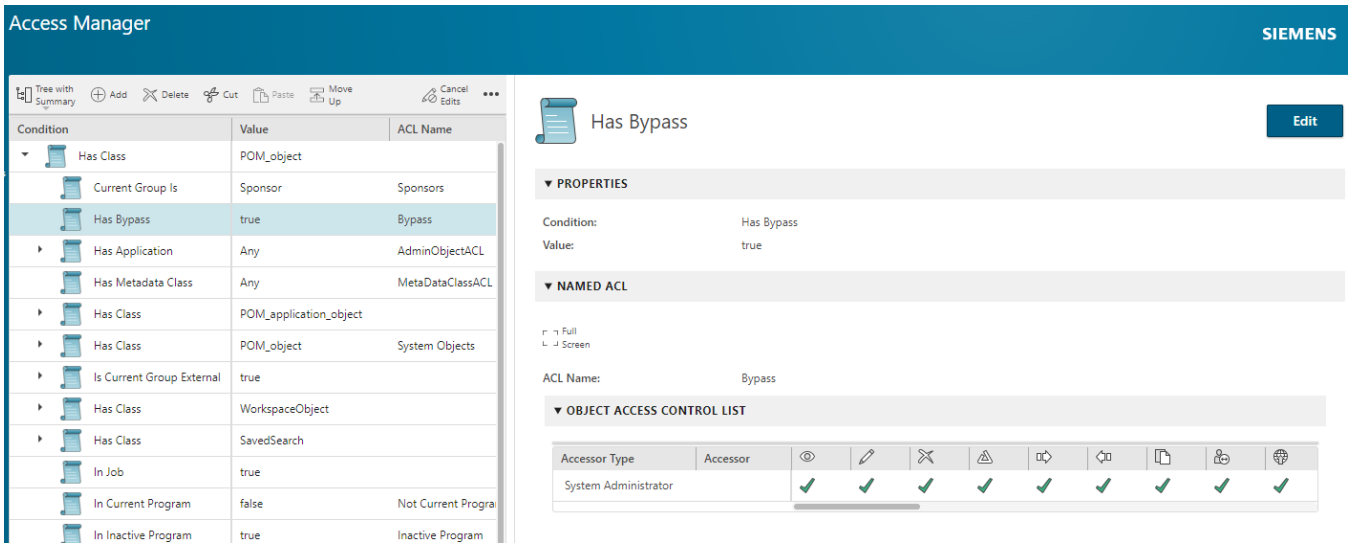
Managing users' access to data using Access Manager

Controlling access to data objects

In addition to licensing and authentication, another way to control information access for users, both internal and external, is by configuring Access Manager rules. These rules control access by user, group, role, organization, and workspace.

Access Manager is available only in the **Active Admin workspace** in Active Workspace for users in the **dba** group and **DBA** role.

> Note:
>
> Access Manager is also available in the Teamcenter rich client.



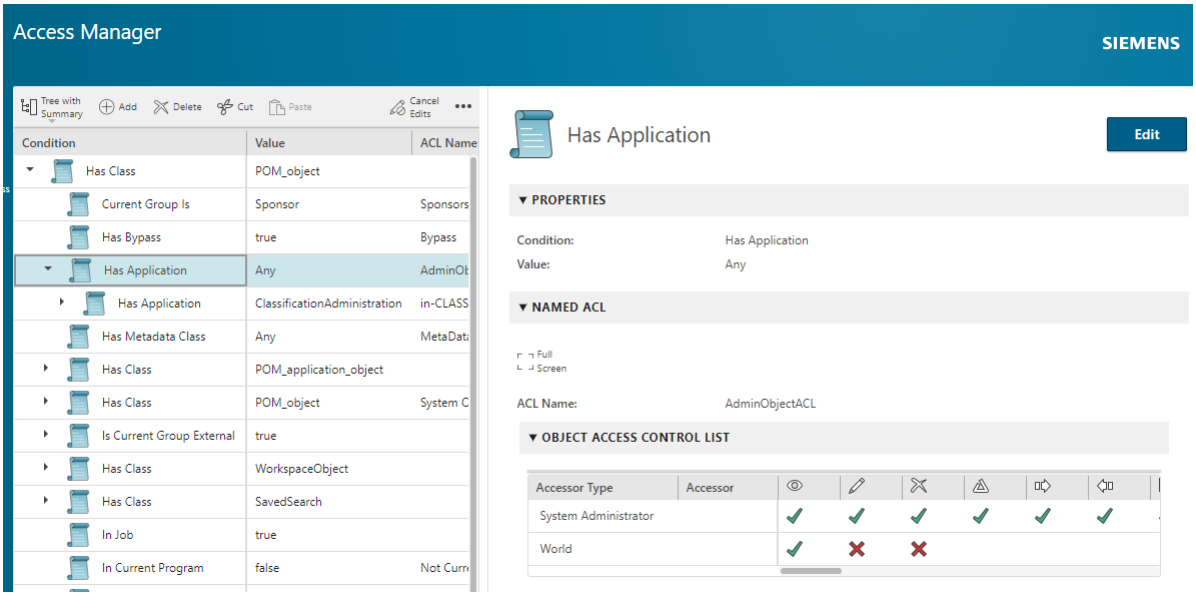
Using Access Manager rules

View Access Manager rules

From the **Access Manager** page, you can view the entire Access Manager (AM) rule tree using either **Tree** or **Tree with Summary** (default) mode.

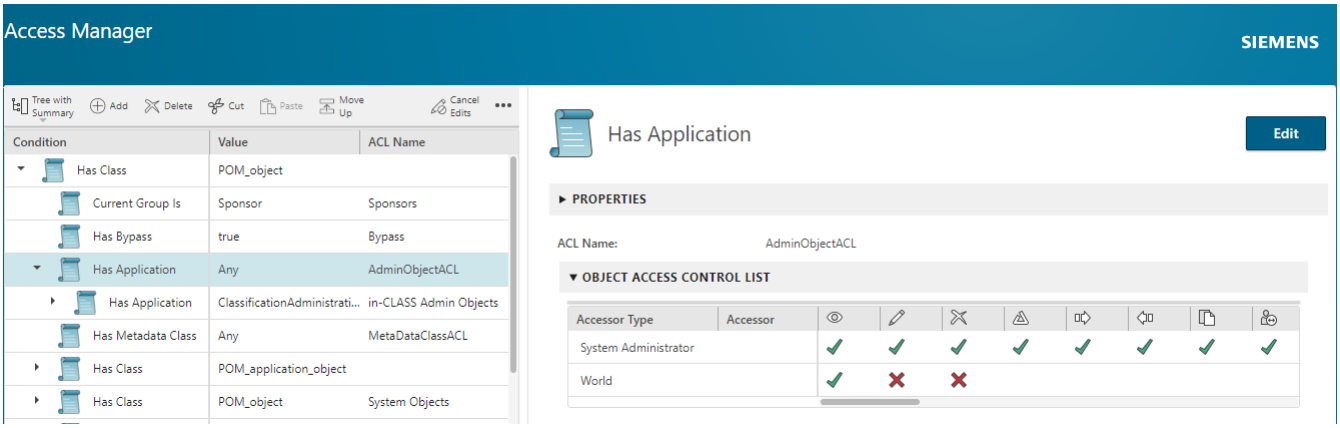
Select a rule from the AM rule tree, for example, **Has Application** to view the following areas:

- **PROPERTIES**, which includes the condition name (**Has Application**) and value (**Any**).
- **NAMED ACL**, which displays the access control list (ACL) name (**AdminObjectACL**).
- **OBJECT ACCESS CONTROL LIST**, which displays the ACL that lists the privileges granted to the specified accessor types. For example, **World** is granted **Read** (👁) access, but it is denied **Write** (✎) and **Delete** (✕) access.



Add an Access Manager rule

1. Select a node from the AM rule tree, such as **Has Application**.



2. Click **Add** ⊕ in the work area toolbar.

   This displays the **Add Rule** panel.

3. Select the condition, for example, **Has Attribute**.

4. Enter a value.

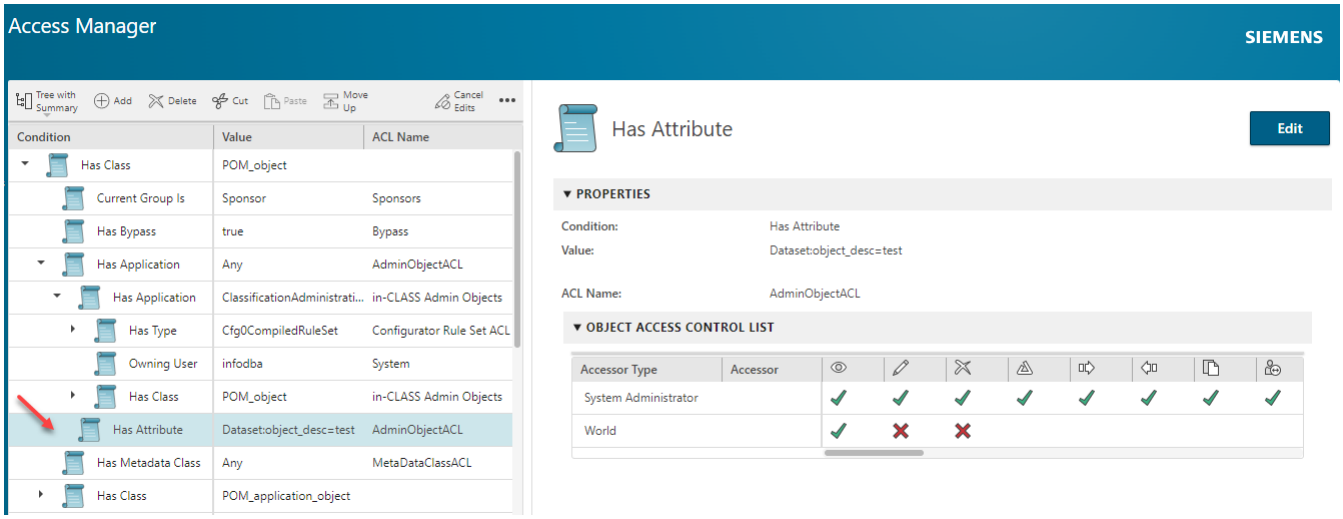
   The value is populated based on the selected condition. However, since the **Has Attribute** condition does not have a value, you can enter any value. For example, **Dataset:object_desc=test**.

5. (Optional) Select an **ACL Name**, for example, **AdminObjectACL**.

   To add additional rules, select **Pin Panel** .

6. Click **Add** to add the new rule under the selected parent node.

   By default, the new rule appears as the last node under the parent.



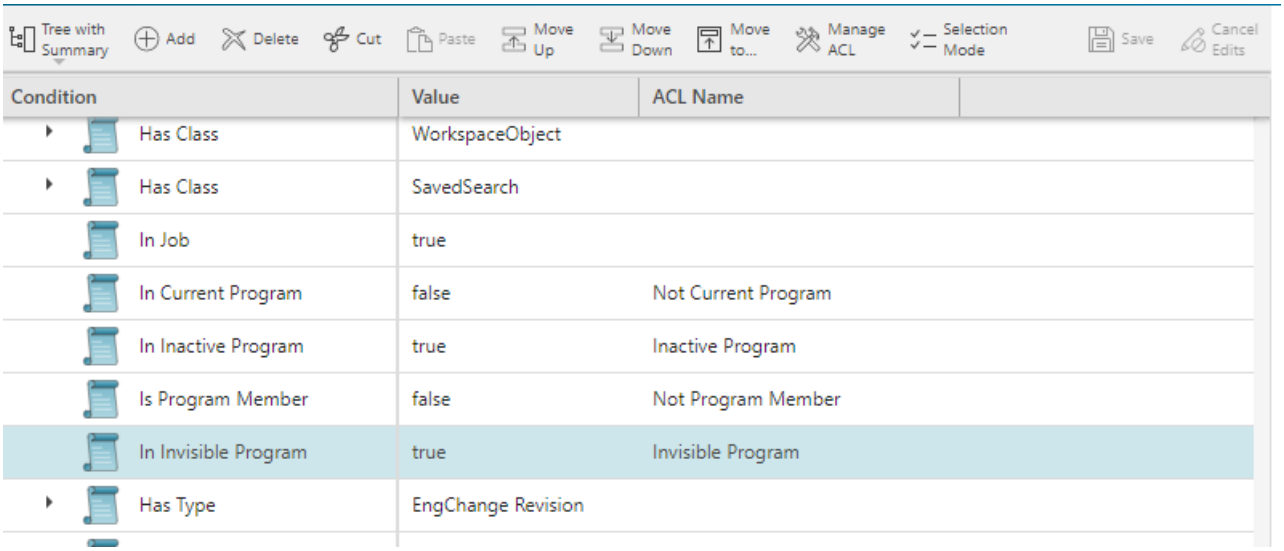
Reorder Access Manager rules

From within the AM rule tree, you can reorder your rules and save your changes.

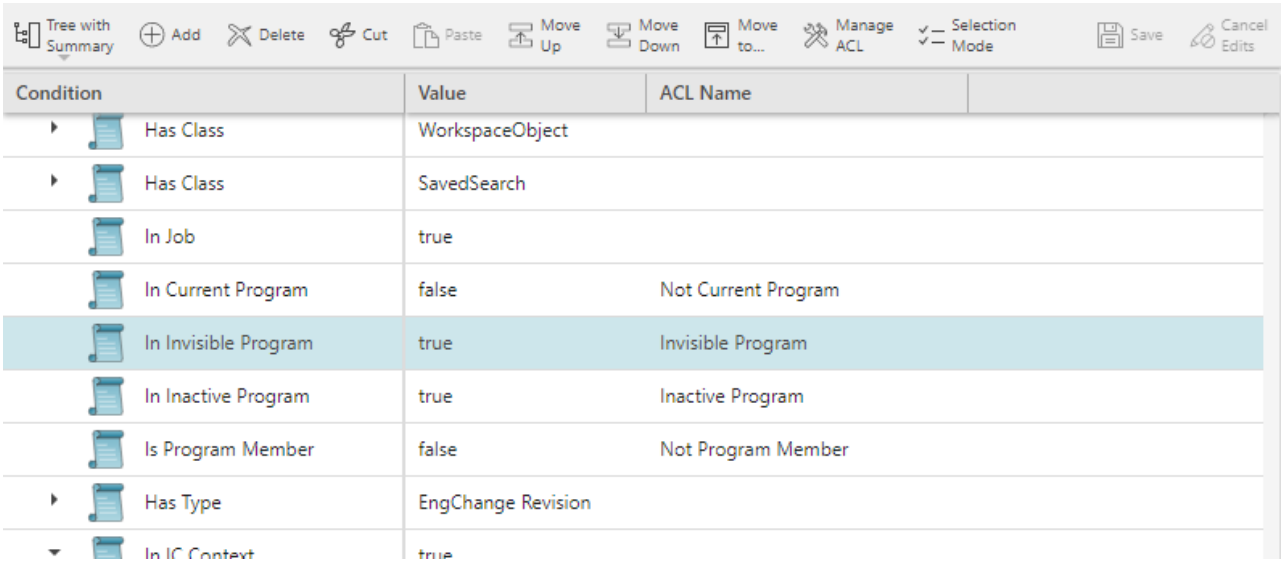
Reorder action	Icon	Description
Cut		Cut a single or multiple rules.
Paste		Paste the single or multiple rules you have cut.
Selection Mode		Turn on selection mode for making multiple rule selections.
Move Up		Move a selected rule up the AM rule tree.
Move Down		Move a selected rule down the AM rule tree.
Move to Top		Move a selected rule to the top of the AM rule tree.

Example — Move a single AM rule up the AM rule tree

1. From the AM rule tree, select a single rule, for example, **In Invisible Program**.



2. Click **Move Up** two times to position the rule directly below **In Current Program**.



3. Click **Save**.

   Edits to the AM rule tree persist for that session until changes are committed to the database using the **Save** command.

Delete an Access Manager rule

> Note:
>
> Some rules cannot be deleted.

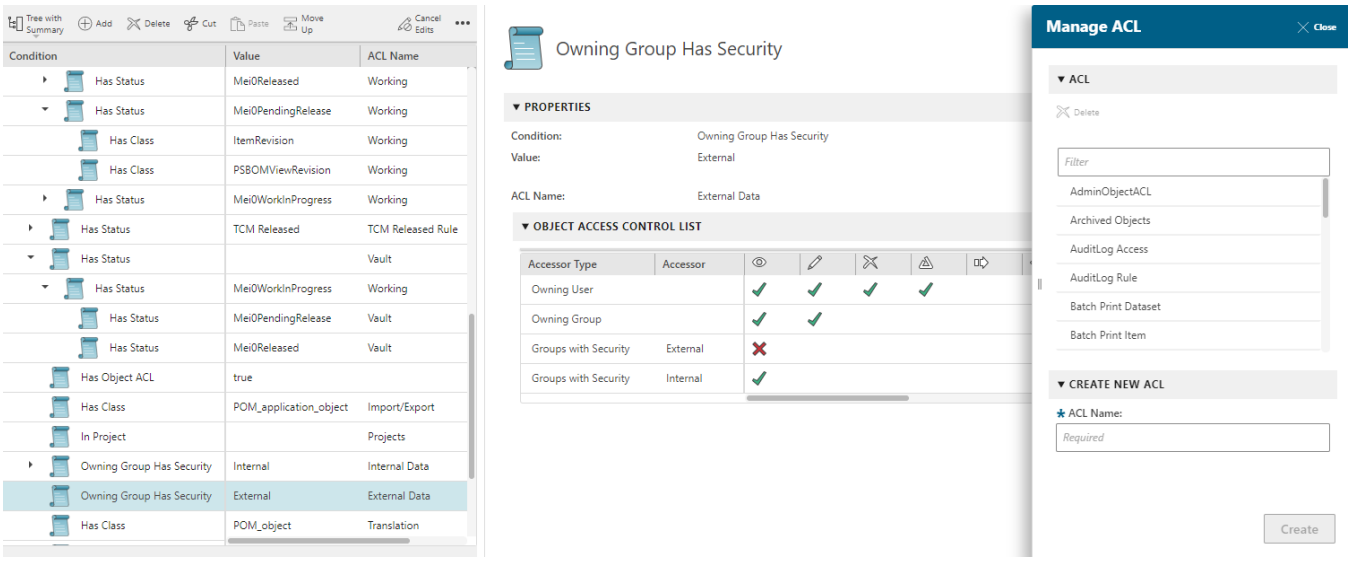
1. From the AM rule tree, select either a single rule or multiple rules to delete.

2. Click **Delete** ⊗ in the work area toolbar.

Managing access control lists

What are access control lists?

Access control lists (ACLs) contain a list of accessors and the privileges granted, denied, or not set for each accessor. Accessors are collections of users who share certain common traits, such as membership in the group that owns the object or membership in the project team. Just as rules have a precedence weighting in the rule tree, accessors have a precedence weighting in the ACL.



Create a new ACL name

1. From the **Access Manager Rules** tab, click **Manage ACL** in the work area toolbar to display the **Manage ACL** panel.

2. From the **CREATE NEW ACL** section, type a unique ACL name in the **ACL Name** field.

3. Click **Create**.

   You can confirm the new ACL name in the **ACL** section by filtering on the new name.

Edit an ACL

1. Select the condition for the ACL you want to edit, for example, **In Project**.
2. From the condition information page, click **Edit**.

   You can edit the **PROPERTIES** fields and the **OBJECT ACCESS CONTROL LIST** fields.
3. Perform one or more of the following functions on an ACL.

Function	Icon	Description
Add		Add an access control entry.
Remove		Remove an access control entry.
Allow All		Allow access to all privileges for the selected row.
Deny All		Deny access to all privileges for the selected row.
Reset		Reset the selected row to the last saved values for the privileges.
Clear All		Clear all privileges of the selection.
Selection Mode		Turn on selection mode for making multiple accessor selections.

4. Click **Apply** to save your ACL updates.

Delete an ACL name

> Note:
>
> There are certain ACL names that cannot be deleted. Refer to your Teamcenter system log for additional information.

1. From the **Access Manager** page, click **Manage ACL** in the work area toolbar to display the **Manage ACL** panel.
2. From the **ACL** section, filter, and select the existing ACL to delete.
3. Select **Delete**.

Import and export Access Manager rules

Why import and export my Access Manager rules?

Access Manager now allows you to import and export your rule tree in Active Workspace. This helps you to easily:

- Distribute access rules to other Teamcenter sites.
- Back up your rule tree.
- Restore your local rule tree.

Import an Access Manager rule tree

You can import your Access Manager (AM) rule tree from within Access Manager. Your imported AM rule tree replaces the current one.

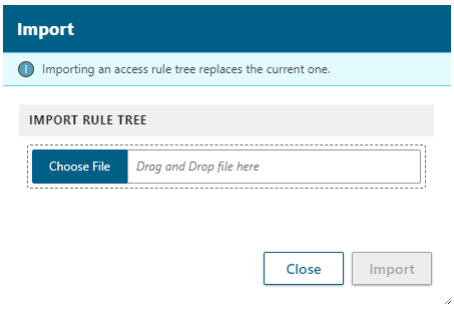
Prerequisites

Before importing a rule tree, you must ensure schema compatibility. To successfully load a new rule tree from a file, the importing site must have the same types, roles, and groups as those referenced in the rule tree file. If there is any incompatibility, the import operation ends and an error message appears. To resolve incompatibility, you can import your organization data and then load your rule tree.

Procedure

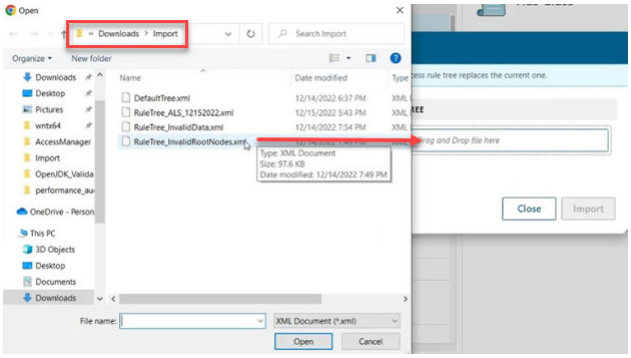
1. From your work area toolbar, select **Import** to display the **Import** dialog box.

   This command is only enabled in non-edit mode.



2. Click **Choose File** to locate the XML rule tree file that you want to import. Then, drag and drop the file into the field.

   For example:



3. Click **Import**.

   A progress indicator is displayed during import.

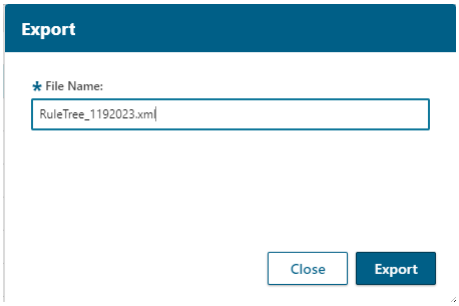
Export an Access Manager rule tree

You can only export your Access Manager (AM) rule tree in XML format from within Access Manager.

Procedure

1. From your work area toolbar, select **Export** to display the **Export** dialog box.

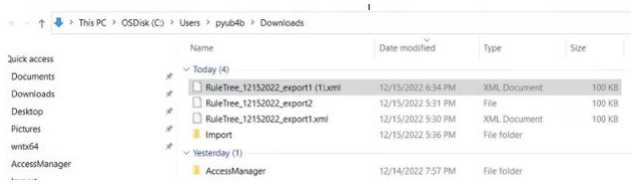
   This command is only enabled in non-edit mode.



2. By default, the rule tree is named. For example, *RuleTree_mmddyyyy.xml*. You can change the file name to one that fits your organization's file naming convention.

3. Click **Export**.

   The file is downloaded based on your default browser settings, for example, to your **Downloads** folder.



4. Relations configuration

Relations configuration tasks

What are relations?

Relations are the associations between two Teamcenter objects. The **Relations** tab in Active Workspace allows you to see all the relationships for a selected object.

Why configure relations?

You may want to change how relations are displayed to end users or change which relations are displayed.

What do I need to do before configuring?

Before you can view relations graphically, you must install the following Active Workspace features using the Teamcenter Environment Manager (TEM):

- **Relationship Browser**

  Installs the user interface elements for viewing relations in Active Workspace.

  Select **Active Workspace→Client→Relationship Browser**.

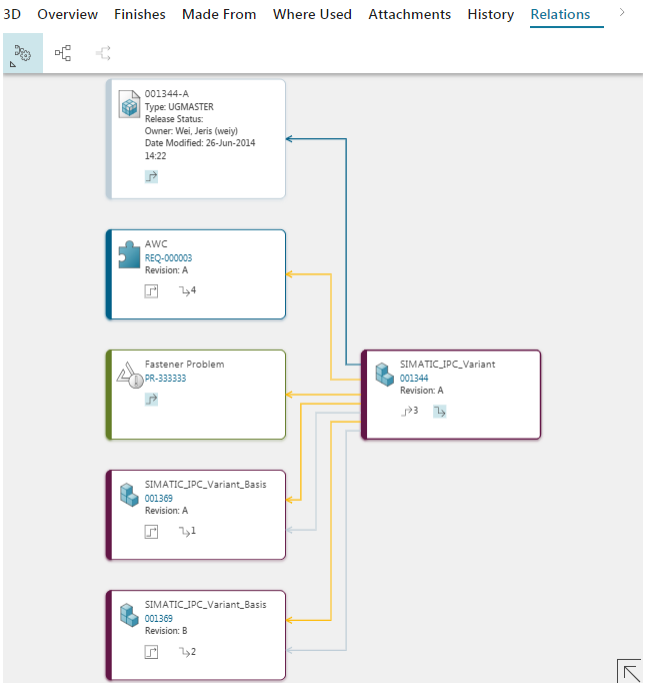
- **Relationship Viewer**

  Installs the server-side definitions for viewing relationships.

  Select **Active Workspace→Server Extensions→Relationship Viewer**.

What do relations look like?

Following is an example of the **Relations** tab in Active Workspace.



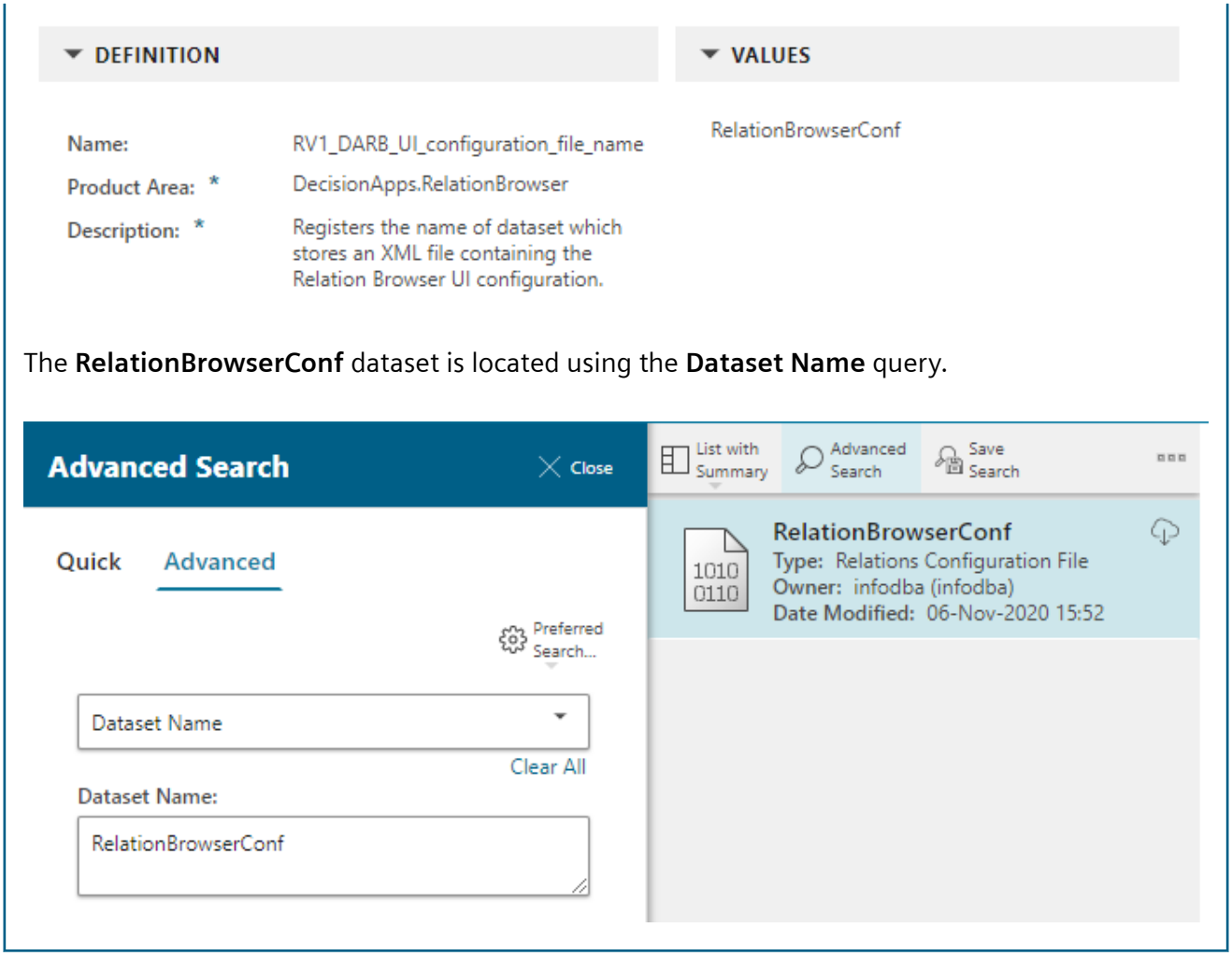
How can I make changes?

You can configure aspects of relations' appearance and behavior using configuration files. These are stored in the Teamcenter database as datasets, which are located using the following preferences:

- **RV1_DARB_UI_configuration_file_name**
- **RV1_DARB_GraphStyle_file_name**
- **RV1_DARB_PresentationRule_file_name**

1. Find the name of the dataset by getting the value of the config file preference.
2. Find the dataset by name using the advanced search functionality.
3. Make the necessary edits to the configuration file.
4. Save the changes.

> Example:
>
> In this example, the **RV1_DARB_UI_configuration_file_name** preference value is **RelationBrowserConf**.



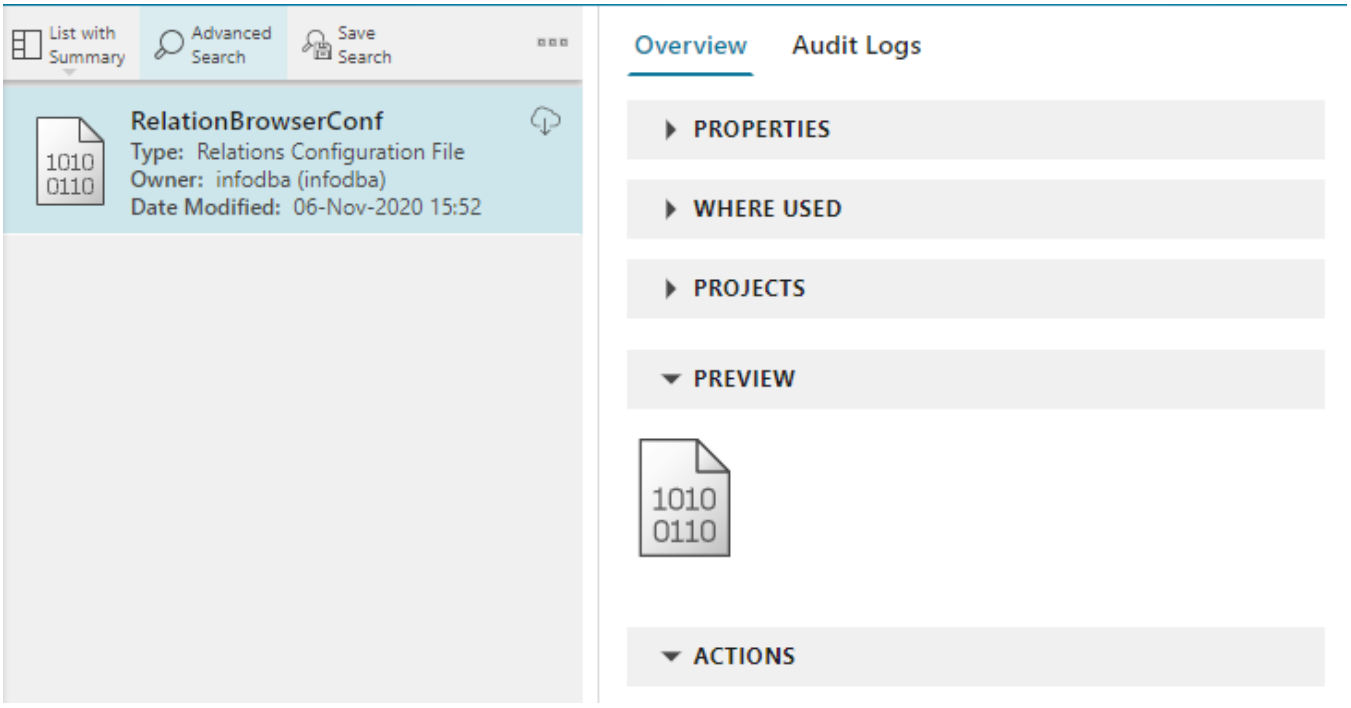
The **RelationBrowserConf** dataset is located using the **Dataset Name** query.

How can I edit the configuration files?

To edit the configuration files, you can:

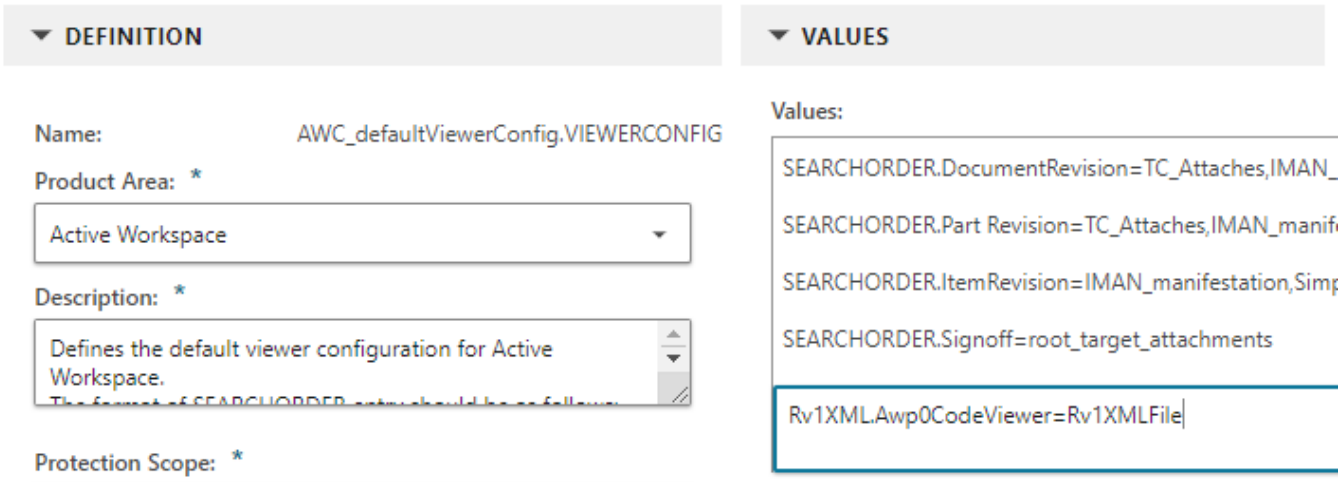
- Download the file, edit it in a text editor, and then upload it back into Active Workspace.
- Edit them in place using the universal viewer.

OOTB, the universal viewer may not recognize the relation configuration file dataset type (**Rv1XML**) as an editable file type and it will only show the generic dataset type icon in the **PREVIEW** section.

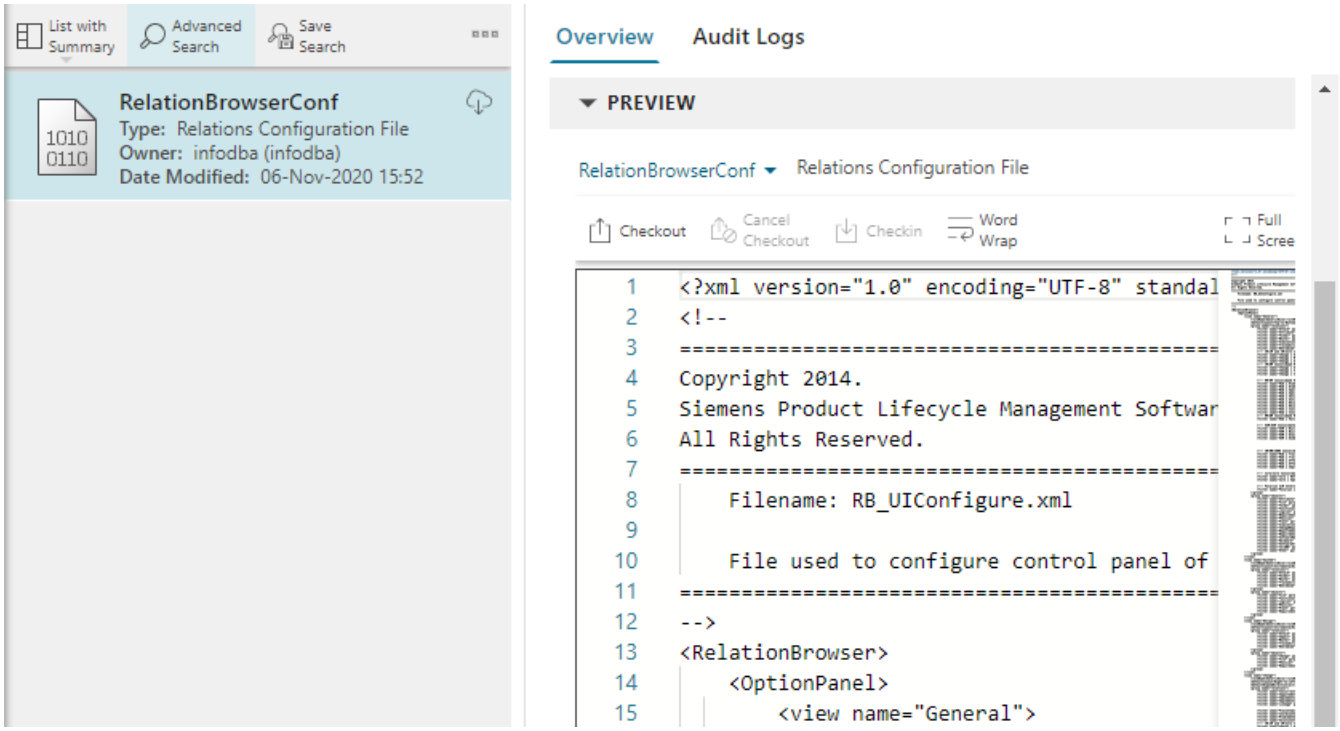


To tell the universal viewer how to open this file type, add **Rv1XML.Awp0CodeViewer=Rv1XMLFile** to the preference.

This is because the **Relations Configuration File** dataset type's database name is **Rv1XML** and the named reference for the XML file is **Rv1XMLFile**.



Now the universal viewer knows to open the configuration files with its code viewer.

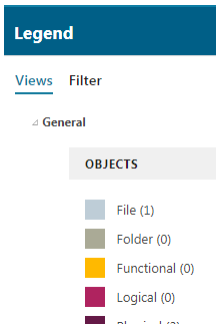


What other preferences control the relation browser?

There are many preferences that can help you configure relations for your users. Their names begin with **Rv1_** to make them easy to find. Inspect each of these preferences and update their content if necessary.

Creating new views or updating existing views

A view is a group of objects and relations in the **Legend** panel.



The **RV1_DARB_RelationBrowserViews.Relations** preference lists the available views. You can update this preference to add new views or update existing views.

The first view on this list is the default view. This preference is overridden by any other preference with an object type name appended.

If you append the name of an object type to the preference, the list of available views changes for that class of objects and all of its children. You can create as many of these preferences as you need. For example, the **RV1_DARB_RelationBrowserViews.Relations.ChangeItemRevision** preference controls the list of views (and the default) for change revisions.

Example of configuring relations expansion

You can configure how the system expands the relations forward and backward, and also how many levels. For example, when users open an object in the **Relations** tab, the system may automatically expand the relations forward one level. If your users are not interested in confirming the data attached by outgoing relations but rather confirming incoming relations, you can set the expansion to automatically expand backward. Set the expansion of relations with the following preferences.

- **RV1_DARB_Expand_All_1_Level_Command_Visible**
- **RV1_DARB_Expand_Incoming_Levels**
- **RV1_DARB_Expand_Outcoming_Levels**
- **RV1_DARB_Expand_Selected_1_Level_Command_Visible**

Localize names that appear in a custom Relations view

No additional action is required to localize the names that appear in a custom relations view. If you localize the Active Workspace client in the declarative definition (**messages.json** file) and the Teamcenter TextServer, names in the **Relations** view are localized.

The file name for relation browser keys in the TextServer is **relationshipviewer_text_locale.xml**. Relation browser uses a **k_relations_keyword_** prefix to help promote unique keys throughout the product.

Relation browser config file syntax

Appearance configuration limitations

The appearance configurations are limited to the color and the edge style (relation), the style of the nodes is not configurable.

RV1_DARB_GraphStyle_file_name

The configuration file value stored in this preference uses the following options:

- **PresentationRule**

Defines rules for one type of object. It the object satisfies the conditions specified by the rule, the style will be applied to the object.

This element has the following subelements:

- **type**

  Specifies the type of object: **node** for object and **edge** for relation.

  > Note:
  >
  > Styling is not supported for **type node**. For the **node** option, set the color from the configuration defined in **RV1_DARB_UI_configuration_file_name** section as shown in this topic.

- **port**

  Specifies the port for relation.

- **styleID**

  Specifies what style to apply. **styleID** must be the same as defined in the GraphStyle XML file. (The name of the GraphStyle XML file is defined in the **RV1_DARB_GraphStyle_file_name** preference).

- **Conditions**

  Specifies a condition value that must be satisfied before the style is applied to the object. The condition value is a logical operator.

  This element has the following subelements:

  - **Property**

    Only used when the PresentationRule type is edge. **Name** specifies the relation type. **Value** specifies the relation name.

    For **Property** elements, only the **equalTo** operator is supported.

  - **Type**

    Only used when **PresentationRule** type is **node**. **Value** specifies the name of the object.

> Note:
>
> Styling is not supported for **type node**. For the **node** option, set the color from the configuration defined in **RV1_DARB_UI_configuration_file_name** section as shown in this topic.

- **Conditions Operator**

  Specifies what conditions must be must before the style is applied. Valid operators are: **and** (all rules must be met) and **or** (at least one of the rules must be met).

  Valid operators for **Type** are **equalTo** and **isTypeOf**. When property is **edge**, only the **equalTo** operator is valid.

RV1_DARB_UI_configuration_file_name

The configuration file value stored in this preference uses the following options:

- **view name**

  Specifies the name of the view, for example, **General**.

- **ruleName**

  Specifies the name of the dataset that implements the traversal logic of the view. The **GenericRule** dataset is the default rule file.

- **group name**

  Specifies if this is a list containing objects or relations. These lists are presented in the **Relation Controls** section of the **Relations** browser.

  The order of the **objects** filters is important. Your object is displayed using the first filter on the list that successfully matches. The last filter in the **objects** section, **Other**, matches all objects because it is associated with **WorkspaceObject**. It is there to ensure all objects receive some formatting. Do not place any filters after the **Other** filter.

- **filter name**

  Specifies the name of the relation or object name.

  For example:

```
<filter name="Attach" parameterSet="Attach" color="(64,100,142)"/>
<filter name="File" parameterSet="Dataset" color="(202,216,234)"/>
```

- **parameterSet**

  Specifies the name of the **parameterSet** element in this configuration file. The **parameterSet** element defines the Teamcenter objects and relations that map to the filter name.

- **color**

  Specifies the display color of the object or relation.

5. Data sharing

Configuring and managing data sharing

Active Workspace offers users and administrators several ways to share Teamcenter data. Each of these methods of sharing data has capabilities an administrator can manage.

- Briefcase lets users share Teamcenter data with connected and unconnected sites using TC XML and Briefcase files.
- Multi-Site Collaboration lets users share and synchronize data in near real-time between Teamcenter sites across the entire enterprise.
- PLM XML lets users share Teamcenter data with third-party applications using the open PLM XML format.
- Bulk data migration tools let administrators exchange large volumes of data when populating test environments.
- Advanced Multi-Schema Exchanger lets user with Active Architect privileges create mapping rules that transform data when it is shared between Teamcenter sites that use different schemas.

Briefcase

Briefcase (on Windows or Linux), TC XML Import and Export, and Teamcenter Dispatcher Server (on Windows or Linux) must be installed to access Briefcase features using Active Workspace

Each Active Workspace site that is importing or exporting Teamcenter data must have a Briefcase license. Active Workspace sites using the following optional import and export features must each also have an Advanced Multi-Schema Exchanger license:

- Briefcase export and import dry run and validation capabilities
- Briefcase preview and compare capabilities
- Advanced Multi-Schema Exchanger

Contact your Siemens Digital Industries Software customer service representative for more information on Briefcase licenses.

See **Configure Briefcase file sharing** to configure Briefcase capabilities.

Multi-Site Collaboration

Multi-Site Integration (on Windows or Linux) must be installed to access Multi-Site Collaboration features using Active Workspace. Collaborating sites also need to be licensed to use Multi-Site Collaboration.

Configure and monitor Multi-Site Collaboration status.

- **Control the scope of remote Multi-Site Collaboration objects checked out and checked in by users**.

- **Configure** and **use Multi-Site Dashboard** to monitor the status of your Multi-Site federation.

PLM XML

PLMXML Export Import (on Windows or Linux), TC XML Import and Export, and Teamcenter Dispatcher Server (on Windows or Linux) must be installed to access PLM XML features using Active Workspace.

See **Configure PLM XML data sharing** to specify the list of PLM XML object types that can be exported and imported at your site.

Bulk data migration tools

Briefcase (on Windows or Linux), TC XML Import and Export, and Teamcenter Dispatcher Server (on Windows or Linux) must be installed to access the Active Workspace bulk data migration tools.

See **Bulk loading product data** to extract data from one Teamcenter environment to copy to another.

Advanced Multi-Schema Exchanger

Teamcenter Dispatcher Server (on Windows or Linux), Advanced Multi-Schema Exchanger, and the Advanced Multi-Schema Exchanger Service microservice must be installed to access **Advanced Multi-Schema Exchanger using Active Workspace**.

To open and use Advanced Multi-Schema Exchanger, the user must be logged on to Active Workspace with privileges to use the Active Architect workspace.

General data sharing

See **Configure report layout settings** to configure the readability of data sharing export, import, and validation reports.

Configure report layout settings

Data sharing export, import, and validation reports are formatted for readability with a monospaced typeface. This layout is controlled by including the following settings in the **AWC_defaultViewerConfig.VIEWERCONFIG** preference value:

```
Text.Awp0TextViewer=Text
XMLRenderingStylesheet.Awp0TextViewer=XMLRendering
```

Ensure the following values, which improve rendering of code, are not included in the **AWC_defaultViewerConfig.VIEWERCONFIG** preference value:

```
Text.Awp0CodeViewer=Text
XMLRenderingStylesheet.Awp0CodeViewer=XMLRendering
```

Configure Briefcase file sharing

Ensure the following **preferences** are set to your organization's needs for exchanging objects using Briefcase files.

Briefcase_checkout_supported_types

The list of types supported for Briefcase checkout.

Briefcase_configured_export_supported_types

The list of types supported for Briefcase configured export.

Briefcase_export_supported_types

The list of types supported for Briefcase export.

Briefcase_ownership_transfer_supported_types

The list of types supported for Briefcase site ownership transfer.

Briefcase_pkg_file_name

The default file name format for exported Briefcase files.

Briefcase_tcmail_notification

Specifies whether an email notification is sent when a Briefcase is created.

Configure PLM XML data sharing

Import and export objects of any type supported by the PLM XML schemas. Set the **AWC_PLMXML_export_supported_types** preference to the list of PLM XML types that can be exported and imported at your site. By default, **AWC_PLMXML_export_supported_types** is set to a list of common PLM XML object types.

Create mapping rules using Advanced Multi-Schema Exchanger

Using Advanced Multi-Schema Exchanger to create mapping rules

Use Advanced Multi-Schema Exchanger to create mapping rules to transform data when it is transferred between Teamcenter sites using different schemas. You can **create mapping rules** for Item types in your source schema. Create and deploy maps using the following process:

1. **Acquire the source and target schemas describing the data being exchanged**.
2. **Create a mapping project in Active Workspace**.
3. **Create rules that map items and their attributes in the source schema to items and attributes in the target schema**.
4. **Deploy the mapping rules by attaching them to the transfer modes used when transferring the data**.

Preparing for a mapping project

The following items are required for creating mapping rules using Advanced Multi-Schema Exchanger:

Source schema

The source schema describing the data being exchanged. This is a full JSON schema covering all possible items and attributes. See Creating a JSON schema file to create a JSON schema file from your Teamcenter database.

Target schema

The target JSON schema describing the data in the target database.

Creating and updating mapping projects

A collection of Advanced Multi-Schema Exchanger schema mapping rules is called a *project*. Create a mapping project for defining the set of mapping rules required for exchanging data between two sites.

Start Advanced Multi-Schema Exchanger

To open and use Advanced Multi-Schema Exchanger, you must be logged on to Active Workspace as a user with privileges to use the Active Architect workspace.

- On the Active Architect workspace, click the **Advanced Multi-Schema Exchanger** tile. Advanced Multi-Schema Exchanger opens with the most recent projects listed.

Create a mapping project

1. Click **Add** ⊕ above the project list to create a project.

   The **Add Schema Map** panel opens.

2. Specify a name for the project, select your source and target schema files, and click **Add** to save the project.

Update a mapping project

Update a mapping project when your source or target schemas change or when you wish to rename the project.

1. On the Active Architect workspace, click the **Advanced Multi-Schema Exchanger** tile. Advanced Multi-Schema Exchanger opens with the most recent projects listed.

2. Select the project you want to update.

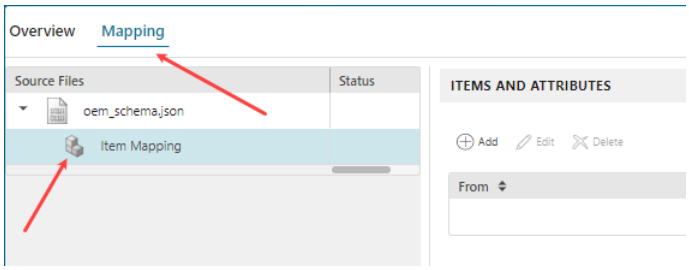
   The project's properties are displayed.

3. Under **Properties**, click **Edit** ✎.

4. Update the name of the project or the schema files as necessary and click **Save Edits** 💾.

Mapping object types

With your project open in Advanced Multi-Schema Exchanger, click the **Mapping** tab to show the **Item Mapping** category of the source schema. For example:



Object type mapping

1. Click the **Mapping** tab to show the categories containing the object types that can be mapped.

2. Click **Item Mapping**. A summary of the currently mapped object types and their attributes is displayed in the **Items and Attributes** pane. (A new project has no types mapped.)

3. Select an object type for mapping.

   - To create a new object type mapping, click **Add** ⊕ in the **Items and Attributes** pane.

     The **Add Mapping** panel opens.

   - To edit an existing object type mapping, select the object type in the summary list and click **Edit** ✎.

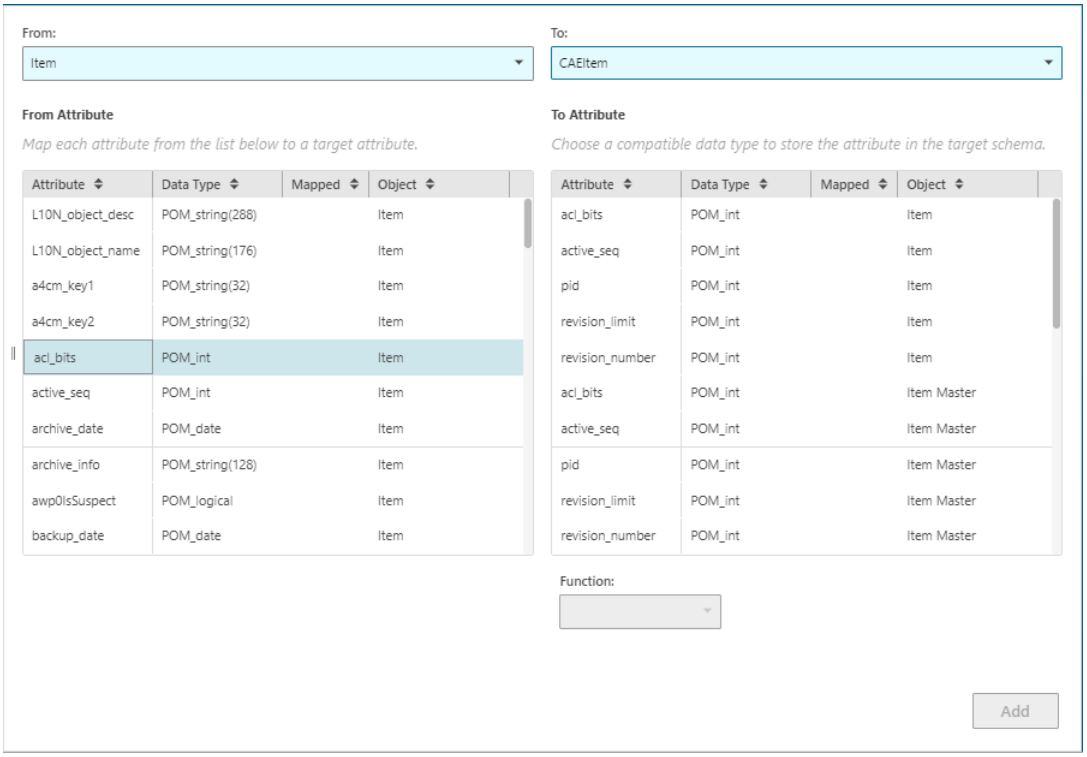
     The **Edit Mapping** panel opens.

4. In the **From** list, select an object in the source schema.

5. In the **To** list, select the target object. (Only valid target objects are listed.)

   The source and target objects, and their attributes with default mappings appear in the panel. By default, attributes in the source object are mapped to attributes in the target object when the objects have the same name, length, and type.

   For example:



6. Map (or remap) a source attribute by selecting it and then selecting the target attribute to which it is to be mapped.

To avoid item ID conflicts, consider adding prefixes and suffixes to the target attributes as part of the mapping. After mapping an attribute, set **Function** to "Prefix" or "Suffix", and specify a value, for example:

7. After mapping an attribute, click **Save** (or **Add** for new mappings) to save the change.

> Tip:
>
> Click **Pin Panel** to keep the panel open as you map several attributes.

To remove the mapping for an object, select the item in the summary list and click **Remove Mapping** .

Deploying mapping rules

Deploying mapping rules attaches the rules to the transfer modes used for transferring the data. Use the following steps to deploy your mapping rules.

To deploy mapping rules, you must be logged on to Active Workspace as a Teamcenter administrator with DBA privileges.

1. Ensure that you have **mapping rules for all object types**.

2. Select the project in the Advance Multi-Schema Exchanger list of projects. Click **Deploy** in the **Deployment** section.

3. Select the transfer mode set you are using to transfer the data.

4. Click **Deploy**.

   You receive a report alert when the deployment is complete. Click on the alert to review the details of the deployment. All recent alerts are available from the **Subscription** tile. Check the **SCHEMA_MAPPING** message type to see all deployment reports.

Once deployed, the mapping rules are attached to the transfer mode. In Active Workspace, you can now use the transfer mode to share data.

Detach rules from a transfer mode

Detach rules from a transfer mode as follows:

1. From a Teamcenter command window, enter the following command to determine the name of the rule file attached to the transfer mode:

```
plmxml_tm_edit_xsl -u=Tc-admin-user -p=password
  -g=group -action=list -transfermode=transfer_mode_name
```

Where:

Tc-admin-user, *password*, *group*

Logon credentials of a Teamcenter administrator with DBA privileges

transfer_mode_name

The name of the transfer mode with the attached rules

2. Use the following command to detach the rule file from the transfer mode:

```
plmxml_tm_edit_xsl -u=Tc-admin-user -p=password
  -g=group -action=detach -transfermode=transfer_mode_name
  -xsl_file=rule_file_name
```

Where:

transfer_mode_name

The name of the transfer mode with the attached rules

rule_file_name

The rule name identified in the first step

Manage Multi-Site

Specifying the scope of Multi-Site remote checkouts and checkins

Use the **MultiSiteCICORule** closure rule to control the scope of objects checked out and checked in by users when they check out and check in remote objects managed by Multi-Site Collaboration. The closure rule defines primary objects and the related secondary objects to be checked out or checked in as well.

Update the closure rule definition to add other related objects to check out and check in automatically with objects. For example, to automatically check out related item revision datasets, add a line to the closure rule definition with the following values:

Clause Item	Value
Primary Object Class Type	**CLASS**
Primary Object	**ItemRevision**
Secondary Object Class Type	**CLASS**
Secondary Object	**Dataset**

Clause Item	Value
Relation Type	**RELATIONP2S**
Related Property or Object	**IMAN_specification**
Action Type	**PROCESS**
Conditional Clause	
Predicate	

Multi-Site Dashboard

Multi-Site Dashboard provides a way to view the issues **in your Multi-Site federation** through charts, graphs, and detailed object reports. Analyze and resolve these issues to reduce the number of errors and time spent by users in attempting to transfer data or to perform other business tasks.

The data reported in Multi-Site Dashboard is gathered when **running the data_report utility**. The dashboard identifies the following issues for the entire federation and for individual sites in the federation.

- ID issues such as:
  - Duplicate Item IDs, Item Revision IDs, or Keys (including multi-field keys)
  - Item IDs, ItemRevision IDs, or keys that are not synchronized with the owning site.
- Item ownership issues such as:
  - Items with multiple owning sites
  - Items with no owning site
  - Replicas with an owning site different than the primary item
- Object ownership issues such as:
  - Objects with ownership different than the item
  - Items and item revisions with inconsistent ownership
  - Objects with ownership inconsistent with their parent

See **Resolving Multi-Site issues** for recommendations on resolving these Multi-Site Collaboration data issues.

Viewing Multi-Site Dashboard issues

When you log on to Active Workspace as an administrator, the Multi-Site Dashboard tile is available on the Active Admin workspace home page. Use the following guidelines for viewing Multi-Site Dashboard issues.

Viewing issues

When first opening Multi-Site Dashboard, the status from the most recently run report is displayed, summarizing all issues across your entire Multi-Site federation. Hover over a chart to view the number of issues of each type.

The lower half of Multi-Site Dashboard breaks down the different types of issues across the federation. Change the value of **Chart by** to toggle between viewing issues by type or by site.

Return to the overall summary of issues across your Multi-Site federation at any time by clearing the selection for all sites in the left pane.

Viewing objects with issues

Click a site name in the left pane to see a breakdown of the types of issues found at that site. To see a further breakdown of an issue type, along with a listing of all objects with that issue, click one of the charts.

Viewing report history

Click **History** to see the federation or selected site trends for each error type over previous runs of the **data_report** utility. Select a different value for **Runs** to change the number of runs displayed. Hover over charted data points for summaries from each run.

Configuring Multi-Site Dashboard

Multi-Site Dashboard presents the status for specified sites in your Multi-Site federation based on data gathered when running the **data_report** utility. Configure and gather Multi-Site Dashboard data as follows.

Define sites from which Multi-Site data is gathered

The Multi-Site sites from which data is gathered and reported must be specified with the **MS_dashboard_Supported_Sites** option.

On the site from which reports are generated, add **MS_Dashboard_Supported_Sites** to the list of Teamcenter site names for which you want data reported by Multi-Site Dashboard. This is also the list of sites that are used with the **data_report** utility.

Run data reports

From a command line, use the **data_report** utility to gather and generate reports presented with Multi-Site Dashboard. You can run this report manually or use your operating system to schedule it to run at regular intervals.

- Run **data_report** on a site with access to the Teamcenter object database.
- Log on with administrator credentials when running **data_report**.

Following are some examples of using the **data_report** utility (not including required logon information). See data_report for additional details.

To gather data and generate reports for all sites and the overall federation (as defined with **MS_Dashboard_Supported_Sites**):

```
data_report
```

To gather data for a specific site:

```
data_report -site=site01 -f=collect_data
```

To generate reports for all sites and the Multi-Site federation using data previously collected:

```
data_report -f=generate_reports
```

Resolving Multi-Site issues

Following are guidelines for resolving issues identified by Multi-Site Dashboard.

Item ownership

Problem	Solution
Item with multiple owning sites	Decide which site is to be the owning site. To determine this, run the **item_report** utility to compare the items on the different sites. Convert the appropriate item from a primary item to a replica using **ensure_site_consistency** with the **-f=recovery** option. Using **-f=recovery** will recover the SST dataset if the dataset exists. If **-f=recovery** fails to convert the item to a replica, retry the command using **-f=offline_recovery** in place of **-f=recovery**. • If you do not have a TC XML meta file, use the form:

Problem	Solution
	`ensure_site_consistency -f=recovery -mode=auto -real_owning_site=`*master_site* • If you have a TC XML meta file, use the option **-mode=min** or **-mode=full** with **-dir=***meta_file_directory*.
Item with no owning site	Decide which site is to be the owning site. To determine this, run the **item_report** utility to compare the items on the different sites. Convert the appropriate item from a replica to a primary item using **ensure_site_consistency** with the **-f=recovery** option. Using **-f=recovery** will recover the SST dataset if the dataset exists. If **-f=recovery** fails to convert the item to a primary item, retry the command using **-f=offline_recovery** in place of **-f=recovery**. • If you do not have a TC XML meta file, use the form: `ensure_site_consistency -f=recovery -mode=auto -remote_site=`*replica_site* • If you have a TC XML meta file, use the option **-mode=min** or **-mode=full** with **-dir=***meta_file_directory*.
Inconsistent ownership replica	From the owning site, run **data_share** to resend the data.

Duplicate IDs

Problem	Solution
Duplicate Item ID or Key	Avoid the ID conflict during import by using the **item_rename** utility to rename the target site item.
Duplicate ItemRevision ID or Key	Avoid the ID conflict during import by using the **item_rename** utility to rename the target site item.
Inconsistent Item ID or Key	From the owning site, run **data_share** to resend the data.
Inconsistent ItemRevision ID or Key	From the owning site, run **data_share** to resend the data.

Object ownership

Problem	Solution
Object ownership error	Add the problem object UID to a UID list file named *uid.txt* and run the **tcxml_ownership_recovery** utility with the following form: `tcxml_ownership_recovery -inputuidfile=uid.txt -action=flip -targetsite=`*owning_site_id*

Monitor data exchange transactions

Monitor data exchange transactions

You can use **Data Exchange Transactions** to view and analyze your organization's history of Multi-Site and Briefcase transactions. Filter transactions based on completion status, exchange type, source and target sites involved, and other factors. With these transaction records, you can:

- Drill down through charts and graphs to quickly diagnose data exchange failures
- Use the broad view of your data exchange activities to better identify patterns of failure across multiple sites
- Analyze patterns and trends in data exchange usage to inform ongoing process improvements

The following types of transactions are recorded and reported.

Multi-Site

- Data shared and retrieved between sites using Active Workspace
- Remote export and import operations made using the rich client
- Exports and imports made using the **data_share** command
- Transactions made using the **data_sync** command

Briefcase

All Briefcase import and export transactions involving the site as a source or a target, whether they are run from:

- Active Workspace
- Rich Client

- The command line

Bulk data exchanges and PLM XML transactions are not recorded.

Configuring data exchange transaction monitoring

Configure the following aspects of gathering and displaying your organization's data exchange transaction records.

Specify transactions to monitor

You can configure your site to record Multi-Site, Briefcase, or both types of data exchange transactions originating at a site. Use the **TXN_Supported_Application_Types** preference to specify which data sharing transactions are recorded and reported. Set the preference to a value of **Briefcase**, **Multisite**, or both values depending on the types of data sharing transactions you want to record.

Specify a central site for monitoring transactions

By default, all transactions started from a site are recorded and can be viewed only when logged onto that site. Alternatively, several sites can send their transaction records to a common site for consolidated viewing of the organization's data exchange transactions at that common site.

To use a common site to view transaction records, on each of the remote sites set the **TXN_Central_Site** preference to the **Site Name** value of the common site.

Change the period of reported transaction records

By default, a site's transaction records for the previous 30 days are reported. Change the default number of days to report by updating the value of the **TXN_history_range** preference.

Clear data from the transaction history

Transaction records remain in a site's history until they are manually removed. To delete records from a site's history, log onto the site, open a command window, and run the **transaction_monitor** utility. (See **transaction_monitor** for more details on the utility.) For example:

Delete records in a date range

Use a command of the following form to delete all transaction records up to a certain date:

```
transaction_monitor -u=youruserid -p=yourpw -f=delete -from="2010-01-01
01:00:00" -to="2021-09-30 24:59:59"
```

Delete records of successful transactions in a date range

Use a command of the following form to delete all successful transaction records that occurred in a certain time period:

```
transaction_monitor -u=youruserid -p=yourpw -f=delete
-final_status=Success -from="2021-09-30 16:20:00"-to="2021-10-15
13:00:00"
```

Viewing data exchange transaction records

When you log on to Active Workspace as an administrator, the **Data Exchange Transactions** tile is available on the Active Admin workspace home page.

By default, records for only those data transactions originating at your site are displayed. Your site may be configured to **view transactions originating at other sites**, too.

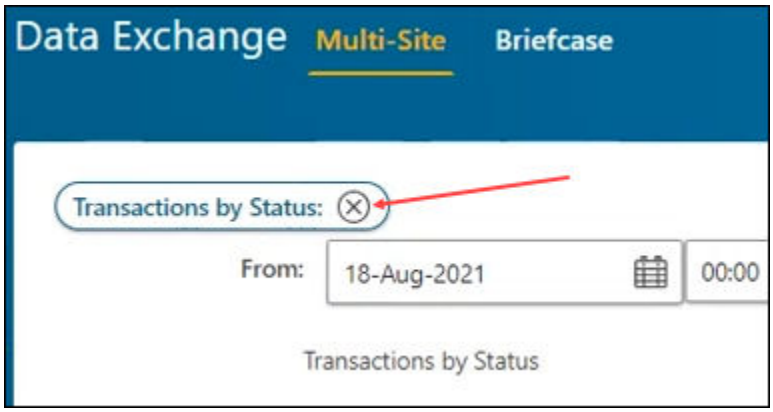
View transaction records

Click the **Multi-Site** or **Briefcase** tab to view transaction records for your site's recorded transactions. (Depending on **your site's configuration**, the tabs available may vary.)

Several graphs summarizing data exchanges originating at your site are displayed. Summaries are organized by status, type, and involved sites.

Below the graphs, the transaction records for the site are listed. Open any of the records in the list to view additional details about the record, such as the source and target sites, transaction type, objects involved in the transaction, any reported errors, date and time of the transaction, and locations of related log files.

Click one or more bar graphs or chart segments to refine the list of transaction records to those selections. Remove filters at any time by closing the selected filter.



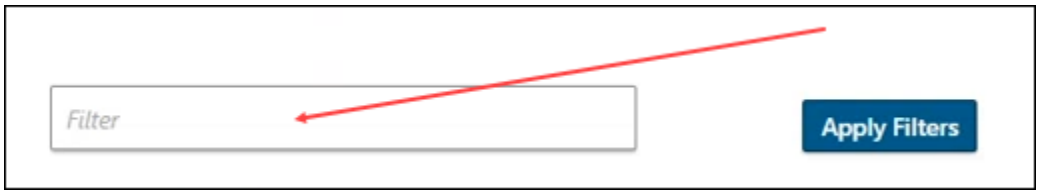
Filter transaction records by date range

Specify a different date range from which to view transaction records by entering **From** and **To** values and clicking **Apply Filters**. The record list is updated to show transactions from the new date range.

By default, the transaction records for the previous 30 days are reported.

Filter transaction records by ID

Enter a value in the **Filter** field and click **Apply Filters** to refine the reported records to only those objects with IDs containing the value and to records with Briefcase file names containing the value.



Share bulk data

Bulk loading product data

Active Workspace provides tools to extract data from one Teamcenter environment to copy to another. You would typically use these tools when testing Teamcenter upgrades and customizations in test environments.

When creating a test environment, you may need to duplicate large amounts of data from a production environment in the test environment. Doing so delivers a test environment with an applicable, broad set of data with which to test customizations and updated software.

Requirements

You must be logged on as a user with administration privileges to use the bulk extract and copy tools.

To bulk copy product data into a site, the site must be designated as a test site. You can designate a site as a test site when installing it. You can also use the **install** utility with the **-mark_as_test_env** argument to convert a site created as a production environment to a test environment.

Copying product data from your production environment

Use the following steps to copy data from a production environment to a Briefcase file that can be loaded into a test environment.

1. Log on to Active Workspace with administrative privileges and select one or more items, assemblies, or folders as root objects to copy.

2. Click **Share** > **Bulk Extract** to display the **Bulk Extract** panel.

3. Select the transfer option set to use when copying the objects. (Only unconfigured transfer option sets are available.)

4. Accept the default file Briefcase file name or update it as necessary.

5. Click **Override Options** and review the default settings for extracting the data. Update the options as necessary and click **Override**.

6. Click **Extract** to begin copying the objects to the Briefcase file. You receive an alert when it is complete.

Review the report and transfer the Briefcase file

You receive a report alert when the Briefcase file is created. Click on the alert to view the report. Access all recent alerts from the **Subscription** tile.

- The **Properties** section of the report includes details such as a list of the user extracting the data and the transfer option set used. Under **Related Objects**, click on the export log entry to view additional details, including a complete list of the objects extracted.

- The **Target Object** section of the report contains a link to the Briefcase file containing the extracted objects. Select the Briefcase file and click **View** > **Load Briefcase** to review the contents of the file.

Download the file and save it to a location accessible by the test site.

Copying product data into your test environment

Use the following steps to load data copied from a Teamcenter production environment into a test environment.

To bulk copy product data into a site, the site must be designated as a test site. You can designate a site as a test site when installing it. You can also use the **install** utility with the **-mark_as_test_env** argument to convert a site created as a production environment to a test environment.

1. Log on to Active Workspace with administrative privileges and select the folder into which the root objects will be copied.

2. Click **New** > **Bulk Copy** to display the **Bulk Copy** panel.

3. Use **Choose File** to locate the Briefcase file containing the data to copy.

4. Select the transfer option set to use when importing the file. Override any options as necessary.

5. Click **Bulk Copy** to import the objects in the Briefcase file. You receive an alert when the import run is complete.

6. Review the selected folder for the imported objects.

> Note:
>
> If you are using Active Workspace with a version of Teamcenter earlier than 13.2 when copying the data from the Teamcenter production environment or to the test environment, the root objects will not be copied to the selected folder. You must search the Teamcenter database for the copied data.

Review the import report

You receive a report alert when the copying completes. Click on the alert to view the report. (Access all recent alerts from the **Subscription** tile.)

The folder into which you copied the data is listed under **Related Objects** in the **Properties** section of the report. Under **Target Object**, download the import log, which includes details such as a list of the objects copied and the transfer option set used.

6. Logging

Monitoring your system

You can use several types of logging to monitor the activities of Teamcenter processes and objects.

Audit logs

Audit logs track the activities performed on selected data model objects. This provides a tracking mechanism for any changes made to those objects for historical record. To use audit logs, they must be **enabled and configured**.

Core Teamcenter logs

These process log files contain diagnostic information for the core foundation of Teamcenter which is described in the Teamcenter *System Administration* topic *Teamcenter Logging*.

Microservice logs

These process log files contain diagnostic information for the logs from the microservices. If your microservices are distributed, consider installing the **Log Aggregator**.

Configuring the Audit Logs page

Audit Logs page configuration tasks

What are audit log types?

In Teamcenter, the following audit log types hold audit records based on logical groupings of object type and event type combinations:

- General logs
- License export logs
- Organization logs
- Security logs
- Schedule logs
- Structure logs

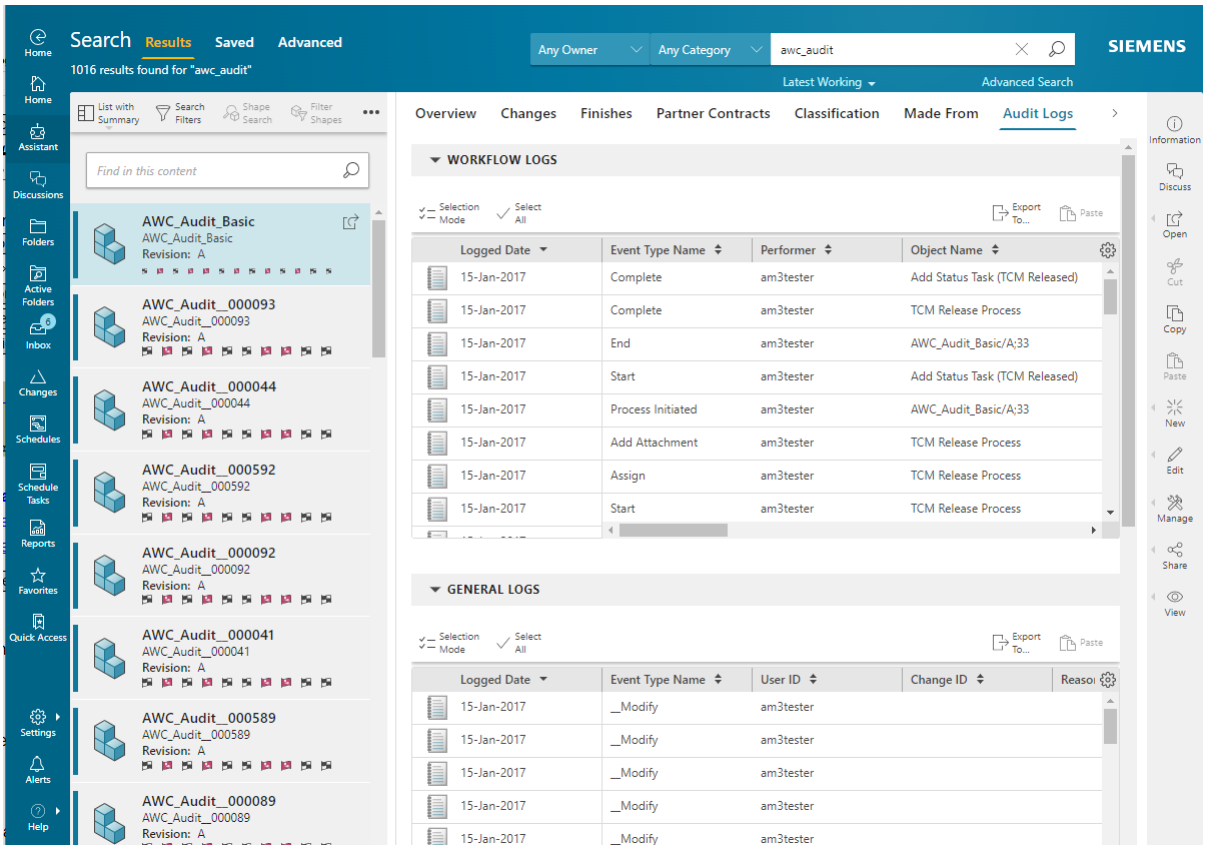
- Workflow logs

What is an audit log dataset?

An audit log dataset is a stylesheet configuration representing applicable audit log types for a context object. The **Audit Logs** tab in Active Workspace provides a segregated view of audit logs in different sections. As a system administrator, you can create and configure audit log datasets.

What do audit logs look like?

As a **DBA** user, you can view audit logs using the **Audit Logs** tab in Active Workspace.



What must I install to enable the audit log feature?

To enable the audit log feature, you must install the Audit feature during your Active Workspace installation using Teamcenter Environment Manager (TEM).

What can I configure?

You can configure the following aspects of audit logs:

- **Activate the Audit Log page.**

- **Customize which audit log fields appear to users.**
- **Customize which audit logs appear to users.**

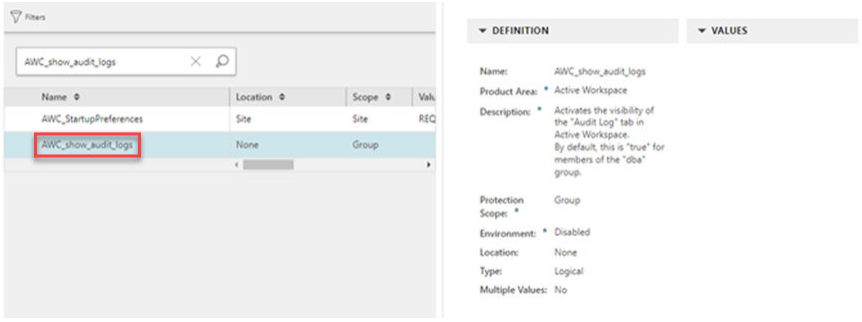
Where can I find out more about audit logs?

See *Audit Manager* in the Teamcenter documentation.

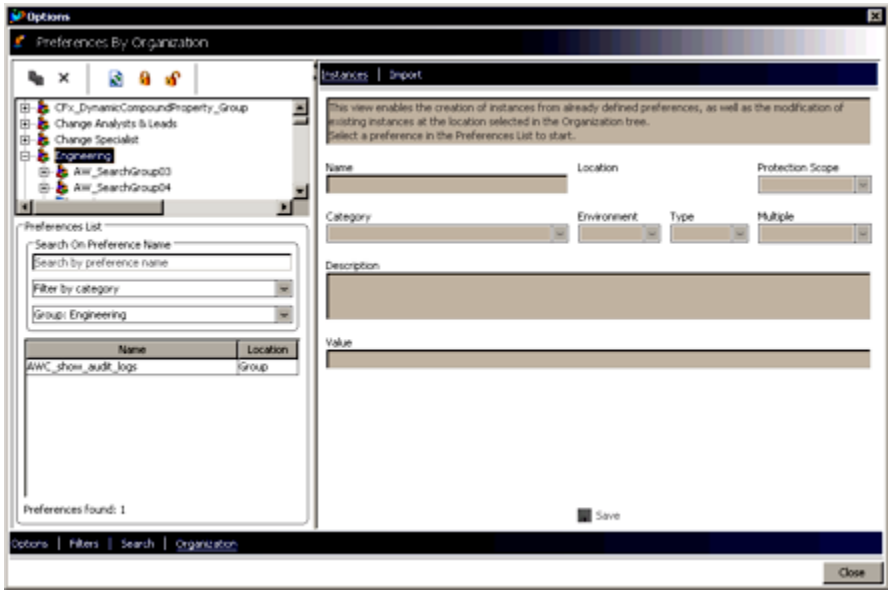
Activate the Audit Log page

Set the **AWC_show_audit_logs** preference to activate the **Audit Log** tab in Active Workspace. By default, the value is **true** for the **dba** group. As a **DBA** user, you can set the preference for specific groups, roles, and users from:

- Active Workspace using the **PREFERENCES** tile.



- The rich client **Options** dialog box **Preferences By Organization** pane.



For more information, see the *Using Teamcenter preferences* video in the Teamcenter documentation.

- The **preferences_manager** utility.

  For more information, see the *Utilities Reference* in the Teamcenter documentation.

Customize audit logs field display

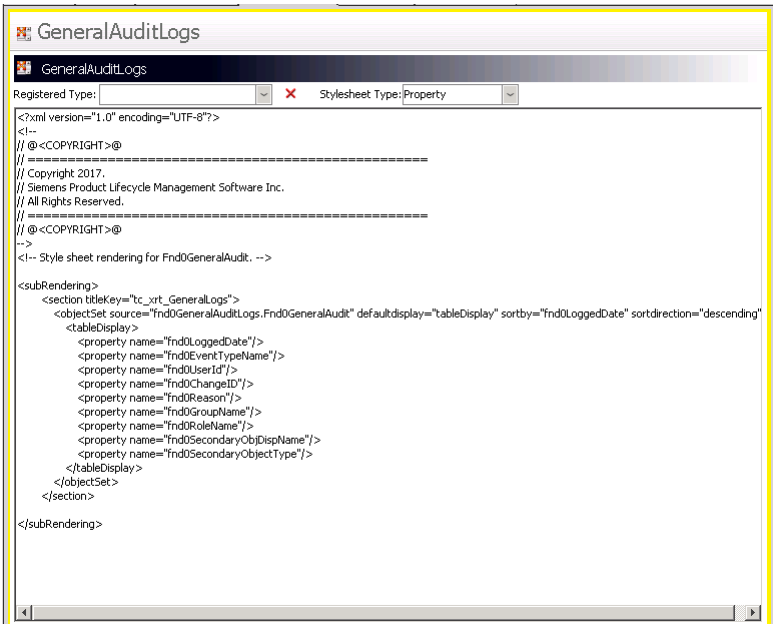
You can customize which fields are displayed in each audit log. For example, by default the **General Logs** audit log displays the following fields:

- **Logged Date**
- **Event Type Name**
- **User ID**
- **Change ID**
- **Reason**
- **Group Name**
- **Role Name**
- **Secondary Object Display Name**
- **Secondary Object Type**

To remove a field from the display:

- In Active Workspace, you can use the **Arrange** panel to reorder, hide, or display columns.
- In Teamcenter, perform the following:

  1. In the rich client, search for the audit log file you want to edit. For example, select the **GeneralAuditLogs** file to remove a field name in the **General Logs** audit log.

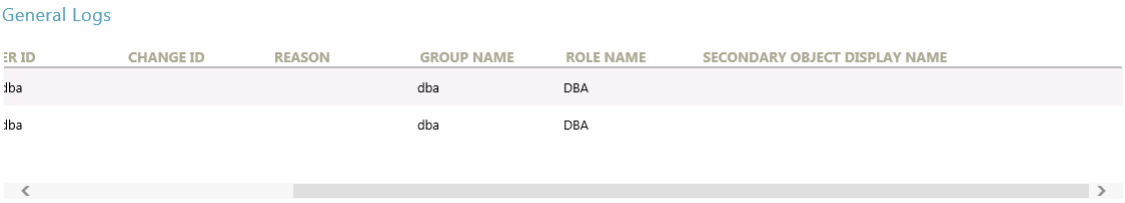


2. Delete the line associated with the field you want to remove. For example, delete the following line to remove the **Secondary Object Type** field:

```
<property name="fnd0SecondaryObjectType"/>
```

3. Save the **GeneralAuditLogs** file.

4. Using Active Workspace, verify the **Secondary Object Type** field was successfully removed.



Using audit logs

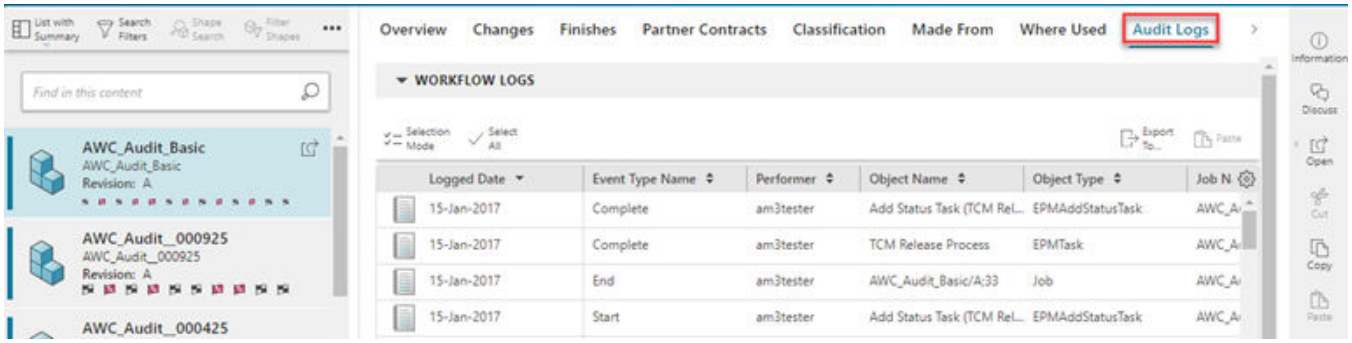
System administrators use Audit Manager to create audit logs. Audit logs track what information has changed and who has changed the information.

> Note:
>
> Your administrator must enable the **Audit Logs** page for Active Workspace. Also, you must have administrative privileges or you must be granted privileges to view audit logs.

In Active Workspace, you can view the following audit logs:

- **Audit - General Report**
- **Audit - General Sponsored Authentication Report**
- **Audit - File Access Read-Write Report**
- **Audit - File Access Report**
- **Audit - File Access Sponsored Authentication Report**
- **Audit - Security Report**
- **Audit - Schedule Report**
- **Audit - Organization Report**
- **Audit - Digital Signature Report**
- **Audit - License Change Report**
- **Audit - License Export Report**
- **Audit - License Export Sponsored Authentication Report**
- **Audit - License Change Sponsored Authentication Report**
- **Audit - Organization Sponsored Authentication Report**
- **Audit - Structure Sponsored Authentication Report**
- **Audit - Workflow Detailed Report**
- **Audit - Workflow Summary Report**
- **Audit - Workflow Attachment Report**
- **Audit - Workflow Signoff Report**

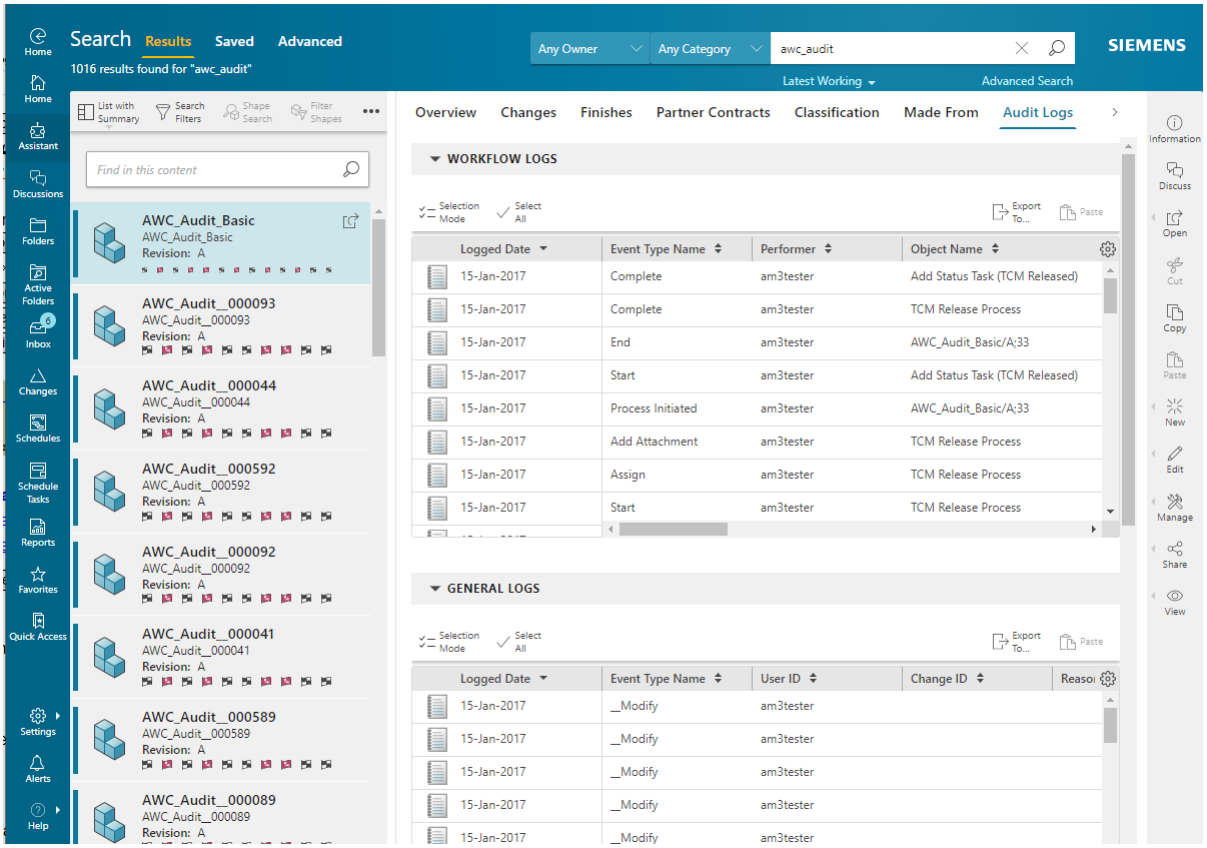
You can view audit logs using the **Audit Logs** tab in Active Workspace.



Customize the audit log display

By default, the following four audit logs are viewable in Active Workspace for **Item**, **ItemRevision**, and its subtype:

- **Workflow Logs**
- **General Logs**
- **License Export Logs**
- **Structure Logs**



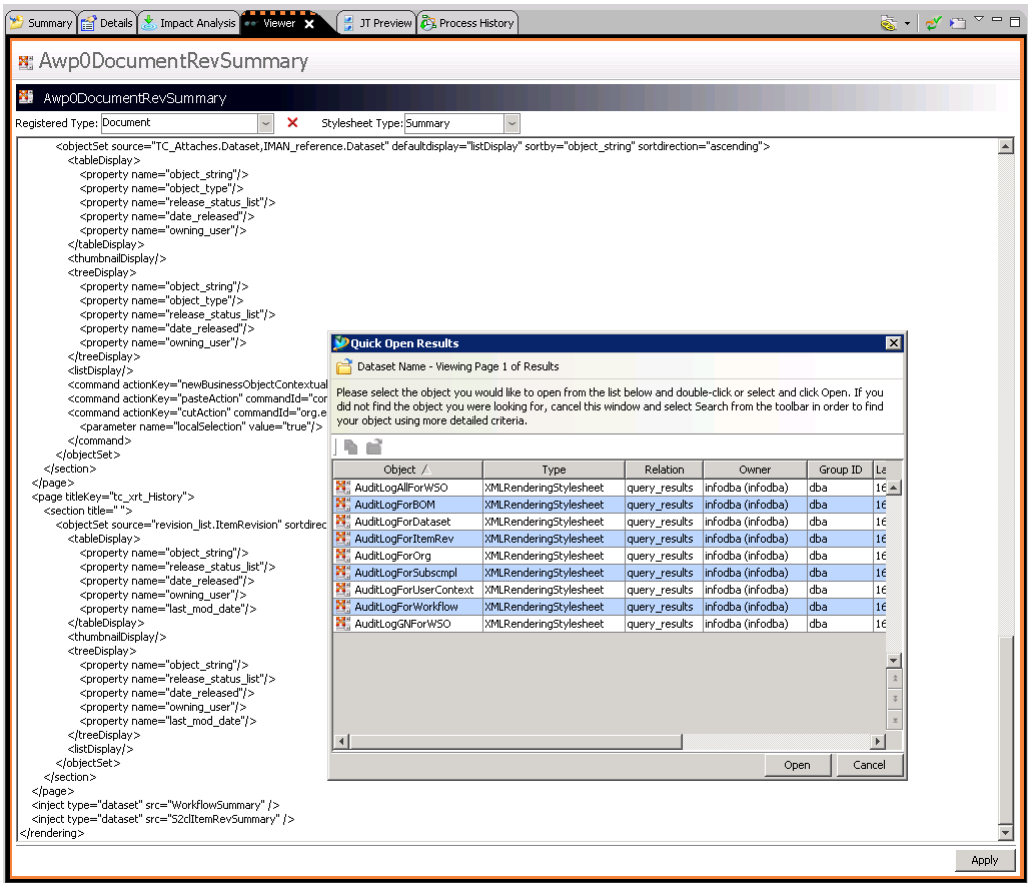
You can customize which audit logs are displayed to users by adding or removing audit logs to customize your XRT pages.

Following is a table that shows the audit dataset for the associated object type.

Object type	Audit dataset
Item/ItemRev and its subtype	**AuditLogForItemRev**
Workspace object	**AuditLogAllForWSO**
BOMLine	**AuditLogForBOM**
Form/Folder/WSO	**AuditLogGNForWSO**
Dataset	**AuditLogForDataset**
User/Group/Project	**AuditLogForUserContext**
GroupMember/Person/ Role/Site/Volume/ TCCalendar	**AuditLogForOrg**
Schedule, ScheduleTask	**AuditLogForSchedule**
SchDeliverable/SchTaskDeliverable/ ScheduleMember	**AuditLogForScheduleMgmt**
EPMJob/EPMTask/ PerformSignoffTask	**AuditLogForWorkflow**
Scp0Regulation/ Scp0SubstanceCmplResult/ Scp0Exemption/ Mat1Substance	**AuditLogForSubscmpl**

To customize which audit logs can be viewed:

1. Open the XRT page that you want to modify, for example, **Awp0DocumentRevSummary**, and add the audit log to your custom XRT page by inserting an **inject** statement for the audit log you want to add.



2. Save the file with a new name.

> Note:
>
> Siemens Digital Industries Software recommends you rename your edited file before saving changes to retain the default file.

Aggregating microservice logs

Microservice log aggregation

In a typical deployment, Teamcenter microservices are distributed across multiple machines. For a particular transaction or operation, microservices across the deployment could be involved, including separate instances of a given microservice on multiple machines. If a failure occurs, part of the investigation may require reviewing multiple microservice logs to find the root cause of the issue.

Log aggregation eliminates the need to manually fetch and inspect each log on each machine in the deployment. A log forwarder on each microservice node forwards logs to a log aggregator for collection in a single location, either in a consolidated file or preferably an Elasticsearch endpoint. In this single location, administrators can search for messages of certain error levels or for messages with a matching correlation ID.

General Teamcenter logging is described in the Teamcenter *System Administration* topic *Teamcenter Logging*.

Install the microservice log aggregator

Use Deployment Center to install the microservice log aggregator. The log aggregator cannot be installed using Teamcenter Environment Manager (TEM).

1. Download the microservice framework install kit and place it in the Deployment Center repository.

2. Open Deployment Center to the environment where you want to install the log aggregator.

3. On the **Applications** panel, add the **Teamcenter Microservice Framework** and **Aggregated Logging** applications.

4. On the **Components** panel, configure the **Log Aggregator** component.

For this property	Do this
Installation Path	Enter the location on the host machine where the **Log Aggregator** must be installed.
Machine Name	Enter the name of the machine where the **Log Aggregator** must be installed. Include the domain in the name. Note that on Linux hosts, a Docker placement constraint is set so that the aggregator continues running on that exact node in the swarm.
OS	Choose the operating system that is installed on the host, either **Windows** or **Linux**.
Type and **Aggregator Port** (for Windows hosts)	To ensure high availability of log aggregation, you can add multiple **Log Aggregator** component instances. Each instance is installed on the node identified in its **Machine Name** parameter. One instance of the Log Aggregator component must be set to **Type=active**. Other instances must be set to **backup**. Set **Aggregator Port** to the port number you want to use for this instance of the log aggregator. You can specify any open port number.
Output Logs to:	Choose the destination for the aggregated logs, either **ElasticSearch** or **File**. **ElasticSearch** Copies the log files to your Elasticsearch endpoint (Elasticsearch version 7.x is recommended). If you choose **ElasticSearch**, enter the settings for your Elasticsearch endpoint: **Host** - The server where Elasticsearch is deployed. **Port** - The port for Elasticsearch traffic on the server where Elasticsearch is deployed.

For this property	Do this
	If Elasticsearch traffic requires authentication, select the **Requires Authentication** checkbox and enter the authorized **Username** and **Password**. **File** Collects all logs in a single file with the naming pattern **tc_aggregated_logs***. A new log file is started daily. All aggregators in the deployment must be able to write to the same physical disk, which can be a network share or mount point. When the destination file is on a Linux host, a mount point is created in the Docker stack for writing logs into the machine's file system. To enable writing the logs, enter the **User ID** and **Group** values for the user account under which the aggregator container will run. To obtain these values, log on to the aggregator host machine using that account and issue the **id -u** and **id -g** commands. On Windows hosts, in **Aggregated Log Path**, enter the location for the aggregated log.

5. Configure the **Microservice Node** as described for the host operating system, either Linux or Windows.

6. Generate deployment scripts as you would for any Deployment Center install procedure, and install the log aggregator on the target host machine.

Once the Deployment Center scripts have been deployed, perform the following platform-specific steps on the target host machine.

> Note:
>
> If authentication is required for Elasticsearch traffic, the credentials are stored unencrypted in a Fluentd configuration file. This is a limitation of the Fluentd plugin. To secure the password, set appropriate file system access controls on the file or control access to the machine. On Windows, the file is *[TC_ROOT]\tc_logging_aggregator\config \aggregator.conf*. On Linux, the file is *[MSF INSTALL]/container/logging_configuration/fluent_aggregator.conf* .

Windows

No additional steps are needed. By default, log aggregation services start automatically. The services are named **Teamcenter Logging Aggregator** (if deployed on the node) and **Teamcenter Logging Forwarder** (all nodes).

Linux

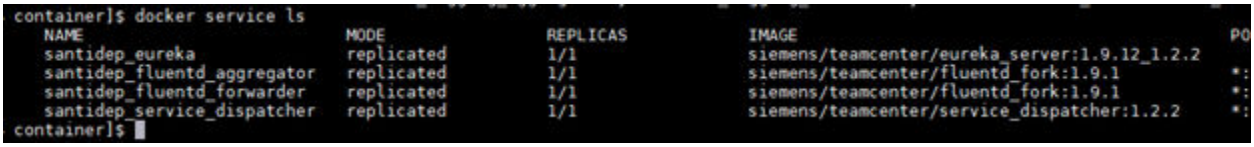
1. On the master node, launch a command prompt.

2. Change the directory to **\containers** and run the following commands:

   docker stack deploy -c tc_microservice_framework.yml mystack
   docker stack deploy -c tc_logging_aggregator.yml mystack
   docker stack deploy -c tc_logging_forwarder.yml mystack

3. To verify that all services are running, run the command **docker service ls**.

   The output of the command should show all the services running.



View aggregated logs

Depending on how the log aggregator was defined in Deployment Center, you can view the aggregated logs either in one file or from an Elasticsearch database.

File-based aggregated logs

Logs are periodically collected in a single file with the naming pattern **file tc_aggregated_logs***. A new log file is started daily. You can view the logs with any text file viewer.

For nodes on Linux, a mount point is created in the log aggregation container on the machine where the log aggregator is installed, and the logs are written there.

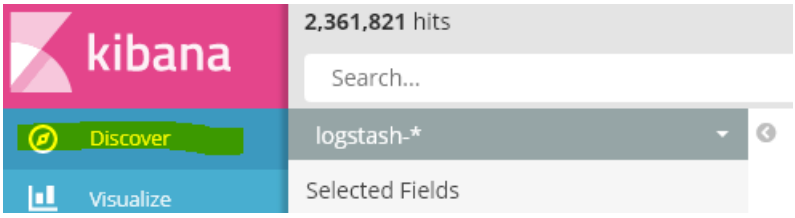
For nodes on Windows, the logs are located in the **Aggregated Log Path** location defined in Deployment Center.

Elasticsearch aggregated logs

Logs are copied to an Elasticsearch endpoint. Typically, this endpoint is part of an Elastic (ELK) Stack, and the logs can be searched using Kibana. Following is an example of how logs might be viewed. The example briefly shows how things work. It is not a tutorial on how to use Kibana.

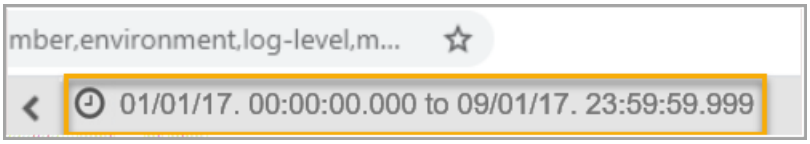
1. Navigate to the Kibana installation.

2. Click **Discover**.



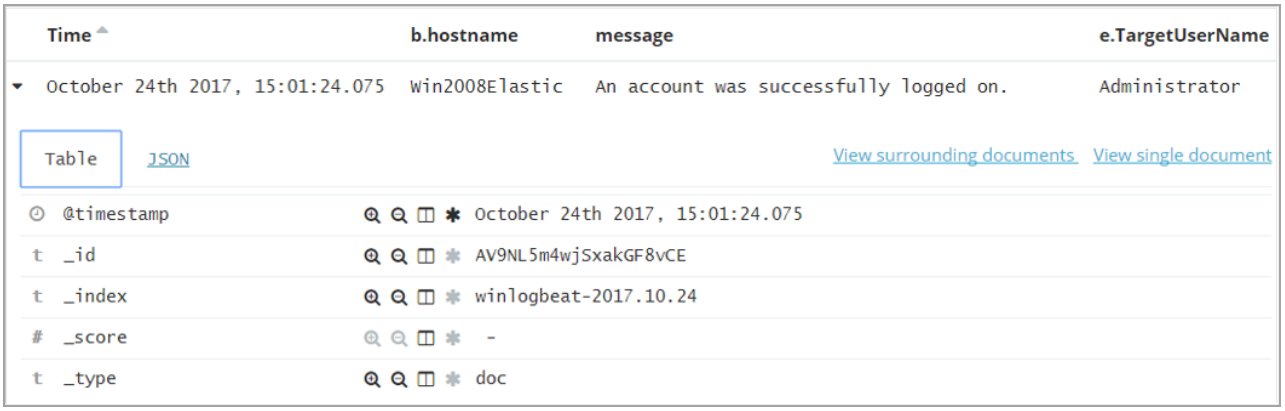
3. Change the time range.

   a. In the toolbar, click the time range section.



   b. Click **Quick** and choose **Last 15 minutes** or the range you prefer.

4. View your logs for the time range. The following example shows a parsed log line.



Enable TLS for log aggregation

You can enable Transport Layer Security (TLS) for the log aggregation solution. Log aggregation makes use of Fluentd and Fluentd plugins. Detailed configuration steps for enabling TLS are described in the Fluentd documentation. The Fluentd documentation is available at https://docs.fluentd.org.

Configure TLS between the log aggregator and the log forwarder

1. Generate a self-signed certificate, following the Fluentd documentation for how to enable TLS encryption for the **forward** input plugin.

   Keep track of the password. You will use it later during configuration.

2. Save the certificate to a location that can be referenced by the log aggregation configuration.

   Example:

   ```
   C:\TR\tc_logging_aggregator\certs\fluentd.crt
   ```

3. On microservice framework nodes where the log aggregator runs, enable TLS mutual authentication by modifying the log aggregator configuration file as described in the Fluentd documentation for the **forward** input plugin.

   The location and name of the aggregator configuration file depends on the node operating system:

Node OS	Location and name of aggregator configuration file
Linux	`/container/logging_configuration/fluentd_aggregator.conf`
Windows	`<installation>\tc_logging_aggregator\config\aggregator.conf`

   Example:

   ```
   <source>
     @type forward
     port 24224
     bind "vc6s004"
     <transport tls>
       cert_path C:\TR\tc_logging_aggregator\certs\fluentd.crt
       private_key_path C:\TR\tc_logging_aggregator\certs\fluentd.key
       private_key_passphrase MyPassword12345
     </transport>
   </source>
   ```

4. Restart the log aggregator.

   Linux

   Stop and restart the logging container.

   a. To identify the log aggregator service in the running stack, run the command:

```
docker service ls
```

The aggregator service will include the name "fluentd_aggregator".

```
TC_MS_STACK_fluentd_aggregator
```

b. To remove the aggregator service from the stack, run the command:

```
docker service rm <log_aggregator_service>
```

c. To restart the log aggregator service with the new config file, run the command:

```
docker stack deploy -c tc_logging_aggregator.yml <stack_name>
```

Windows

On Windows nodes where you modified the aggregator configuration file, in the Windows services application, stop and restart the **Teamcenter_Log_Aggregator** service.

5. On all nodes, to connect to a TLS SSL-enabled server, modify the forwarder configuration file as described in the Fluentd documentation for the **forward** input plugin.

The location and name of the forwarder configuration file depends on the node operating system:

Node OS	Aggregator configuration file
Windows	`<installation>\tc_logging_forwarder\config\forwarder.conf`
Linux	`/container/logging_configuration/fluentd_forwarder.conf`

Example:

```
<match **>
      @type forward
      send_timeout 60s
      recover_wait 10s
      hard_timeout 60s
      transport tls
      tls_cert_path C:\TR\tc_logging_aggregator\certs\fluentd.crt
      tls_verify_hostname false

      #
      # The below include defines all the aggregator
      # servers.
      #
```

```
      @include ./servers/*.conf
</match>
```

6. Restart the log forwarder.

Linux

Stop and restart the forwarder container.

a. To identify the log forwarder service in the running stack, issue the command:

```
docker service ls
```

The forwarder service will include the name "fluentd_forwarder".

```
TC_MS_STACK_fluentd_forwarder
```

b. To remove the forwarder service from the stack, issue the command:

```
docker service rm <log_forwarder_service>
```

c. To restart the log forwarder service with the new config file, issue the command:

```
docker stack deploy -c tc_logging_forwarder.yml <stack_name>
```

Windows

On Windows nodes where you modified the aggregator configuration file, in the Windows services application, stop and restart the **Teamcenter_Log_Forwarder** service.

Configure HTTPS/TLS from the aggregator to an Elasticsearch server

To configure HTTPS/TLS from the aggregator to your Elasticsearch server, refer to the Fluentd documentation for the output plugin **elasticsearch**. The *elasticsearch* plugin is included with the microservice framework kit.

Aggregate syslogs

When you configure log aggregation for a Teamcenter environment, deployment scripts install log forwarder software on every corporate server in the environment. However, forwarding of server system log (syslog) files is disabled by default. This is because syslog files can be very large. Copying the logs across a network can create a large traffic load, and searching aggregated logs is practical only when aggregation is to an Elasticsearch endpoint.

Depending on the corporate server operating system, use the following procedures to enable the aggregation of syslog files.

Enable syslog aggregation - Windows

1. On the Teamcenter corporate server whose syslog you want to aggregate, in the file *Program Files\Siemens\tc_logging_forwarder\config\sources\tcserver.conf*, remove the comment **#ENABLE_TCSERVER#** from all lines.

Example:

```
#####################################################################
# Source Input - TCServer syslogs
#####################################################################
#Uncomment lines below to enable TC syslog aggregation
#ENABLE_TCSERVER#<source>
#ENABLE_TCSERVER#  @type tail
#ENABLE_TCSERVER#
#ENABLE_TCSERVER#  #
#ENABLE_TCSERVER#  # The below path may be updated to the location
of
#ENABLE_TCSERVER#  # tcserver syslogs, if changed from default.
#ENABLE_TCSERVER#  #
#ENABLE_TCSERVER#  path C:/temp/*tcserver*.syslog
#ENABLE_TCSERVER#  pos_file C:/temp/fluentd-tcserver.syslog.pos
#ENABLE_TCSERVER#  read_from_head true
#ENABLE_TCSERVER#  path_key log_file
#ENABLE_TCSERVER#  <parse>
#ENABLE_TCSERVER#       @type none
#ENABLE_TCSERVER#  </parse>
#ENABLE_TCSERVER#
#ENABLE_TCSERVER#  #Prefix with the parser type to use
#ENABLE_TCSERVER#  tag mld.*
#ENABLE_TCSERVER#</source>
```

must become

```
#####################################################################
#
# Source Input - TCServer syslogs
#####################################################################
#
#Uncomment lines below to enable TC syslog aggregation
<source>
  @type tail

  #
  # The below path may be updated to the location of
  # tcserver syslogs, if changed from default.
  #
  path C:/temp/*tcserver*.syslog
```

```
    pos_file C:/temp/fluentd-tcserver.syslog.pos
    read_from_head true
    path_key log_file
    <parse>
          @type none
    </parse>

    #Prefix with the parser type to use
    tag mld.*
  </source>
```

2. In the Windows services application, stop and then restart the log forwarder service **Teamcenter Logging Forwarder**.

Enable syslog aggregation - Linux

Constraints for Docker swarm configuration:

- Docker must be installed on the corporate server.
- For high availability and ease of administration, best practice is to join all corporate server hosts to the same Docker swarm.

1. On every Teamcenter corporate server, start Docker. Docker may already be started if the corporate server is also a microservice node.

   To start Docker, run this command:[1]

   ```
   docker swarm init
   ```

   The output of the command is similar to the following:

   ```
   Swarm initialized: current node (lccilqci5tpvy6xmsjlu8gap3) is now a manager.

   To add a worker to this swarm, run the following command:

       docker swarm join --token SWMTKN-1-26h1be2gk2kozzecvgkw93smho5ueb7azn8uw1j2079
   isc8b25-dfc8r1f6qhh50ev250tb4st9r 192.168.0.8:237
   ```

1 If the host is a virtual machine, then Docker may have trouble identifying the physical IP address of the hardware. In that case, run the command with the switch and parameter `--advertise-addr <machine IP address>` to supply the physical IP address. For example, `docker swarm init --advertise-addr 123.123.123.123`

> Tip:
>
> If this is the master node and you intend to later join other nodes to this swarm as workers, save the output command string for later use.

Once you have started Docker on a node, you can join the node to a running swarm.

2. To determine if the Docker Fluentd image needs to be loaded, run the command:

   ```
   docker image ls
   ```

   and search the response to see whether "siemens/teamcenter/fluentd_service" image, version "1.9.1" is loaded.

3. If the Docker Fluentd image is not loaded, issue the following commands:

   ```
   cd $TC_ROOT/container
   docker image load -i fluentd_service-1.9.1.tar
   ```

4. If the log aggregator microservice is not running in the same Docker swarm:

   In the file *$TC_ROOT/containers/logging_configuration/master_servers.conf*, change the **host fluentd_aggregator** entry to the fully qualified domain name or IP address of the aggregator.

   Example:

   ```
   <server>
           name fluentd_aggregator
           host fluentd_aggregator
           port 24224
           weight 60

   </server>
   ```

   must become

   ```
   <server>
           name fluentd_aggregator
           host 123.456.78.9
           port 24224
           weight 60

   </server>
   ```

5. In the file *$TC_ROOT/containers/logging_configuration/sources/master/master_sources.conf*, remove the comment **#ENABLE_TCSERVER#** from all lines.

Example:

```
#####################################################################
# Source Input - TCServer syslogs
#####################################################################
#Uncomment lines below to enable TC syslog aggregation
#ENABLE_TCSERVER#<source>
#ENABLE_TCSERVER#  @type tail
#ENABLE_TCSERVER#
#ENABLE_TCSERVER#  #
#ENABLE_TCSERVER#  # The below path may be updated to the location
of
#ENABLE_TCSERVER#  # tcserver syslogs, if changed from default.
#ENABLE_TCSERVER#  #
#ENABLE_TCSERVER#  path /tmp/*tcserver*.syslog
#ENABLE_TCSERVER#  pos_file /tmp/fluentd-tcserver.syslog.pos
#ENABLE_TCSERVER#  read_from_head true
#ENABLE_TCSERVER#  path_key log_file
#ENABLE_TCSERVER#  <parse>
#ENABLE_TCSERVER#       @type none
#ENABLE_TCSERVER#  </parse>
#ENABLE_TCSERVER#
#ENABLE_TCSERVER#  #Prefix with the parser type to use
#ENABLE_TCSERVER#  tag mld.*
#ENABLE_TCSERVER#</source>
```

must become

```
#####################################################################
#
# Source Input - TCServer syslogs
#####################################################################
#
#Uncomment lines below to enable TC syslog aggregation
<source>
  @type tail

  #
  # The below path may be updated to the location of
  # tcserver syslogs, if changed from default.
  #
  path /tmp/*tcserver*.syslog
  pos_file /tmp/fluentd-tcserver.syslog.pos
  read_from_head true
  path_key log_file
  <parse>
        @type none
```

```
    </parse>

    #Prefix with the parser type to use
    tag mld.*
  </source>
```

6. To deploy the log forwarder to the stack, change the directory to **\containers** and run the command:

   ```
   docker stack deploy -c tc_logging_forwarder.yml mystack
   ```

7. To verify that the forwarder service is running, run the command **docker service ls**.

   The output of the command should show all services running, including at least the forwarder.

7. Assistant configuration

Assistant configuration tasks

What is the Assistant?

The Assistant suggests the next possible actions to perform and provides the relevant data required to perform them. These suggestions are based on the context, history, and usage frequency of actions performed by other previous users belonging to the same role and group.

What can I configure?

You can **configure the Assistant panel** using the provided site and user preferences.

What do I need to do before configuring?

Before you can configure the **Assistant** panel, you must **install the features and the microservice**. Install the following from the **Features** panel of Teamcenter Environment Manager (TEM):

- **Assistant** (server)

  Installs the server-side definitions for the Assistant.

  Select the **Active Workspace→Server→Active Workspace Assistant** feature in the corporate server.

- **Assistant** (client)

  Installs the user interface elements for the Assistant.

  Select **Active Workspace→Client→Active Workspace Assistant**.

- **Command Prediction Services** (microservice)

  Installs the microservice for the Assistant.

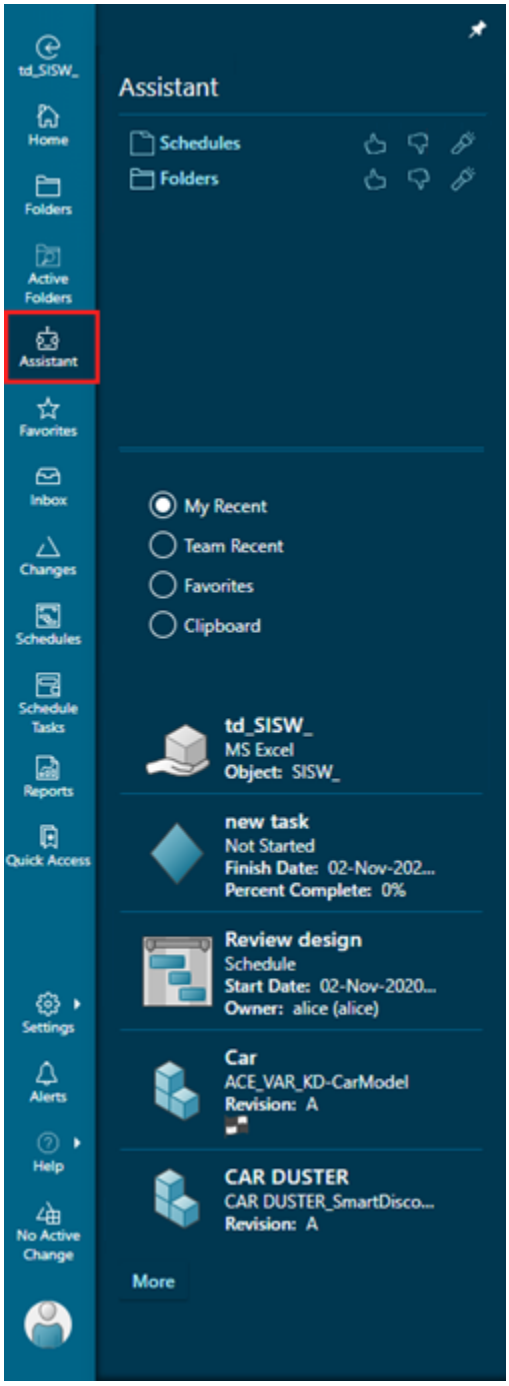
  Select **Microservices→Command Prediction Services**.

Where can I find out more about the Assistant?

See The Teamcenter Assistant in the help.

What does the Assistant panel look like?

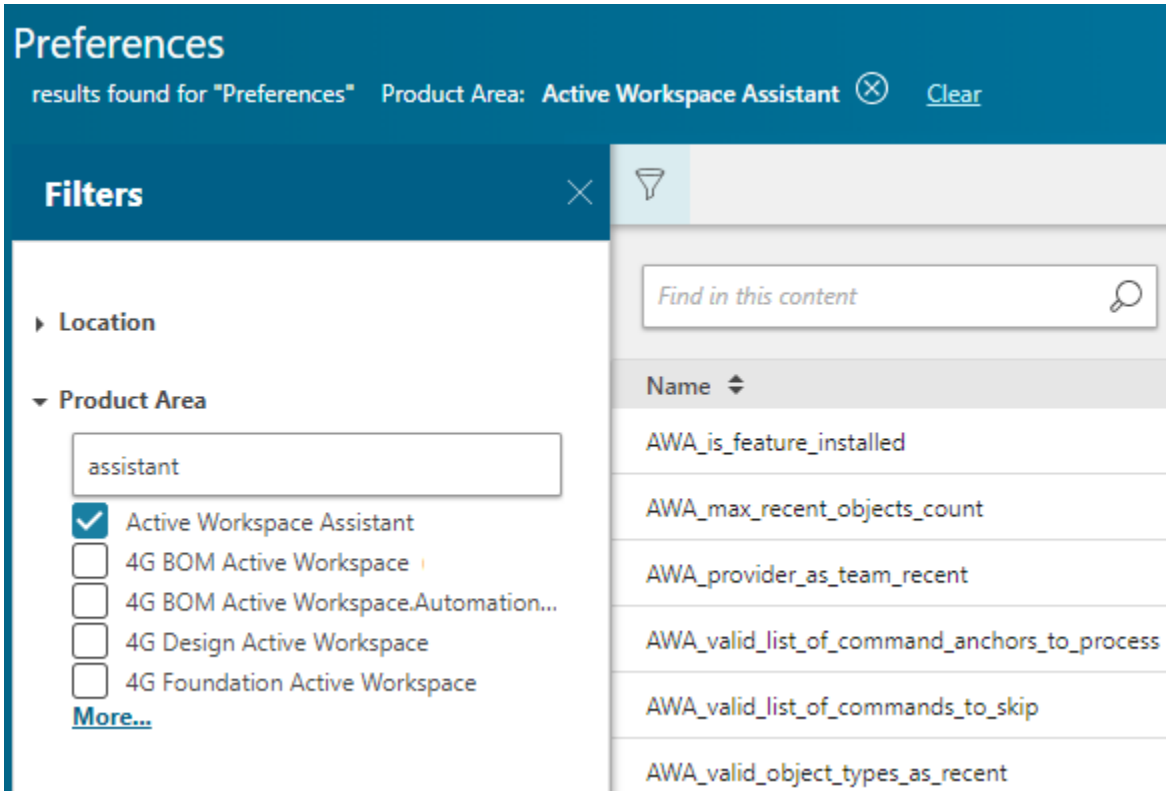
Following is an example of the **Assistant** panel in Active Workspace.



Configuring the Assistant panel

You can manage the settings for the **Assistant** panel using the provided site and user preferences. The availability of options such as **Like**, **Dislike**, **Show**, or **Tutor Mode** can also be configured using preferences.

Find the list and description of these preferences in the **Active Workspace Assistant** product area.



Where can I get a list of preferences?

Install the Assistant

The **Assistant** uses the **Command Prediction Service** microservice, which stores data in a dedicated database that you configure during installation.

This procedure assumes that Teamcenter and Active Workspace, including the microservice framework, are installed.

1. Ensure your environment includes the Teamcenter Foundation, Active Workspace, and Teamcenter Microservice Framework software.

   - Deployment Center

     - In the **Software** step, select these software kits.

   - TEM

     - In the **Media Locations** panel, specify locations of these software kits. If you use a minor release version of Teamcenter, make sure you include the major *and* minor release software kits.

2. Add the Assistant to your environment:

   - Deployment Center
     - In the **Applications** step, select the **Active Workspace Assistant** application.
     - In the **Components** step, select the **Command Prediction Service Configuration** component.
   - TEM
     - In your server *and* client configurations, add the corresponding server and client **Active Workspace Assistant** feature.
     - In your microservice framework configuration, add the **Command Prediction Service** microservice.

     For information about the TEM panels, in TEM, see the **Help** button

3. Complete the installation as appropriate for your installation tool.

Note:

- When you configure the database for the **Command Prediction Service** microservice, make sure you have the database system user credentials, and make sure you do not use the same tablespace as the Teamcenter database. The PredictiveUI user,database, and tablespace must be different from the Teamcenter and Server Manager database.

  If you choose to use an existing database for the **Command Prediction Service** microservice, make sure that you **manually create the database** before the installation.

- Due to the architectural changes in the Active Workspace client in Active Workspace 6.2 release, the command usage data required for the Teamcenter Assistant is not available and it has to be retrained. Active Workspace users will not be able to leverage the data that was created in releases prior to Active Workspace 6.2.

Manually create a database for the Command Prediction Service microservice

If you choose to use an existing database for the Command Prediction Service microservice, you must create the database using template scripts prior to install.

These scripts can be modified to create the database user, the tablespace, and the schema that includes the tables and indexes. Apart from changing tokens to appropriate values, and minor syntax changes, no other changes to the scripts are advisable.

Manually create an Oracle database for the Command Prediction Service microservice

1. Copy the template scripts from *<OS>\tc\microservices\commandprediction_service.zip\tc\db_scripts\<database>*.

2. Rename them as .sql files.

   Following SQL scripts must be used for on-premise Oracle database:

   - `oracle_create_predui.sql.template` - Use this script to create the base schema database.
   - `oracle_update_predui.sql.template` - Use this script to update the base schema database.

   Following SQL scripts must be used for cloud hosted Oracle database:

   - `oracle_rds_create_predui.sql.template` - Use this script to create the base schema database.
   - `oracle_update_predui.sql.template` - Use this script to update the base schema database.

3. Replace the tokens to appropriate values.

   The following table describes the database parameters to be replaced in the template. Additionally, the comments in the template file also indicate the values that must be replaced.

Parameter	Example value	Description
@TABLESPACE_NAME@	**predictivedb**	Name of the tablespace.
@DB_PATH@	**D:\oracle\data**	Path to the directory in which the data file will reside.
@DB_USER@	**predictivedbuser**	Database log in name for the Teamcenter database.
@DB_PWD@	**predictivedbpw**	The password for the database user.

4. Save the modifications to the scripts and execute them.

   If syntax errors occur while executing the database scripts, the following additional changes are required:

   - On the last line in the SQL script, delete one semicolon after END statement.
   - Make sure that the last line of the SQL script ends with the / character. If not, you must insert the / character on a new line after the last line of the script

The last two lines of the SQL script must appear as shown below:

```
;END;

/
```

> Note:
>
> For a complete database setup, it is necessary to execute both the *create* and *update* scripts after they are modified.

Manually create an MSSQL database for the Command Prediction Service microservice

1. Copy the appropriate template scripts from *<OS>\tc\microservices\commandprediction_service.zip\tc\db_scripts\<database>*.

2. Rename them as .sql files.

   The following SQL scripts must be used for the SQL Server database:

   - `mssql_create_predui.sql.template` - Use this script to create the base schema for the SQL Server database.

   - `mssql_update_predui.sql.template` - Use this script to update the base schema database.

3. Replace the tokens to appropriate values.

   For more information, see Create an SQL Server database (Windows) or Create an SQL Server database (Linux).

4. Save the modifications to the scripts and execute them.

   - To execute the script on the command line, enter the following:

     ```
     > sqlcmd -i mssql_create_predui.sql

     > sqlcmd -i mssql_update_predui.sql
     ```

     For detailed information and help about the `sqlcmd` utility and its arguments, run the utility as follows:

     ```
     sqlcmd -h
     ```

   - To execute the scripts using the SQL Server Management Studio, do the following:

a. Open the *mssql_create_predui.sql* file in Microsoft SQL Server Management Studio.

b. In the **SQL Editor** toolbar, click **Execute**, or choose **Query→Execute** to start creating the database.

c. Open the *mssql_update_predui.sql* file in Microsoft SQL Server Management Studio.

d. In the **SQL Editor** toolbar, click **Execute**, or choose **Query→Execute** to start updating the base schema database.

> Note:
>
> For a complete database setup, it is necessary to execute both the *create* and *update* scripts after they are modified.

Managing user passwords using the CPS_manage_password utility

The **CPS_manage_password** password management utility is used for generating an encoded database user password for the Command Prediction Service database. Changing the database user password for Command Prediction Microservice database requires updating the same in the microservice to be able to connect to the database. Failure to update the password results in database connection failure. This utility encodes the given input string, which can be replaced in the *pred.pwd* file.

The Command Prediction Microservice reads the database user password from the *pred.pwd* file for connecting to the Command Prediction Service database.

```
CPS_manage_password
```

The following options are available:

-h | - -help - Displays help for the utility.

-encode - Encodes input string.

-input= - Input string.

Manage user passwords using the CPS_manage_password utility

On Windows

1. Traverse to the location *<microservice_root>\commandprediction-<service_version>* and execute the following command:

```
CPS_manage_password -encode -input=<input_string>
```

2. Copy the generated string with the above command and update the *pred.pwd* file to replace the existing string with newly generated string.

3. Restart the **Teamcenter Process Manager** to enable the microservice to read the updated password from the file.

On Linux

1. Get the container ID of the running container for the Command Prediction Service.

   ```
   docker container ls
   ```

2. Generate a new encoded password string by executing the utility inside the container.

   ```
   docker exec -it <container_id> /app/CPS_manage_password -encode
   -input=<input_password_string_to_encode>
   ```

   Retain the generated string for further updates in *pred.pwd*.

3. Stop the running container.

   ```
   docker stop <container_id>
   ```

4. Get the Command Prediction Service ID.

   ```
   docker service ls
   ```

5. Remove the Command Prediction Service.

   ```
   docker service rm <service_id>
   ```

6. Get the secret ID for *pred.pwd*.

   ```
   docker secret ls
   ```

7. Remove the secret ID for *pred.pwd*.

   ```
   docker secret rm <secret_id>
   ```

8. Update the newly generated password string in *pred.pwd* located at *<microservice_container_root>/secrets*.

9. Go to the location *<microservice_container_root>* and execute the following command to update and redeploy the service.

   ```
   docker stack deploy -c commandprediction.yml <stack_name>
   ```

Ensure that the new docker secret is created.

Migrating user data using the CPS_migrate_user_data utility

The **CPS_migrate_user_data** utility migrates MD5 hashed data for users, groups, and roles to SHA256 hashed data in the Command Prediction Service database. Before running this utility, you must use the **admin_data_export** utility export the Teamcenter user, role, and group data to a file.

```
CPS_migrate_user_data [OPTION]
```

The following options are available:

-dbplat - Database platform used for Command Prediction Services such as MSSQL, ORACLE, or POSTGRESQL.

-username - Database username.

-password - Database password.

-hostname - Database hostname.

-port - Database port.

-namedinstance - For MSSQL platform, connect with named instance instead of database port.

-instance - Command Prediction Service database instance name. In the case of the Oracle database, the instance is SID, while in the case of POSTGRESQL and MSSQL databases, the instance is the name of the database

-inputfile - Full file path of the *Organization.XML* file generated using the Teamcenter **admin_data_export** utility.

-batchsize - Number of user profiles to be updated during the user data migration run. If not provided, the utility migrates the data of all the users.

Migrate user data using the CPS_migrate_user_data utility

1. Run the **admin_data_export** utility to export Teamcenter user, group and role data.

   For Windows

   a. Open the Teamcenter command prompt.

   b. Run the following command:

```
admin_data_export -u=<tc_user> -p=<password> -g=dba
-adminDataTypes=Organization -outputPackage=<export_file.zip>
```

For Linux

a. Open the terminal at <TC_ROOT>/bin.

b. Set TC_ROOT, TC_DATA and run <TC_DATA>/tc_profilevars for the terminal.

c. Run the following command:

```
/admin_data_export.sh -u=<tc_user> -p=<password> -g=dba
-adminDataTypes=Organization -outputPackage=<export_file.zip>
```

2. Extract the newly created ZIP file and locate the *Organization.XML* file in the *<extracted_folder>\ADMINISTRATION_DATA\Organization* folder.

3. Run the **CPS_migrate_user_data** utility to migrate the data.

For Windows

a. Open the Command prompt at the <Microservice_Root>\CommandPrediction-<version> folder.

b. Run the following command:

```
CPS_migrate_user_data -dbplat=<db_platform>
-hostname=<db_hostname> -username=<db_user>
-password=<db_password> -port=<db_port>
-instance=<db_instance> -inputfile=<path_to_organization_xml>
```

The log file is created in the *<Microservice_Root>\CommandPrediction-<version>\Logs\UserDataMigration* folder.

For Linux

a. Get the running container ID for the Command Prediction Service.

```
docker container ls
```

b. Copy the *Organization.XML* file into the container.

```
docker cp <path_to_oraganization_XML_on_host>
<command_prediction_container_id>:/app/
```

c. Run the following command:

```
ocker exec -it <command_prediction_container_id> ./
CPS_migrate_user_data -dbplat=<db_platform>
-hostname=<db_hostname> -username=<db_user>
```

```
-password=<db_password> -port=<db_port>
-instance=<db_instance> -inputfile=/app/Organization.xml
```

The log file is created in a docker container in the */tmp/Logs/UserDataMigration* folder.

8. Subscription configuration

Subscription configuration tasks

What are subscriptions?

Subscriptions are objects being followed using the **Follow** command. When objects are changed in Active Workspace, a number indicator appears to the right of the **Alert** button on the global toolbar indicating when subscription notifications are received. Users click the **Alert** button to view their notifications.

What can I configure?

You can configure the following aspects of subscriptions:

- **Notifications for a two-tier environment**.
- **Subscribable properties**.
- **Email and news feed notifications**.
- **Number of objects to which a user subscribes**.
- **Number of events to which a user follows**.
- **Number of days news feed notifications are retained**.
- **Purge of old news feed notifications**.

What do I need to do before configuring?

Before you can configure subscriptions, you must install the features. Install the following from the **Features** panel of Teamcenter Environment Manager (TEM):

- **Subscription** (client)

  Installs the user interface elements for viewing subscription notifications in Active Workspace.

  Select **Active Workspace→Client→Subscription**.

- **Subscription** (server)

  Installs the server-side definitions for subscriptions.

Select **Active Workspace→Server Extensions→Subscription**.

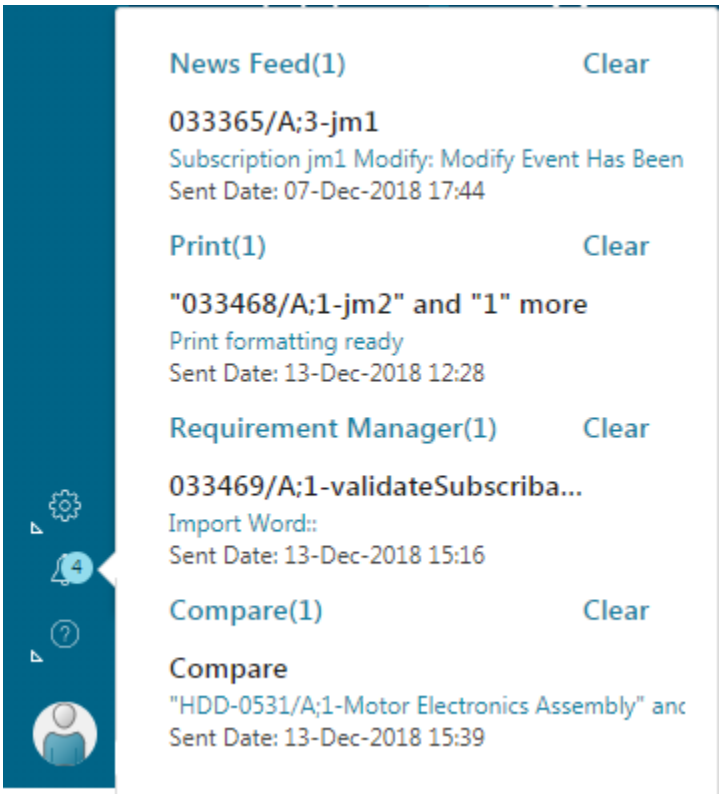
> Tip:
>
> After installing new features, you must rebuild the Active Workspace application.

Where can I find out more about subscriptions?

See *Subscription Administration* in the Teamcenter documentation.

What do subscription notifications look like?

The following is an example of notifications.



Configuring notifications

Configuring notifications for a two-tier environment

To use the notification functionality in a two-tier environment, you must manually configure the **TC_MESSAGING_MUX_URL** environment variable. Otherwise, alert information about new or changed messages is not sent from the server program to the user. This environment variable is configured correctly for four-tier environments. However, in stand-alone two-tier environments and dedicated hosts

used for servers, such as the Subscription Manager daemon or the Dispatcher module, this environment variable must be configured manually:

```
TC_MESSAGING MUX_URL=protocol://host:mux_port
```

host is the address of the host on which a server manager is installed, and *mux_port* is the value of the mux port set when the server manager was installed.

The following are examples of the configuration:

- On Microsoft Windows machines, add the following line to the **tc_profilevars.bat** file:

  ```
  set TC_MESSAGING_MUX_URL=http://blserver1:8087
  ```

- On Linux machines, add the following line to the **tc_profilevars** file:

  ```
  TC_MESSAGING_MUX_URL=${TC_MESSAGING_MUX_URL:=http://blserver1:8087}
  ```

Configuring notifications for a four-tier environment

If you have multiple server managers in a four-tier deployment, the value of the **TC_MESSAGING_MUX_URL** environment variable must depend on whether your environment uses a shared *TC_DATA* directory or unique *TC_DATA* directories:

```
TC_MESSAGING MUX_URL=protocol://host:mux_port
```

If the four-tier deployment shares the same *TC_DATA* directory for all server managers in the environment, the **TC_MESSAGING_MUX_URL** host must be set to **localhost**.

If the four-tier deployment does *not* share the same *TC_DATA* directory (this is, each server manager has its own *TC_DATA*), the **TC_MESSAGING_MUX_URL** host must be set to the host on which the server manager is installed.

Configuring subscribable properties

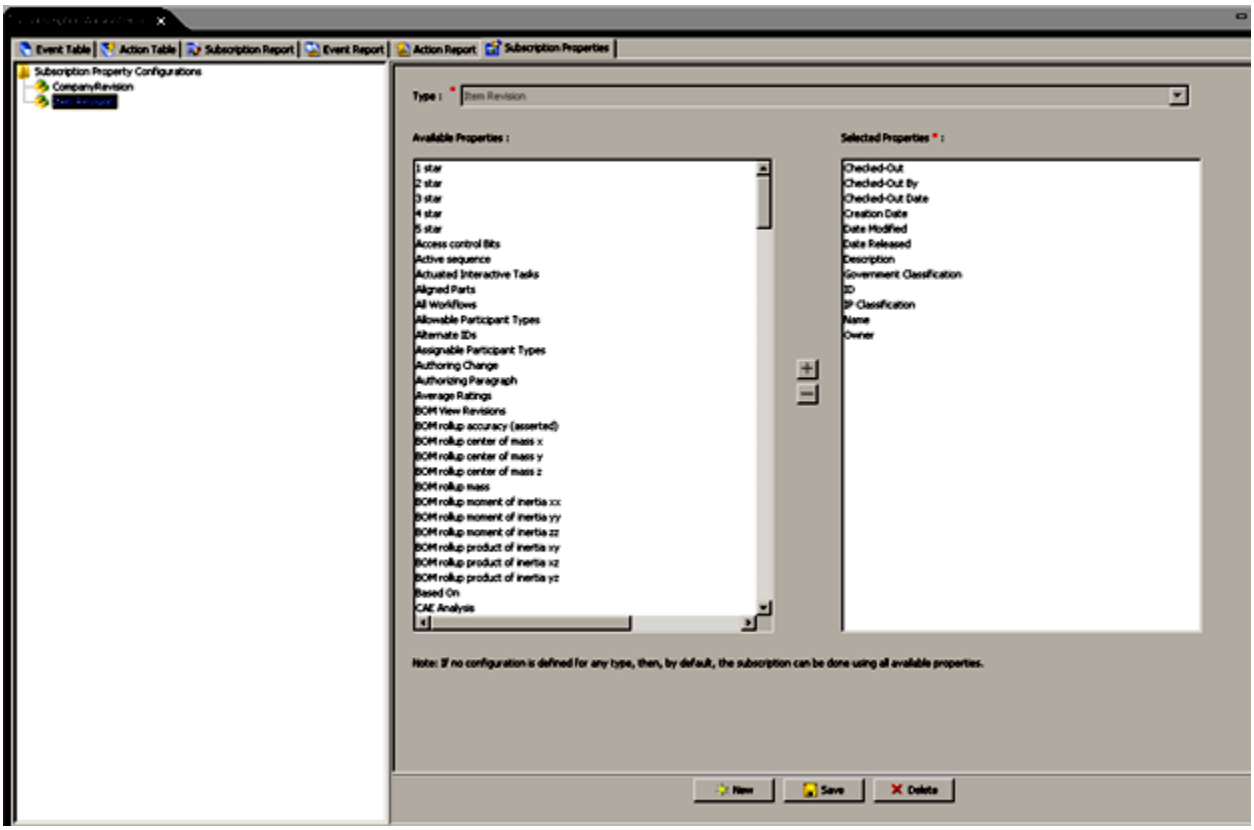
If you want users to only subscribe to certain properties on subscribable objects, such as an **Item** or **ItemRevision**, use the **Subscription Properties** tab in **Subscription Administration** in Teamcenter to configure the properties on which users can subscribe.

For example, using the **Subscription Properties** tab, you can configure several **ItemRevision** properties to make them available to users.

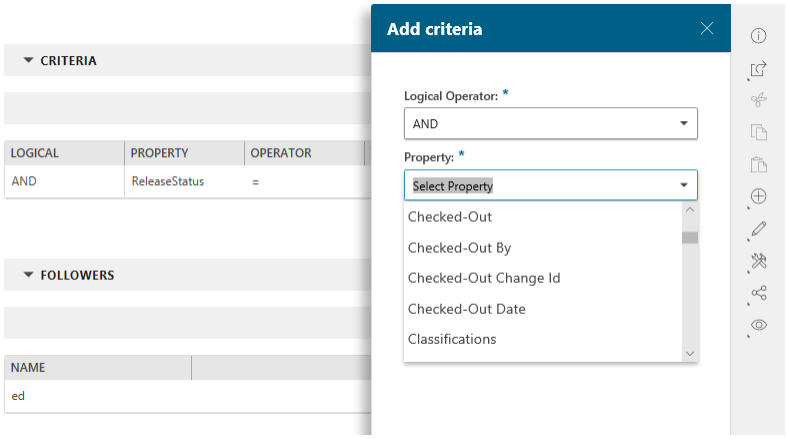
When configuring subscribable properties, consider the following:

- If no configuration is defined on a subscribable object, all properties are available to Active Workspace users for defining subscription criteria.

- A subtype inherits the configuration of the parent type unless it has its own configuration.
- If a property is turned off from subscription, but existing subscriptions utilize that property, then these subscriptions continue to have the property in the criteria until the subscriber manually removes it. Though existing criteria continue to apply, the Active Workspace user cannot define a new subscription using that property.



Example:



Setting subscription notification preferences

Setting email and news feed preferences

Set the following preferences to control notification behavior in Active Workspace:

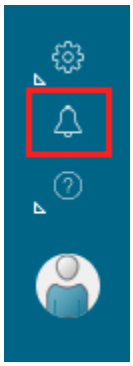
- **SCM_notification_mode**

  Indicates whether you want notifications to be delivered by email or news feed or both. If this preference is set to **1** (default), your notifications are delivered by email. To receive notifications by news feed, set the preference to **2**. To receive notifications by both email and news feed, set the preference to **3**.

- **AWS_Notifications_Polling_Interval**

  Specifies (in minutes) how frequently the system is polled for notifications, site-wide. The default setting is **5**. If this preference is set to **0**, the **Alert** navigation button is disabled.

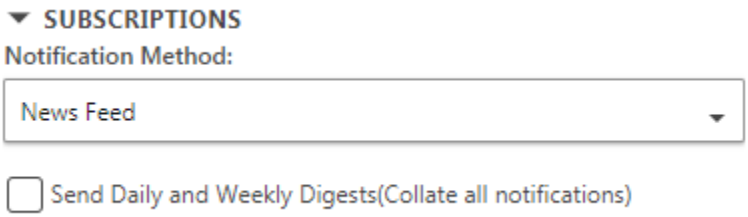
You are now able to view the number indicator to the right of **Alert** when:



- Print notifications are received.
- News feeds to which you have subscribed are received.
- There are existing unread notifications.

Setting periodic digest preferences

In addition to receiving notification by email or news feed, users can also select to receive daily and weekly digests that contain subscription notifications by selecting **Set Daily and Weekly Digests (Collate all notifications)** from the profile page.



The periodic digest collates all the daily notifications into a single email and it collates all notifications from the week into a weekly digest that is sent as a single email.

Set the following preferences to control periodic digest notification:

- **SCM_notification_digest**

  Indicates whether notifications are delivered as a digest. If this preference is set to **1** (default), digest notifications are disabled at the Site level.

  - **Active Workspace**

    Once the user enables the digest from the profile page, the digest is enabled for that user.

  - **Rich client**

    The user can create a User preference to override the value to set it to **2** to enable the periodic digest.

- **SCM_notification_digest_file_size_limit**

  Specifies the digest notification file size limit in megabytes (MB). The default value is **1 MB**.

  When the size of the collated digest notification exceeds the specified size limit, the digest is sent in multiple parts.

  This applies to both email and news feed notification methods.

- **SCM_execution_day**

  Specifies the day the weekly digest is triggered. The default is **Sunday**.

- **SCM_execution_time**

  Specifies the time the digest is triggered. The default is **15:00**.

- **WEB_default_site_server**

When set, the digest contains the link for the subscription.

- **Active Workspace**

  Use the format *localhost*:7001; for example, http://10.123.54.46:7001/awc.

- **Rich client**

  Use the format *WEB_SERVER_HOST*:*PORT*; for example, 10.123.54.46:7001.

Configuring subscription to multiple objects

Since users can subscribe to multiple objects, you can use the **AWC_followMultiObject_max** preference to control the number of objects to which a user subscribes at a time. By default, this preference is set to **5**.

Configuring My Events

Users can use **My Events** to follow multiple events on an object. Because it is important to control the number of events to which a user follows at a time to prevent users from creating many subscriptions, use the following site preferences:

- **AWC_followMultiEventConfig_max**

  Controls the maximum number of events a user can select on an object to follow. By default, this preference is set to **5**.

- **AWC_followMultiEventConfiguredEventTypes**

  Controls default configured event types for multiple events. Valid values are **__Attained_Release_Status**, **__Attach**, and **__Item_Rev_Create**.

Configuring news feed retention

Use the **SCM_newsfeed_purge_threshold** site preference to configure the number of days user news feed notifications are retained before being purged. The default setting is **0** days, which retains the news feed messages always. If you remove the preference value, the **Retain News Feed (In Days)** field still displays on the **Profile** page.

Users can view their news feed retention time by going to the **SUBSCRIPTIONS** area of their **Profile** page. From there, they can configure their threshold value. Otherwise, the purge is based on the site configuration.

Purging news feed notifications

You can purge old news feed notifications using the **clear_old_newsfeed_messages** command-line utility. To process only read messages, enter the following:

clear_old_newsfeed_messages -u=*Tc-admin-user* **-p=***password* **-g=***group* **-process_only_read_messages**

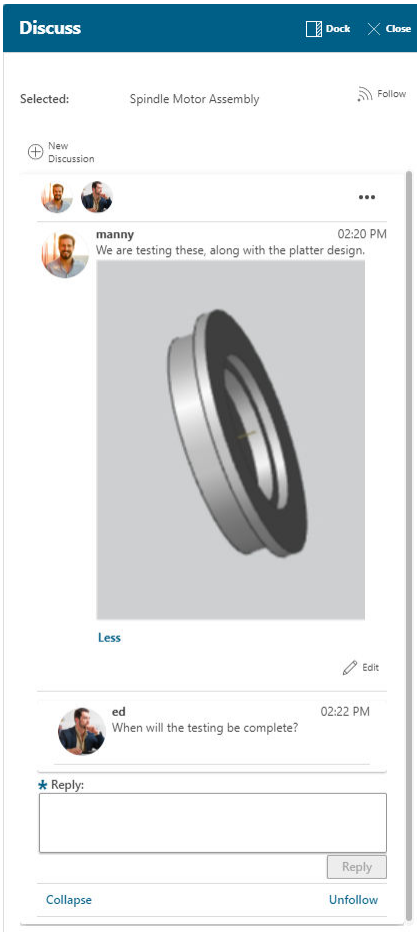
This utility purges messages based on the **purge threshold** that you set using the **SCM_newsfeed_purge_threshold** preference.

9. Active Collaboration configuration

What is Active Collaboration?

Active Collaboration, accessed using the **DISCUSSIONS** tile on the home page, or the **Discuss** button on the navigation bar, is an internal collaboration application in Active Workspace that allows:

- Discussions on one or more objects, such as items, parts, and documents.
- Threaded discussions, consisting of both public and private messages, with multiple users discussing any given workspace object.
- Comments with embedded images (GIF, JPEG, JPG, and PNG).
- Product snapshots (3D data associated with a product), which requires Teamcenter lifecycle visualization.
- Following and unfollowing capability on a single discussion or all discussions on an object.
- Receiving notifications via the **Alerts** button.
- Filtering and editing of existing discussions.
- Tracking discussions with an assigned status (**Open**, **In Progress**, and **Closed**) and priority (**Low**, **Medium**, and **High**).
- Receiving automated messages that show changes to a discussion or action, such as a status change, the addition or removal of participants, and changes to privacy.
- Assigning role-based permissions to specific users to delete discussions that are no longer needed.



What do I need to do to install Active Collaboration?

Install Active Collaboration from either Teamcenter Environment Manager (TEM) or Deployment Center.

From the Features panel of TEM:	From the Applications panel of Deployment Center:
• **Active Collaboration Client** Installs the user interface elements for viewing communication in Active Workspace. Select **Active Workspace→Client→Active Collaboration Client**. • **Microservices** Select **Teamcenter GraphQL Service**.	• **Active Collaboration** Installs the **Active Collaboration** feature in Active Workspace. Select **Teamcenter→Active Workspace→Active Collaboration** • **Microservice Node** Confirm that the **Microservice Node** component is configured.

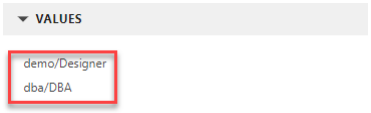
From the Features panel of TEM:	From the Applications panel of Deployment Center:
• **Active Collaboration** (server) Installs the server-side definitions for communication in Active Workspace. Select **Active Workspace→Server Extensions→Active Collaboration**.	

Note:

If you have existing questions, replies, and comments from Active Collaboration 5.0 or earlier or Active Collaboration for Retail 6.0 or earlier, you may optionally perform a one-time migration of these questions, replies, and comments to Discussions using the **ac0_migrate_s2cldata** utility.

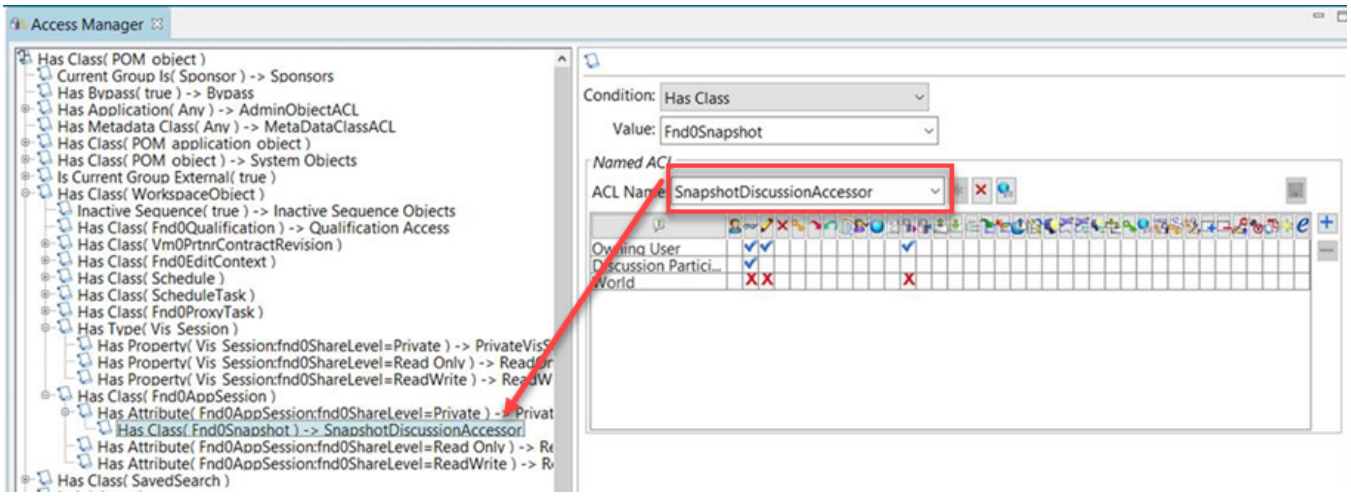
What can I configure?

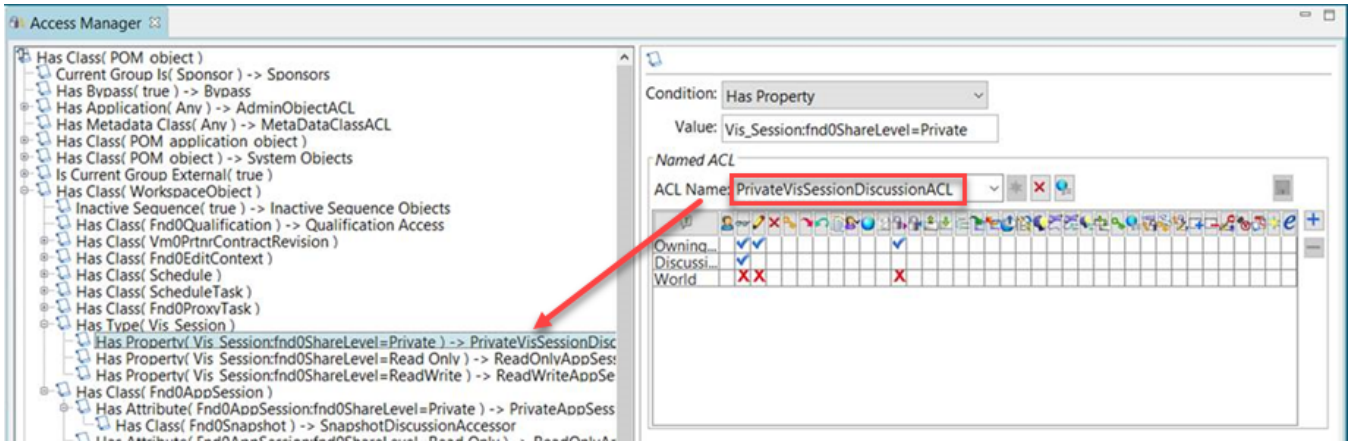
You can configure the following preferences.

Preference	Definition
Ac0AutoMessagesEnabled	Indicates whether automated messages are enabled. If set to **true**, automated messages are generated on the Active Collaboration **Discussion** panel whenever: • A participant is added to or removed from the discussion. • A tracked discussion's status is changed. • There are changes to privacy. • A snapshot is removed from the discussion (no longer shared in the discussion). The default is **true**.
Ac0DeleteDiscussionGroupRole	Grants permission to users of a specified group and role to delete discussions that are no longer needed. Valid values are in the format *group_id|role_id*. You can have multiple combinations, for example: 

Preference	Definition
	The default is **dba/DBA**.
Ac0EnableTrackedDiscussions	Indicates whether **Tracked** discussions are enabled. If set to **true**, a discussion can be set to tracked by selecting the **Tracked** check box. This enables the **Status** and **Priority** fields. The default is **false**.
Ac0SnapshotDiscussionsEnabled	Indicates whether 3D snapshots can be shared in discussions. If set to **false**, users cannot create a discussion containing a 3D snapshot. If set to **true**, users can create discussions using: • Previously captured product snapshots. • The **Capture Snapshot** icon when creating a new discussion from the **3D** tab on an assembly where visualization is installed. The default is **true**.

To enable your users to use snapshots shared in discussions, you must configure two access control lists (ACLs) in either the rich client or Active Workspace. Use Access Manager to create a **SnapshotDiscussionAccessor** rule and a **PrivateVisSessionDiscussionACL** rule. These enforce participant checks and give permissions to those participants to view a snapshot shared in a discussion.





10. Settings and performance

Manage system settings and performance

There are many utilities and settings that help you maintain the health and performance of your site.

Troubleshooting

Perform many basic tasks including retrieving software release versions, resetting your gateway server, monitoring the browser activity, and so on.

Client performance

Discover settings and concepts that may help improve client performance.

Preferences

Learn about how Teamcenter and Active Workspace store various settings as preferences.

Data model settings

Learn about various constant types that are part of the data model.

Server-side utilities

Gain an overview of certain Teamcenter server command-line utilities to help monitor and manage your site.

Troubleshooting

Retrieving Active Workspace client and server versions

Information about the running Active Workspace client and server, as well as the Teamcenter server version, site ID, and database ID to which they are connected is available when you are logged in.

To retrieve version information, click **Help** ⓘ > **About**.

Your results will vary, but following is an example of the results.

```
active-workspace@5.0.0 (Active Workspace Client (Staging Environment))
afx@4.1.0-361 (Siemens Web Framework)
Client Build: Wed May 06 2020 08:35:37
Server Build: aw5.0.0.13x.2020050601;...
```

```
Server Version: P.13.0.0.20200429.00
Site: IMC--1821067151 (-1821067151)
Database: tc
User Session Logfile: tcserver.exe41f085b3.syslog
```

General troubleshooting

> Note:
>
> If the Active Workspace client exhibits unexpected behavior, it is always good practice to clear the browser cache, and try the operation again. This is particularly important when server-side changes are made, such as updating to a new version of Active Workspace.

Issue	Possible resolution
No server available error	Tune the **tcserver** pool size using the **PROCESS_WARM** parameter. For details, see *System Administration* in the Teamcenter collection.

Intermittent image loading issues	Perform one of the following:
	
	• On the server, configure the web application server to exclude the problematic cipher. For example, if you have a jetty server:
	
	1. In a text editor, open the **jetty\etc\jetty-ssl.xml** file and add the following lines after the **<Set name="TrustStorePassword"***xxx***</Set>** line:
	
	`<!-- avoid IE TLSv1 issue by excluding the problematic cipher -->`
	`<Set name="ExcludeCipherSuites">`
	`<Array type="java.lang.String">`
	`<Item>TLS_RSA_WITH_AES_128_CBC_SHA</Item>`
	`</Array>`
	`</Set>`
	
	2. Save the file.
	
	3. Restart the Jetty server.
	
	The steps for other servers will vary.
	
	• On the client, configure the browser to not use TLS 1.0.

Upload file size exceeded max limit error during file uploads	The Active Workspace gateway sets a default maximum file size of 128Mb. `maxUploadFileSizeLimit: 134217728` To upload larger files, Siemens Digital Industries Software recommends that you use Data Share Manager.

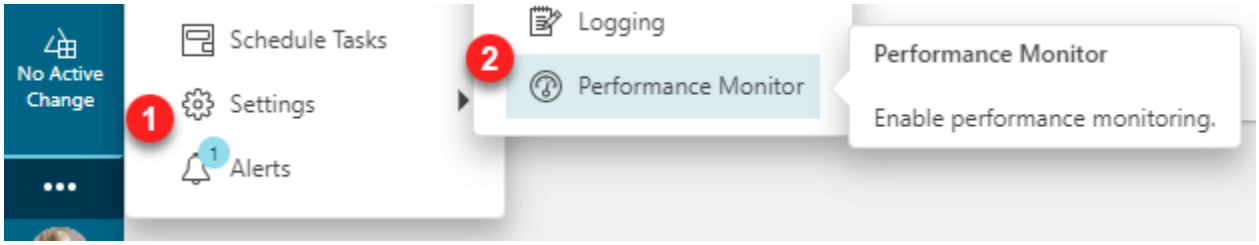
Issue	Possible resolution
	Otherwise, if you only need a small Increase in file size, you can modify the **maxUploadFileSizeLimit** setting in the gateway's config file. **AW ROOT**`/microservices/gateway-`**nnn**`/config.json` When increasing this size, you must consider the capabilities of your hardware and other software. Test any new values thoroughly before changing your production environment. After making any changes to this file, you must restart the gateway to implement the changes.
Users working with Active Workspace experience 403 errors when accessing thumbnails, files, or the viewer. (The 403 error may only be visible in the network page of the browser's developer tools.)	The Active Workspace administrator should verify that the **tcSOAURL** parameter is set correctly in the **web.xml** file. 1. Open the **web.xml** file in a text editor. The **web.xml** file located in the web application file (*awc.war* for Java or *awc.zip* for .NET). 2. Search for the following: **<filter-name>TCLoginVerifier</filter-name>** 3. If necessary, update the value of the **tcSOAURL** parameter so that it is the same as the value used for the **ProxyServlet redirectURL** parameter, which is also specified in the **web.xml** file. 4. Save the file and close the text editor. 5. Redeploy the application.
Active Workspace does not display the same language (locale) as the Teamcenter server.	Ensure the following: 1. Set the operating system of the computer running Active Workspace to the correct locale. 2. Set the browser running Active Workspace to the correct locale. 3. Ensure that **the web application file is set to the correct locale**.

View Active Workspace performance data

Use the **Performance Monitor** command to view performance and optional telemetry data.

When you use the **Performance Monitor**, it opens a panel and reports to the browser console about memory usage, overhead times, DOM node count, and so on. Additional information may be available

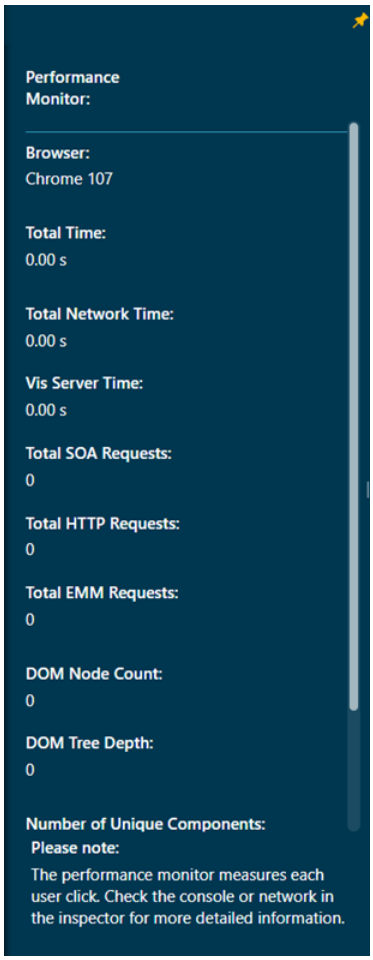
depending on which components you have installed in your Teamcenter environment. Close the panel to stop tracking the statistics.



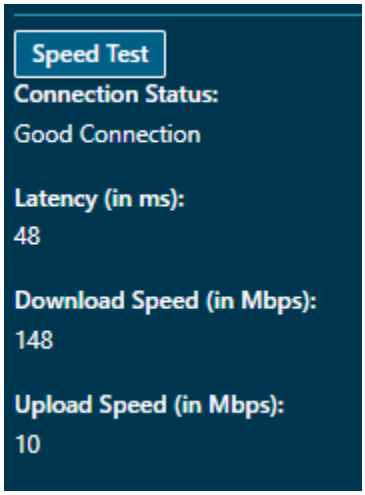
1. Open the **Settings** menu.

2. Select the **Performance Monitor** command.

Observe the **Performance Monitor** panel.



Additionally, you can run the **Speed Test** to see your bandwidth and latency to the server.



What else should I know?

In the detailed view provided in the console output, all values that are preceded by an asterisk will be reported to Siemens Digital Industries Software, if analytics is enabled.

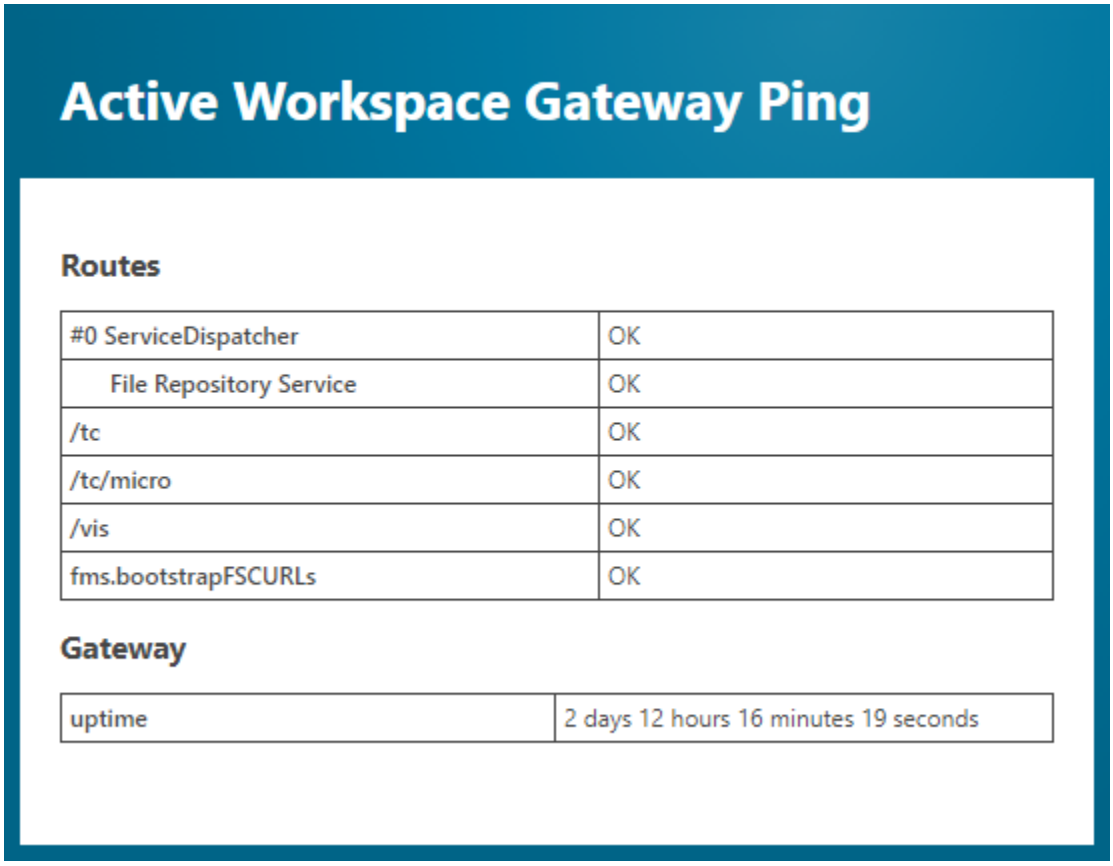
Example:

```
*ScriptingTime: "xxx.xxms"
```

Verify the Active Workspace gateway and other microservices

Use the **ping** functionality to check the various components of the Active Workspace gateway architecture, and verify connectivity.

```
http://hostname:3000/ping
```



You can disable this functionality by changing the **pingEnabled** setting to **false** in the gateway *config.json* file.

AW ROOT/*microservices/gateway-x.x.x/config.json*

```
"pingEnabled": false
```

> Tip:
>
> You must **restart the gateway** to apply the change.

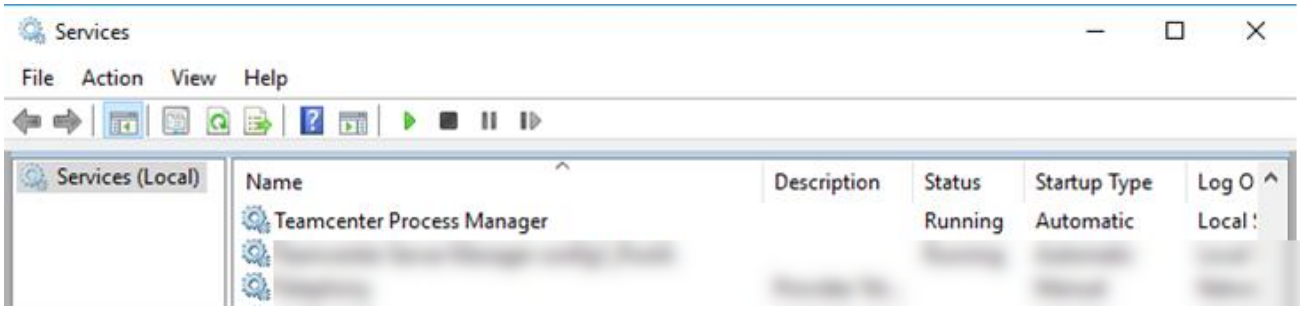
Resetting the Active Workspace gateway and microservices

When you make changes to the configuration files for the **Active Workspace gateway** and microservices, you must restart them for your changes to be recognized.

Make sure the FMS server cache (FSC) service is running before you start the Active Workspace gateway.

Windows

On Windows, all of the gateway and microservices on a given machine are managed by a single multi-threaded Windows service. To implement your configuration changes, restart the service using the **Services** control panel:



Or from the command line:

```
net stop "Teamcenter Process Manager" && net start "Teamcenter Process
Manager"
```

> Caution:
>
> You *must* use Microsoft **Services** to start the service. Do not run the service script directly.

Linux

On Linux, the gateway and microservices are manged by **Docker**. Remove and recreate the gateway services and config. The other services will restart in turn.

- Locate the **gateway** service and remove it.

```
TC_ROOT/container> docker service ls | grep gateway
wfvrc598nkbz   config1_MS_STACK_gateway
replicated   1/1        localhost:5000/teamcenter/afx-gateway:1.9.0
TC_ROOT/container> docker service rm wfvrc598nkbz
wfvrc598nkbz
TC_ROOT/container>
```

- Locate the **config.json** config and remove it.

```
TC_ROOT/container> docker config ls | grep config.json
e9ldu5xqhhwsya7t4i22skr9u   config1_MS_STACK_config.json
TC_ROOT/container> docker config rm e9ldu5xqhhwsya7t4i22skr9u
e9ldu5xqhhwsya7t4i22skr9u
TC_ROOT/container>
```

- Deploy the **gateway.yml** Compose file.

```
TC_ROOT/container> docker stack deploy -c gateway.yml config1_MS_STACK
Creating config config1_MS_STACK_config.json
Creating service config1_MS_STACK_gateway
TC_ROOT/container>
```

Start up race conditions

It is recommended to start the gateway after any graphQL services have had a chance to stabilize. The gateway will make several attempts before giving up, but in some cases this will not be enough. You can adjust the number of attempts made in the gateway's *config.json* file. Each attempt is 15 seconds.

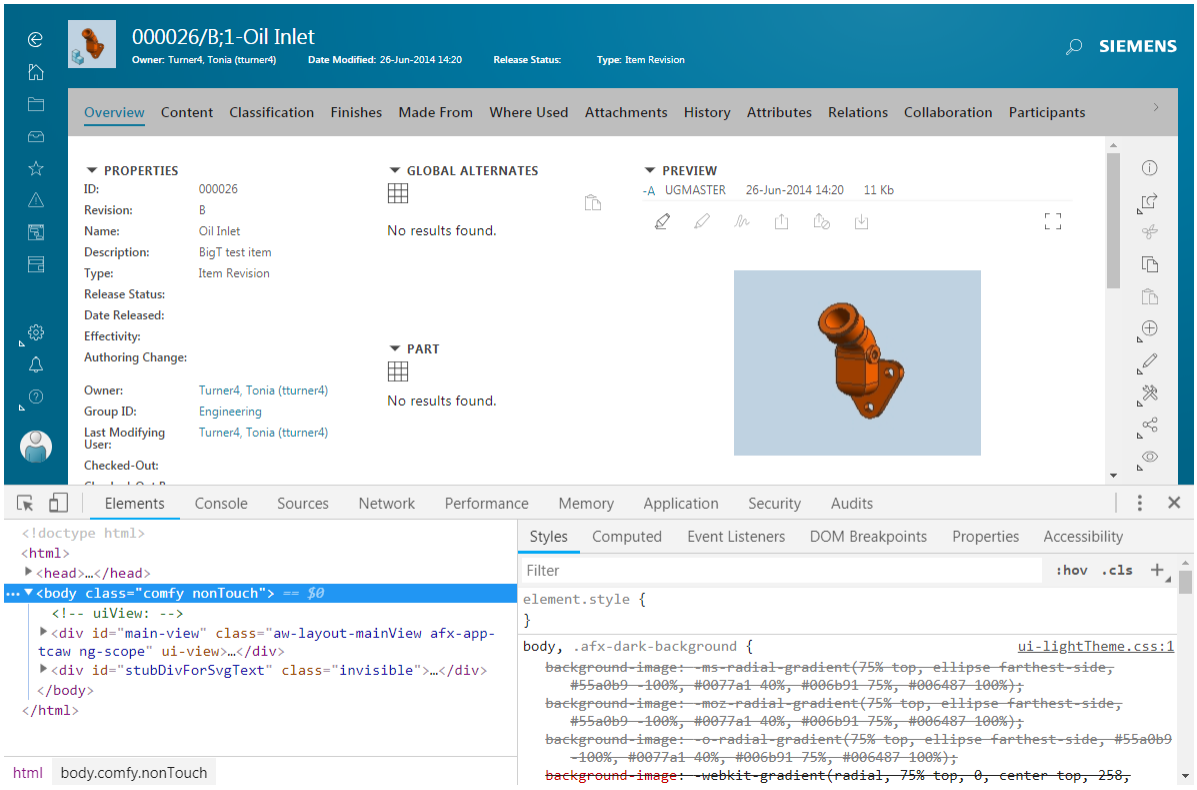
```
"graphql": {
     "endpoints": [
         "darsi",
         "tcgql"
     ],
     "attempts": 5
},
```

This problem is more prevalent on Linux and Docker and especially if all of your gateway services are installed on the same machine.

Monitoring browser activity

When you press the F12 key, a window displays the developer tools provided with your web browser. You can use these tools to monitor browser activity when using Active Workspace.

> Note:
>
> These tools are not provided by the Active Workspace client. See your web browser documentation for complete information about how to use the tools accessed with the F12 key.



Performance and settings

Enabling browser caching

When thumbnail images are displayed in Active Workspace, the image is loaded from the FMS system server using a file read ticket. Each time you display the same thumbnail, a new ticket is created. You can, however, enable browser caching so that the first time an image is loaded it is saved in the cache. This improves performance if the image is loaded again within a specified time period in the same session.

Enable browser caching

In Teamcenter, set the **Ticket_Expiration_Resolution** preference to the maximum number of seconds an image could be saved in the cache.

Essentially, the preference value defines the expiration time resolution of the file read ticket. For example, if you load a thumbnail image at 1:00 p.m., a file read ticket is created. If the value of the preference is set to 7200, the image remains in the browser cache for 7200 seconds (2 hours) after 1:00 p.m. So, any time that image is loaded within the next 2 hours, the same ticket is used. If the image is loaded again after 2 hours, a new ticket is created.

The current default value for this preference is 7200 seconds. Previous versions of Teamcenter used a default value of 1 second.

Compressing images for loading them quickly

Image files are used in Active Workspace for tiles, preview images, thumbnails, breadcrumbs, and so on. Image resolution is the clarity with which you can view the image with distinct boundaries. The resolution of the image depends on the number of pixels; more pixels correspond to more clarity, but also increases the size of the image. Large images take a lot of time for rendering and viewing.

To render images not only quickly but also with high clarity in Active Workspace, you can compress them and reduce their sizes without distorting the quality. You can manage the quality, sharpness, color, and accuracy of the images with lower resolutions. You can generate low, medium, and high resolutions of the original uploaded image while maintaining their aspect ratio. You can also define custom resolutions for the images.

Configure image resolution

You can compress images in Active Workspace used for tiles, preview images, thumbnails, breadcrumbs, and so on. This reduces their size without distorting the quality. Following are the prerequisites for configuring image resolution in Active Workspace:

- Teamcenter Visualization with **Mockup** and **Convert & Print** features.
- Dispatcher Server and Dispatcher Client components under Teamcenter Enterprise Knowledge Foundation are installed using Teamcenter Environment Manager.
- Image translator installed using the Teamcenter Environment Manager.

To compress images:

1. Enable the image compression feature using the **TC__image_compression_enabled** preference in Teamcenter rich client. The default value for this feature is set to **false**.
2. Configure the resolution values in the **TC_image_compression_types** preference in Teamcenter rich client.

   The out-of-the-box (OOTB) values are:

   - **64px::Low**
   - **300px::Medium**
   - **600px::High**

   You can also define custom values for images, such as **1200px::LARGE** or **2800px::EXTRALARGE**.

   These values are for the height of the translated image, and the appropriate width is automatically adjusted by the image translator based on the aspect ratio of the original image.

3. To specify the default image to be used for scaling across Active Workspace application, set the value for the **AWC_default_image_resolution** preference. The default OOTB value is **Medium**.

4. To customize the image for the **Overview** tab:

   In the **tc_xrt_Preview** tag, specify the value for the default image:

```
 <section titleKey="tc_xrt_Preview">
 <section titleKey="tc_xrt_Preview">
<image resolution=”<user_input>” source="thumbnail"/>
</section>
```

   - If no image resolution is defined, the system resolves to a high resolution image.
   - If the resolution preference value is **Medium**, the system resolves to medium resolution.
   - If image resolution is an undefined or invalid resolution type, the system resolves to high resolution.
   - If the image resolution is a custom value as defined in the **TC_image_compression_types** preference, it resolves to the specified custom resolution value. For example, if you specify **2800px::EXTRALARGE** as the image resolution, the image resolves to the custom value **EXTRALARGE**.

> Note:
>
> The values for image resolution are not case sensitive.

Preferences

Why do I need preferences?

You can use Teamcenter preferences to control various aspects of Teamcenter's behavior and appearance.

Following are only a few examples of what preferences control:

- Whether or not live updates are allowed.
- Password requirements when not using LDAP.
- Which XML rendering template (XRT) to use.
- Which query to use as the default quick access query.

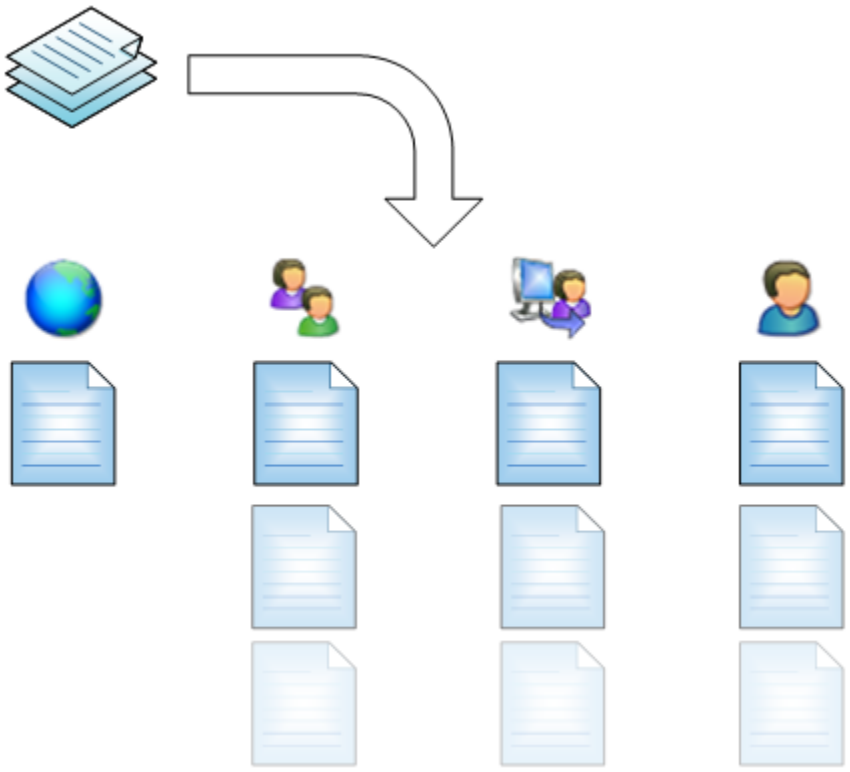
Siemens Digital Industries Software recommends browsing through the list of preferences to see which ones might be useful to you. Each preference's definition will document its use.

How do preferences work?

At their core, preferences are simply a way to store information. They are similar to environment variables, except that they operate with several layers of permissions.

Overview

Each preference consists of two major components, a definition and instances.



A preference *definition* along with all of its preference *instances* are together considered to be a preference.

Definition

The preference definition is like a blueprint. It defines the nature of the preference and is used to create the instances at the various locations. Even though it may define a default value, the definition itself is never retrieved or read as a preference. If there are no instances of this preference, there is no value.

Site

A preference instance created at the site location applies to everyone logged in to Teamcenter unless overridden.
There can be only one site instance.

Group	Any preference instances created at the group location apply only to users who are currently logged in as that group, and they supersede site preferences. There can be one group instance created for each group.
Role	Any preference instances created at the role location apply only to users who are currently logged in as that role (regardless of group), and they supersede site and group preferences. There can be one role instance created for each role.
User	Any preference instances created at the user location apply only to that user, and they supersede site, group, and role preferences. There can be one user instance created for each user.

Preference definition

You use the preference definition to create the overall limits and restrictions on the preference as well as setting the default value. Think of this as an abstract template from which the preference itself will be instantiated. Following are the fields used to define a preference definition:

Name	The name of the preference. Naming patterns help organize the preferences and give an idea of what they do even before you read the description. See the list of existing preferences for examples.
Protection Scope	Determines where and by whom it can be instantiated.
Type	Specify the preference value type.
Multiple	Specify if this preference can hold multiple values.
Description	Explain the use of the preference. What does it control? What format is expected for the values? Etc.
Value	Specify the default value that an instance will contain when initially created.
Environment	Retrieve the value from an OS environment variable of the same name.
Category	Organize related preferences based on their category. There are many existing categories you can use, or you can create your own.

Preference instance

You create a preference instance from its definition. When you create a new instance of a preference it must belong to a location. This location specifies when it is active and its priority in the hierarchy. You cannot create a preference instance if the protection scope does not allow it.

When referring to preference instances, it is common to shorten the phrase. For example, the *preference instance in the Engineering group location* is commonly referred to as the *Engineering group preference*.

When you create a new preference, you specify two things:

Location	Locations are where the preference instances reside. You can create preference instances at the following locations: • User • Role • Group • Site / System
Value	You can keep the default value from the definition or specify a new one.

Preference locations

- **User**

  This assigns the instance to a specific user. These are commonly the preferences that Teamcenter uses to track things like column widths in the rich client, or most recently searched text, for example.

  Although you can control your active preferences like style sheet registration down to the user level, it is normally recommended that you keep those kinds of settings to the Group level or higher. It makes things easier when people move in and out of groups and roles.

- **Role**

  You can control the behavior based on a user's role. This is handy for things such as style sheets. Keep the consumer's page simple while being able to provide the information the author or approver needs.

- **Group**

  Similar to the **Role** location, you can control the behavior at the next step up, at the group level.

- **Site / System**

  Preferences created at these locations apply to everyone. This is typically where you instantiate preferences that control system-wide behavior or default behavior that can be overridden at the group, role, or user level.

  Site preferences only allow a single instance, but a dba can change the protection scope of a site preference to something else.

  System preferences do not allow their protection scope to be changed, *even by a dba*. In all other ways, they behave like a site preference.

Caution:

An existing non-system preference may be changed into a system preference by a dba, but once it has been changed, it *cannot* be changed back. If you want to change it, it *must* be deleted and re-created.

Customer-facing preferences

You control an aspect of the UI or behavior directly by making changes to the preference. Examples of these preferences are configuring default paste relations, which style sheets are used in a given situation, or how the Dispatcher handles certain file types.

Internal preferences

Teamcenter uses preferences extensively to remember application parameters, like column width. Even though you can see and possibly modify the values of these preferences, it is not advised to do so.

An example of preference hierarchy

Everything in this example is based on a single preference, one which registers a style sheet to a business object for the summary view. It could be any preference as all preferences behave the same way. Since this preference definition's protection scope is **User**, you can create instances at the **Site**, **Group**, **Role**, and **User** location. This means you can control its value based on your users' current group, role, or even user name.

Example: I want the summary view's property layout for item revisions to depend on my users' login information

Following are the details of this example.

- You have three groups: Engineering, Manufacturing, and Testing.
  Each group has three roles: Manager, Designer, and Viewer.
- You want a default style sheet that everyone will use unless otherwise specified.
- Your technical users need an extended set of properties.
- Your managers need a page of workflow information.
- Your designers need classification information.
- You have users that just need a simplified layout for viewing.
- You have Conner. Conner is a power-user.
  Conner needs a special layout regardless of which group or role he's in.

Style sheet datasets

Five style sheet datasets are considered.

ItemRevSummary

Configured to be the default style sheet for the Item Revision summary page. This applies to everyone unless overridden.

IRSumTech

Configured to provides the extra properties for the Engineering and Manufacturing groups, but not for any other groups.

IRSumMgr

Configured to display workflow information for the Manager role, regardless of group.

IRSumDes

Configured to show the classification trace for the Designer role, regardless of group.

ConnersIRSum

Configured for Conner. Conner has his own requirements

Preference instances

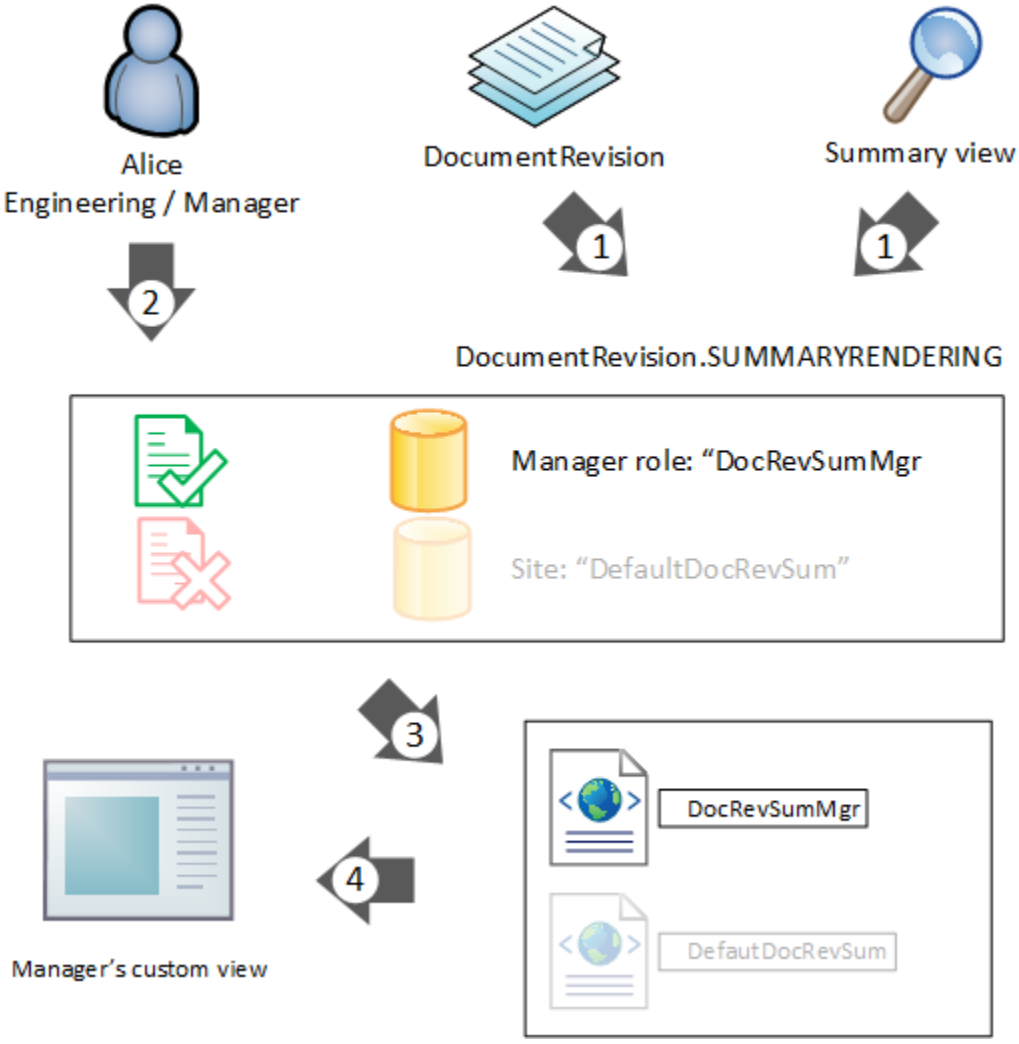
Assign the style sheets to the various groups and roles, and even users if desired, by creating each preference instance with the value pointing to the respective style sheet. In this example, there are 6 preference instances created.

User preferences	Conner: ConnersIRSum
Role preferences	Manager: IRSumMgr
	Designer: IRSumDes
Group preferences	Engineering: IRSumTech
	Manufacturing: IRSumTech
Site preference	*value:* ItemRevSum

The Viewer role and the Tester group have no preference instances created for their location.

How does Teamcenter choose which preference to use?

In this example, Alice selects a **DocumentRevision** business object and uses the **Summary** tab. When she does this, Teamcenter performs a few steps to determine which style sheet to use.



1. Based on the object type and the view location, the system knows the name of the preference instances to retrieve.

   In this example, **DocumentRevision.SUMMARYRENDERING**.

   There are two instances: one at the **Site** location, and one at the Manager **Role** location.

2. Based on the user's current session information, Teamcenter chooses the appropriate preference instance.

   Less specific locations are overridden by more specific locations.

3. The value of the chosen preference instance is read, providing the name of the style sheet to retrieve.

4. Teamcenter uses the style sheet to render the view.

Result

Your users see a different set of information based on what group or role they are in because the client uses different style sheets.

User - Group / Role	Preference instance build-up	Resulting style sheet
Alice — Engineering / Manager	Alice: *none* **Manager: IRSumMgr** Engineering: IRSumTech Site: ItemRevSum	IRSumMgr
Ted — Manufacturing / Manager	Ted: *none* **Manager: IRSumMgr** Manufacturing: IRSumTech Site: ItemRevSum	IRSumMgr
Sue — Testing / Manager	Sue: *none* **Manager: IRSumMgr** Testing: *none* Site: ItemRevSum	IRSumMgr
Bob — Engineering / Designer	Bob: *none* **Designer: IRSumDes** Engineering: IRSumTech Site: ItemRevSum	IRSumDes
Carol — Engineering / Viewer	Carol: *none* Viewer: *none* **Engineering: IRSumTech** Site: ItemRevSum	IRSumTech
Pat — Testing / Viewer	Pat: *none* Viewer: *none* Testing: *none* **Site: ItemRevSum**	ItemRevSum
Conner — Engineering / Manager	**Conner: ConnersIRSum** Manager: IRSumMgr Engineering: IRSumTech Site: ItemRevSum	ConnersIRSum
Conner — Testing / Viewer	**Conner: ConnersIRSum** Viewer: *none* Testing: *none* Site: ItemRevSum	ConnersIRSum

- Alice sees the style sheet for Managers because she does not have a user preference set to supersede it. The site preference is overridden by the Engineering group preference, which is overridden by the Manager role preference. Ted has the same result; the Manufacturing group preference is overridden by the Manager preference. Sue doesn't have a group preference, but she still gets the Manager role preference.

- Bob sees the style sheet for Designers because of his role, similar to the preceding example.

- Carol sees the tech style sheet because there is no role preference for Viewers.
- Pat's group and role do not have preferences associated with them, and neither does she have a user preference, so she gets the default style sheet defined by the site preference.
- Conner gets Conner's style sheet regardless of which group or role he's in, since a user preference supersedes all others.

What are environment preferences?

You can define a preference to retrieve its value from an environment variable in the operating system.

If you want to pass multiple values from the environment to the preference, you must configure the following:

- Set the preference's **Multiple** setting to **multiple**.
- Use the appropriate separator in the environment variable. The environment variable is read from the operating system on which the **tcserver** process is running.

Windows	Semicolon — For example, `MyEnvPref=Value1;Value1;Value3`
Linux	Comma — For example, `MyEnvPref=Value1,Value1,Value3`

The environment variable is only read by the **tcserver** process when the value is first requested, so any changes made to the environment variable after that will not be reflected in the Teamcenter preference until after the next time the **tcserver** process is started.

Remember, the environment variable is read from the environment where the **tcserver** process is running, which is not necessarily the environment where the client is running.

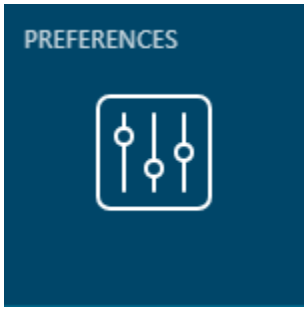
Working with preferences in Active Workspace

You can work with all Teamcenter preferences from within the Active Workspace client using the **Preferences** page.

Preference Management is part of the **Active Admin** installation option for Teamcenter. Once installed, you can get to this page by either:

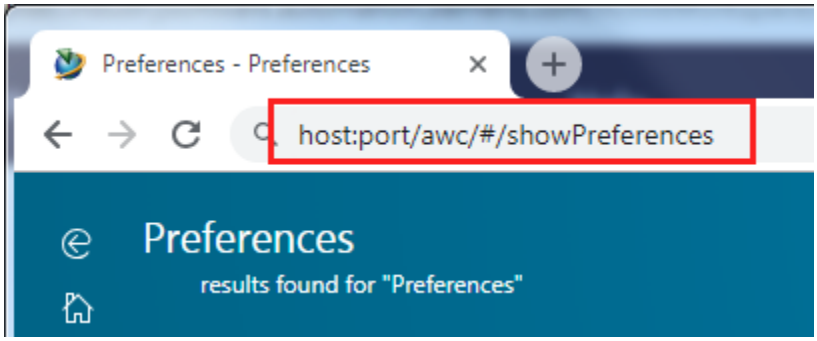
- Using the **PREFERENCES** tile from your home page.

  By default, this tile appears in the home page of the **TcActiveAdminWorkspace** workspace.



- Navigate directly to the page with the `host:port/awc/#/showPreferences` URL.

  This option is only available if your current workspace allows it.



What can I do with the preferences location?

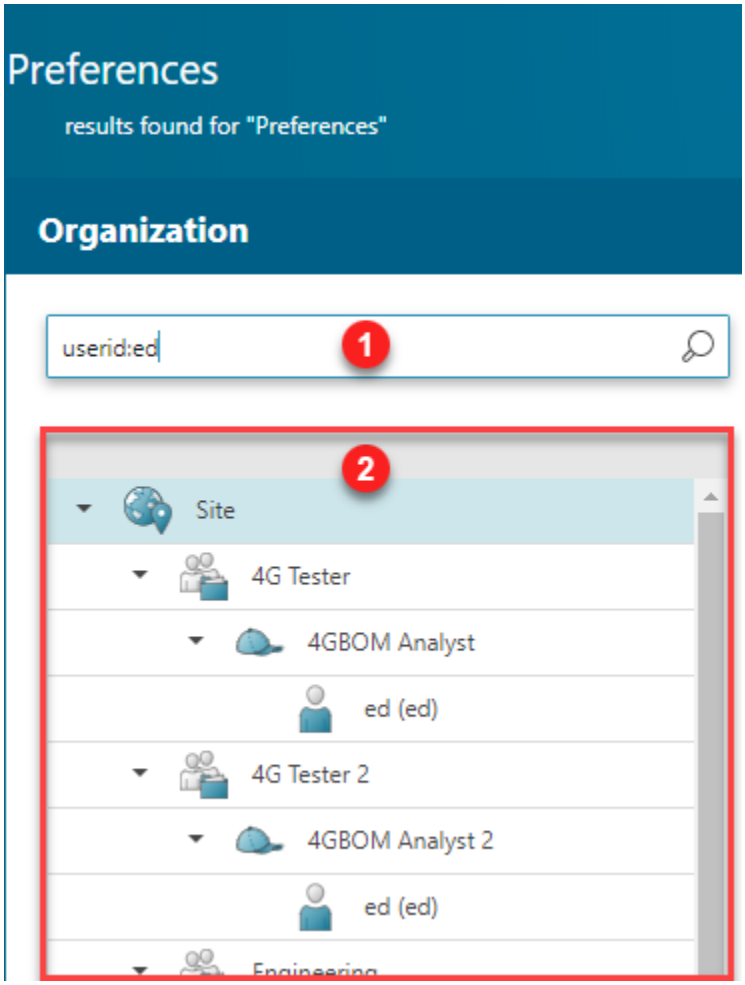
Your ability to work with preferences is determined by whether you are currently logged in to a group with administrator privileges.

Administrator?	Permissions.
Administrator	Search and modify preferences Create and override site, system, group, role, and user preference instances Delete preference instances and definitions
Group Administrator	Search and modify preferences Create and override group, role, and user preference instances within your group
User	Search existing preferences Create and override your own user preference instances

The organization panel

Use the **Organization** panel to select in which session context you wish to work.

If you do not have a choice of working in other session contexts, (you have no administration privileges), then you will not see the **Organization** panel, and you can only work in your current session context.



1. **(optional) Filter the organization list.**

   If you simply use text, the system will match within group, role, user name, or user id. If you use quotation marks, it will search for exact matches, if you don't it will append a wildcard to the end of your text. If you want to include spaces or commas in your search, you must use quotes.

   You can narrow down the search by using the following prefixes:

   - group:
   - role:
   - username:
   - userid:

   You can specify more than one of these by putting a space between them.

Example:

To search for the word, **design**, put `design` in the field.

To search for the specific user id, **ed**, put `userid:"ed"` in the field.

To search for all users with user ids beginning with **ed**, put `userid:ed` in the field.

To search for the specific user named **Smith, Bob** in roles beginning with **design**, put `username:"Smith, Bob" role:design` in the field.

2. **Select which session context in which you wish to work.**

   If you select the site, you can only work with site locations.

   If you select a group, you can work with that group's location overrides.

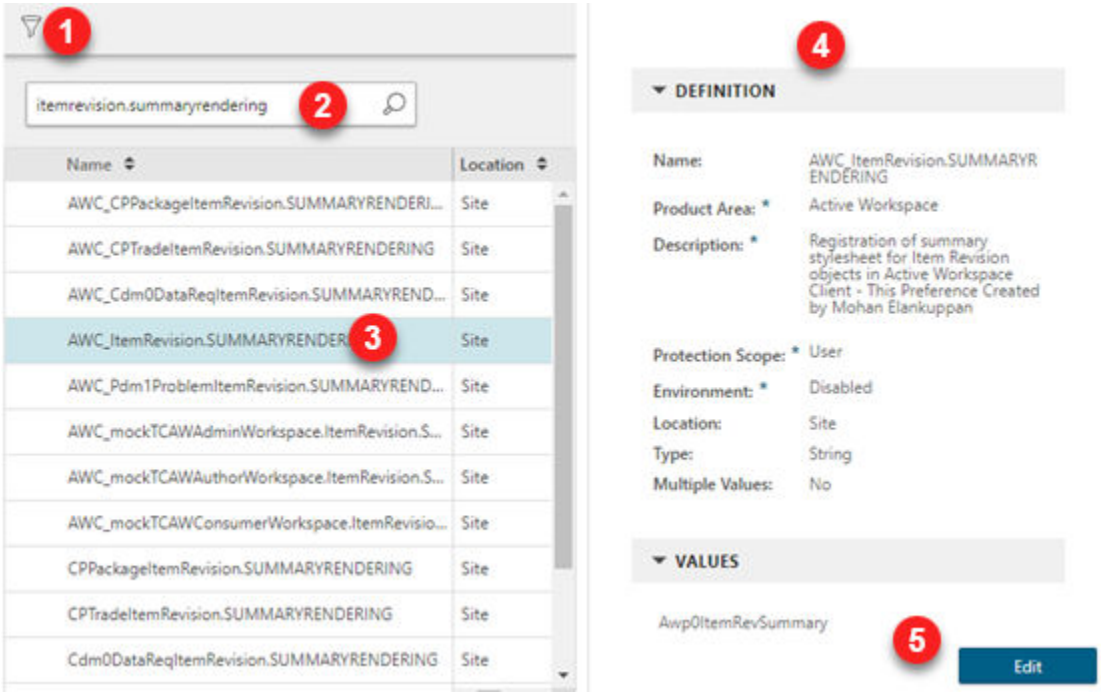
   If you select a role, you can work with location overrides for that role and its group.

   If you select a user, you can work with location overrides for that user, role, and group.

The preference list will be populated with all valid preference locations for the session context that you have selected, and you are able to:

- Modify the values of existing preference locations in the session context.
- Create new preference locations for the session context.
- Override preferences for this session context, if the preference scope allows it.

The preference list



Select your working context in the **Organization** panel, if available.

1. (optional) Filter the preference list by category.
2. (optional) Filter listed preferences.
3. Select a preference.
4. View preference information.
5. (optional) Edit the value at this preference location.

   If you do not have permission, you will not see this button.

Override a preference

To override a preference, you must create a new instance of the preference at a higher-precedence **location**. Each preference defines its own **scope**, which is the highest precedence location allowed.

For example, If a preference's scope is **Site**, then it cannot be overridden, but if its scope is **User** then it can be overridden at every level.

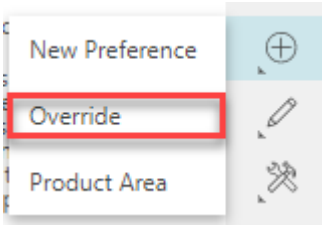
If a preference instance's location is **Site**, it will be overridden by any other location instance but if its location is **User** then it overrides any other location for that specific user.

> Tip:
>
> If a preference in the list has a **location** of **None**, then that means it is the preference *definition* and there are no current location instances.

Following are the levels of precedence for locations.

	scope	location
User	Can override at any location.	Overrides all other location values.
Role	Can override at group and role locations.	Will override Site and Group location values.
Group	Can only override at group locations.	Will override Site location values.
Site	Can not override.	Is overridden by any other location

1. (optional) Filter the preference list.
2. Select the preference you want to override.
3. Open the **New** command stack ⊕, and then choose **Override**.



4. In the **Add Override** panel, choose the location for the override (if allowed), set the new value, and then choose **Add**.

Displaying items instead of revisions

> Caution:
>
> This is a non-standard configuration and requires careful planning. Work with your Siemens Digital Industries Software representative if you need this functionality.

Active Workspace is designed for the user to work almost exclusively with objects of the **ItemRevision** type (and its children).

If you have a *special use case* and you need to display item types, then you need to configure the following:

- Allow the user to create an Item.

  Modify the **AWC_DefaultCreateTypes** preference to include an item type. That item type and all subtypes will be considered creatable.

- Change the **Fnd0ItemRevPasteOnTargetUponCreate** business object constant for the new type. This will automatically paste the item type into the user's folder when it is created.

- Configure indexing to work with Items instead of revisions.

In addition, you should also suppress the ItemRevision type from the UI.

> Caution:
>
> Siemens Digital Industries Software does not recommend that you present both items and revisions to your users.

Deleting various object types

By default, the **Delete** command does not appear for every object type your users can see. If you want to add additional object types to the list, then you must change the following preference:

AWS_allowedTypesForDelete

This is a multiple-value preference that accepts a list of business object types for which the **Delete** command appears in the Active Workspace interface.

> Caution:
>
> Even when the **Delete** command is visible, there are still two conditions that must be met for your users to delete an object:
>
> - They must have the delete permission for the object.
> - The object must not be referenced by other objects.

Special behavior for folders

You can control what happens when your users attempt to delete an object with folder references by changing the following preference:

TC_auto_delete_folder_references

- **true (default)**

  The default value is **true**, which ignores folder references when checking for references to other objects, and if no *other* references are found, then the folder references are automatically removed, and then the object is deleted without complaint.

- false

  Changing this to **false** prevents the object from being deleted from the database and presents an error message if it has any references to any other objects, including folders.

This preference applies when deleting a folder that contains objects, and when an object is contained in a folder.

Controlling notification timeout

You can control the notification panel timeout using a preference.

AWC_notification_timeout

The value is the number of seconds to wait before closing the notification. If the value is negative, the window will not close automatically.

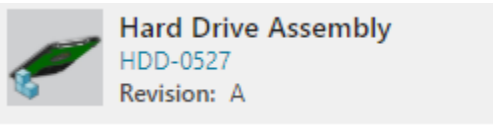
Defining properties that display in object cells

To define the properties that display on the cells for objects in Active Workspace list view, use the *business-object*.**CellProperties** preference. The first two properties in the list of properties in the preference are displayed without labels and are formatted as a primary title and subtitle. The remaining properties are displayed in the cell as *name*:*value*.

The default values vary by object type. For example, following are the default values of the **ItemRevision.CellProperties** preference:

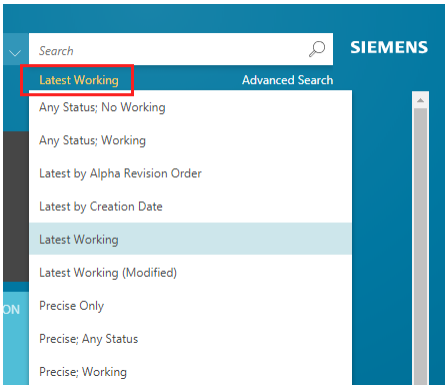
```
object_name
item_id
item_revision_id
```

The values in this example appear as follows in Active Workspace.



Defining the revision rules list

Revision rules determine the state of objects you view in the user interface. The active revision rule is shown to the right of the user name. Users click the revision rule to display the list of all available revision rules. To set a different revision rule, a user selects another revision rule from the list.



By default, the list of available revision rules is obtained from Teamcenter. However, as an administrator, you may want to provide different revision rules for Active Workspace than are used in the rich client. For example, you may want to have Active Workspace default to **Latest Released** whereas you want the rich client to still default to **Latest Working**.

To set a different list of revision rules for Active Workspace, add revision rules to the **AWC_Rev_Rule_List** preference. Whenever a custom revision rule is created, you must add it to this preference for it to appear in the revision rules list. By default, the preference is empty, meaning that the revision rules list in Active Workspace defaults to the revision rules from the rich client.

To set the revision rule that is selected by default, add it to the **AWC_Rev_Rule_Selected** preference. The revision rule in this preference must match a revision rule in the **AWC_Rev_Rule_List** preference.

If the revision rule in the **AWC_Rev_Rule_Selected** preference is removed from the **AWC_Rev_Rule_List** preference, you must change the revision rule in the **AWC_Rev_Rule_Selected** preference to one in the **AWC_Rev_Rule_List** preference.

By default, the **AWC_Rev_Rule_Selected** preference is empty, meaning that the first revision rule in the **AWC_Rev_Rule_List** preference is the one that is selected by default in the user interface.

Where can I get a list of preferences?

There are several sources from which to retrieve a list of preferences and their definitions.

Administration data report

You can find the **Administration Data Report** in the **References for Administrators and Customizers** in the Teamcenter documentation area in Support Center. In this report, you will find a complete list of all preferences shipped with Teamcenter. When you install additional features, like Dispatcher, NX Integration, 4th Generation Design, and so on, additional preferences will be

added to your site. To get the most accurate and up-to-date listing of preferences contained in your site, you must create your own Administration Data Documentation report.

Rich client

You can use the various tabs of the rich client's **Edit→Options** menu to interact directly with preferences, including a report of which preferences have changed since installation.

Raw XML export

You can produce an XML file containing preference information using the **preferences_manager** utility.

Active Workspace client

You can interact directly with preferences using the **showPreferences** location.

Business Modeler IDE constants

Global constants

Following are the global constants unique to Active Workspace:

- **Awb0SupportsStructure**

  Specifies the business objects that can have a structure under it. If you want to display a custom business object in the **Content** tab, add the custom business object to this constant. This constant is added by the Active Content Structure template (**activeworkspacebom**).

- **Awp0FilterCategoryDisplayCount**

  Specifies the default number of search filter categories to display in the **Search Filters** panel.

- **Awp0FilterValueDisplayCount**

  Specifies the default number of search filter values to display within a search filter category. If additional values are available for filtering in any category, a **More** button appears to display the remaining values within each category. The default value is **5**.

  The threshold to display the box to search filter values is twice the value of **Awp0FilterValueDisplayCount**.

- **Awp0IndexableFileTypes**

  Specifies the list of file types that are allowed for text content extraction during search indexing. By changing the value of this constant, you can specify the file types you want to index. (This global constant is used if no value is set for the **AW_Indexable_File_Extensions** preference.)

  The following values are supported:

.as	*.dotm*	*.msg*	*.various*	*.xltm*
.aw	*.dotx*	*.ods*	*.vdx*	*.xltx*
.csv	*.eml*	*.pdf*	*.wo*	*.xlw*
.dat	*.epub*	*.ppt*	*.wpd*	*.xlsx*
.dc	*.fff*	*.pptx*	*.xml*	*.zip*
.dif	*.htm*	*.rtf*	*.xla*	*.7z*
.doc	*.html*	*.stc*	*.xlam*	
.docm	*.ip*	*.sxc*	*.xls*	
.docx	*.mdb*	*.tar*	*.xlsm*	
.dot	*.mif*	*.txt*	*.xlt*	

For example, to enable indexing on compressed files, add any combination of *.zip*, *.7z*, or *.tar* to the list.

Read permission is required for indexing a file. If any file is password protected, the file will be skipped and no warning will be generated.

- **Awp0StoreDatasetContent**

  Global search results can display the location of search terms inside file content attached to items. Search results that match content from attached dataset files display as snippets of text matching the search terms. The Indexing Engine (Solr) requires that you set this global constant In Business Modeler IDE to true to ensure that dataset fields are stored in the Solr schema. You must also configure the preferences to enable snippets, merge the schemas, and reindex your data, including datasets.

Business object constants

Following are the business object constants unique to Active Workspace:

- **Awb0AvailableFor**

  Lists the business object types for which a feature should be made available. The values are comma separated. This constant honors type hierarchy.

  When this constant is used with the **Ase0ArchitectureFeature** business object, the constant controls visibility of the **Architecture** tab for business object types. The **Architecture** tab is made visible for all listed business object types and their all subtypes. The types should be those that represent the top line in structures. This constant supports comma-delimited values of business object types, for example:

  Functionality
  Fnd0LogicalBlock

RequirementSpec
Requirement
Paragraph
Fnd0SystemModel

> Note:
>
> The **Architecture** tab is not visible for custom business objects. Determine the business object types that require the **Architecture** tab. From these types, determine those that are the top line in structures. Add only those types to the value of the **Awb0AvailableFor** business object constant on the **Ase0ArchitectureFeature** business object.
>
> You can edit the display name configured for the **Ase0ArchitectureFeature** business object in Business Modeler IDE to suit your business processes. By default, the display name of the tab is **Architecture**.

- **Awb0BOMArchetypeToOccurrence**

  Determines the instance of which particular subtype of the **Awb0Element** business object is created. This business object constant is a comma-separated list of item revision or GDE subtypes. Using such a list avoids the need to create a separate **Awb0Element** business object for each item revision type.

- **Awp0SearchIsIndexed**

  Indicates that the business object will be indexed for searching when this constant is set to **true**. This information is propagated through the business object hierarchy. For example, if **ItemRevision** is selected for indexing, all business objects under **ItemRevision** (such as **Part Revision** and **DocumentRevision**) are also indexed.

  > Note:
  >
  > Do not set this constant to **true** for the **WorkspaceObject** business object. This results in indexing errors.

- **Awp0SearchIsIndexedExt**

  Indicates that external business objects are indexed for searching. By default, the value of this constant is **false**, meaning that external objects are not indexed. The scope for this constant is the **Awp0AWCExternalSystemObject** business object, which designates objects originating in systems external to Teamcenter.

  To change the value to **true**, open the **Awp0AWCExternalSystemObject** business object and select the **Awp0SearchIsIndexedExt** business object constant on the **Business Object Constants** tab. Then click **Edit** and select the **Value** check box.

- **Awp0SearchClassifySearchEnabled**

Enables the searching and filtering of classification data.

- **Awp0SearchIsClassifyDataIndexed**

  For the specified business object type and below, specifies that classification data be indexed for searching and filtering.

- **Awp0SearchDatasetIndexingBehavior**

  Defines the behavior of inline indexing for dataset file contents. The scope for this constant is **WorkspaceObject** types and their subtypes. Specify one of the following:

Inline	Dataset content is indexed inline with the parent business object. When a search matches dataset content, the search results returns the parent business object instead of the dataset. The datasets are defined using **Awp0DatasetTypeToBeIndexedInline**.
Relation	Dataset content is indexed as part of the dataset but it maintains the reference to the parent business object. When a search matches dataset content, the search results return the dataset as well as the parent business object.

  The default value is **Inline** except for **DocumentRevision**, where the default is **Relation.**

- **Awp0DatasetTypeToBeIndexedInline**

  Identifies the datasets to be indexed along with the business object. The scope for this constant is **WorkspaceObject** types and their subtypes.

  Set this property only for types that are also marked for indexing and **Awp0SearchDatasetIndexingBehavior** is set to **Inline**.

  The format is:

  `<INHERIT | NO_INHERIT>:`*`RelationName`*`:`*`DatasetTypes`*

  The keyword specifies the behavior to apply to the rule:

INHERIT	Applies the rule to the specified type and all its subtypes. For example, index PDX dataset content related to **TC_Attaches** for **ItemRevision** and its subtypes: INHERIT:TC_Attaches:PDF
NO_INHERIT	Applies the rule only to the type where the rule is defined. A rule applied to a parent is not inherited by child types. Specifying **NO_INHERIT** can help improve performance. NO_INHERIT:IMAN_Specification:Text

  You can specify one to many relationships between *RelationName* and *DatasetTypes*.

RelationName is a relation name or the wildcard character *****. Specify one or more clauses separated by commas.

INHERIT: TC_Attaches: PDF, INHERIT: IMAN_Specifiation: Text

INHERIT: *: PDF

DatasetTypes is a dataset type. Specify one or more values separated by a tilde **~**.

INHERIT:TC_Attaches: PDF~MSWordX

Specifying only wildcards is not valid (for example, do not specify **INHERIT: *: ***).

No default value is specified with the exception that **SpecElementRevision** is set to **INHERIT: *: FullText**.

As a best practice, do not specify all relations (*****) for inline indexing and then subsequently try to limit inheritance by setting a subtype clause to index only a specific relation to a specific type. You can avoid inheritance by:

- Using **NO_INHERIT** to limit the scope of indexing for a specific type.

  For example, if all **ItemRevision** PDFs for any relation are being indexed inline, do not write a qualifying **INHERIT** rule for a subtype. For example:

  If an **INHERIT** rule for **ItemRevision** is defined as **INHERIT:*:PDF**,

  And, an **INHERIT** rule for an **ItemRevision** subtype indexes only PDFs associated with the **TC_Attaches** relation,

  Then the indexing behavior at the subtype level might not behave as expected, because you already specified all **ItemRevision** subtypes to index all PDFs,

- Configuring the subtype to override the parent. For example, to index PDX content for all the relations of the subtype, set **INHERIT: *: PDX** .

- Setting **Awp0DatasetTypeToBeIndexedInline** to an empty string for the subtype avoids all inheritance from the parent type.

- Setting **Awp0SearchIsIndexed** to **false** to turn off indexing for the type.

By default, the indexing of **FullText** datasets is not enabled because they are indexed inline for **SpecElementRevision** and its subtypes. If you choose to enable indexing of **FullText** datasets, users see **FullText** and **SpecElementRevision** objects in search results.

Property constants

The following property constants are unique to Active Workspace:

- **Awp0FilterPropFromRefType**

  Applicable only when the property to be indexed is a reference type or a compound property whose source property is a form data file property.

  You can use the **awp0MasterFormStorageClass** compound property, available by default on all Master forms for **ItemRevision** and its subtypes, to index and filter the properties of the form.

  Specify a comma-separated list of properties that are a subset of the properties listed in the **Awp0SearchPropFromRefType** property constant. For example, you can set the following constants for the property constant reference type you want to filter:

  Awp0SearchIsIndexed

  Set the Boolean value to **true** to search on the property.

  Awp0SearchCanFilter

  Set the Boolean value to **true** to filter on the property.

  Awp0SearchPropFromRefType

  Enter the list of properties to index.

  Awp0FilterPropFromRefType

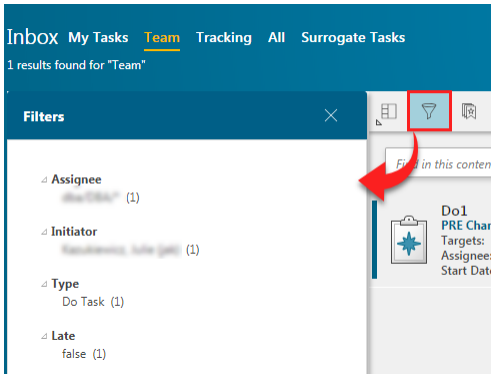
  Enter the list of properties to filter.

  Awp0SearchRefTypesNames

  Enter the referenced object type names.

- **Awp0InboxCanFilter**

  Indicates that tasks shown in the inbox can be filtered on a specific property of a workflow business object (**EPMTask** and its subtypes). The following example shows tasks found when selecting the **Team** tab.



By default, the following properties are shown as filters for workflow business objects in the inbox:

- **object_type** – The type of object.
- **due_date** – The date the object is due.
- **fnd0Assignee** – The user to whom the task is assigned.
- **fnd0Priority** – The priority of the task.
- **fnd0WorkflowInitiator** – The user who initiated the workflow on the task.

- **Awp0InboxFilterPriority**

  Sets the priority of the property of a workflow business object (**EPMTask** and its subtypes). It determines the property's order in the list of filters displayed in the inbox. The lower the value, the higher its priority and, therefore, the higher its position in the list of filters.

  Siemens Digital Industries Software recommends that you assign values from a range to accommodate additional properties in the future. For example, assign priorities such as 100, 200, and 300, instead of 1, 2, and 3.

- **Awp0SearchCanFilter**

  Indicates that the search results can be filtered on the specific property. It assumes that the property was marked for indexing using the **Awp0SearchIsIndexed** property constant. For the filters to show up correctly in the user interface, this property constant should be set for the property on its source business object.

  In a Multi-Site Collaboration environment, apply **Awp0SearchCanFilter** to published record objects so that they can be indexed using the **POM_owning_site** property.

- **Awp0SearchFilterPriority**

Sets the priority of the property that determines its order in the list of filters displayed in the client—the lower the value, the higher the priority. This means that the filter is positioned higher in the list of filters shown in the filters panel. Siemens Digital Industries Software recommends that you assign values from a range in order to accommodate additional properties in the future. For example, assign priorities such as 100, 200, and 300, instead of 1, 2, and 3.

For the filters to show up correctly in the user interface, this property constant should be set for the property on its source business object.

When a **Table** type property is marked for filtering, all valid properties of the referenced **TableRow** type are available as filters. All the table row properties get the same filter priority, so they are displayed together, vertically listed in the filter pane.

- **Awp0SearchIsIndexed**

  Indicates that the property on the business object will be indexed for searching by the indexing engine. This information is propagated through the business object hierarchy. For example, if **object_type** on **ItemRevision** is marked for indexing, all business objects under **ItemRevision** (such as **Part Revision** and **DocumentRevision**) also have their **object_type** property indexed. The following constraints apply when indexing properties:

  - Only attribute, compound, table, reference, and publication record properties can be indexed. Indexing of runtime and relation properties is not supported.
  - For multi-site searching the **POM_owning_site** property can be indexed out of the box. Apply the **Awp0SearchIsIndexed** to published objects to enable indexing.
  - To index compound properties, they must reference attribute properties from the source object.

    > Note:
    >
    > If the compound property value comes from a form, the compound property must use the form storage class in the property definition rather than the form itself, or indexing fails.

  - To index reference properties, the **Awp0SearchRefTypeNames** and **Awp0SearchPropFromRefType** property constants must contain valid values.
  - Table type property indexing is only supported for properties that reference **Fnd0TableRow** and its subtypes. Indexing is not supported for **Fnd0NameValue** and its subtypes.

    When a table type property is marked for indexing, all the valid properties of the referenced table row type are indexed. You do not need to mark individual table row properties.

  Incorrect values are omitted from indexing; no message appears.

- **Awp0SearchPropFromRefType**

Applicable when the property to be indexed is a reference type or a compound property whose source property is a form data file property.

You can use the **awp0MasterFormStorageClass** compound property, available by default on all Master forms for **ItemRevision** and subtypes, to index and filter the properties of the form.

Specify a comma-separated list of properties that are on the business objects specified in the **Awp0SearchRefTypeNames** property constant. For example, on the **owning_user** reference property on **ItemRevision**, specify a value of **user_id,user_name**.

The following rules apply:

- You can only specify attribute and compound properties.

  > Note:
  >
  > If the compound property value comes from a form, the compound property must use the form storage class in the property definition rather than the form itself, or indexing fails.

- Each property in the list specified for **Awp0SearchPropFromRefType** is matched against each business object in the list specified for the **Awp0SearchRefTypeNames** property constant. Only properties that are valid and applicable on a business object are considered for indexing. In addition, if filtering is enabled on the reference property, only the first property from the list is used.

- The first property in the list must be a string property.

Incorrect values are omitted from indexing; no message appears.

- **Awp0SearchRefTypeNames**

  Applicable only when the property to be indexed is a reference type or a compound property whose source property is a form data file property. Specify a comma-separated list of business object names that the reference property can contain. For example, on the **owning_user** reference property on **ItemRevision**, specify a value of **User**. The following rules apply:

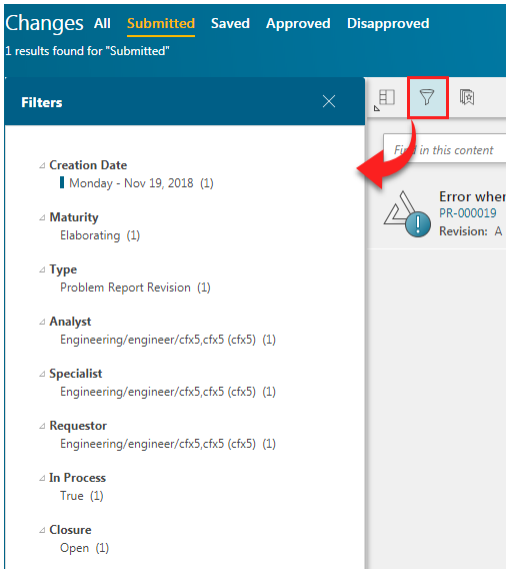
  - If no value is specified on typed reference properties, the business object that is specified as the referenced type is used as the type. For example, **release_status_list** results in **ReleaseStatus**.

  - On untyped reference properties, if no value is specified, the **POM_object** is used as the type.

  Incorrect values are omitted from indexing; no message appears.

- **Cm1ChangeCanFilter**

Indicates that the changes in the **Changes** page can be filtered on a specific property of the change business object (**ChangeItemRevision** and its subtypes). The following example shows the changes found when clicking the **Submitted** tab.



The default properties of a change object that can be filtered are:

- **creation_date** – The date the change was created.
- **CMMaturity** – The degree of completion of the overall change process (its *Maturity*).
- **object_type** – The type of change.
- **cm0Analyst** – The user assigned as the analyst.
- **cm0ChangeSpecialist1** – The user assigned as the change specialist.
- **cm0Requestor** – The user who created the change.

- **Cm1ChangeFilterPriority**

  Sets the priority of the property of the change object (**ChangeItemRevision** and its subtypes). It determines the property's order in the list of filters displayed in the **Changes** page. The lower the value, the higher its priority and, therefore, the higher its position in the list of filters.

  Siemens Digital Industries Software recommends that you assign values from a range to accommodate additional properties in the future. For example, assign priorities such as 100, 200, and 300, instead of 1, 2, and 3.

Note:

Compound properties presume that the security level of the source property of the source object is read access. This is because the compound property belongs to the target object related to the source object through the compound property.

For example, Object B has a compound property that is related to its source property on Object A. When Object B and its compound property are indexed, the indexer presumes that Object A has a security level of read access to everyone. That means that anyone with read access to the compound property of Object B could also find the source property on Object A, regardless of its security level.

Enabling searching and filtering on referenced objects or forms

Enable searching and filtering for a referenced object using a property value defined on the referenced object. You need to add or update the property constants for the property of the referenced object.

In the first example, an **ItemRevision** object has a referenced **Item** object, where the **description** contains the value **Example Text**.

In the Business Modeler IDE, find the template containing your object definitions, and find the **ItemRevision** object. On the property that references the **Item** object, add or update the following property constants:

Awp0SearchIsIndexed

Set the Boolean value to **true** to index this property.

Awp0SearchRefTypesNames

Set the referenced object type name, **Item** in this example.

Awp0SearchPropFromRefType

Set the list of properties on the referenced object type specified in **Awp0SearchRefTypesNames**. In this example, the property is **description**.

To filter the search results by the preceding property values, add or update the following property constants:

Awp0SearchCanFilter

Set the Boolean value to **true** to filter on the property.

Awp0FilterPropFromRefType

Set the list of properties on the referenced object. In the example, the property is **description**.

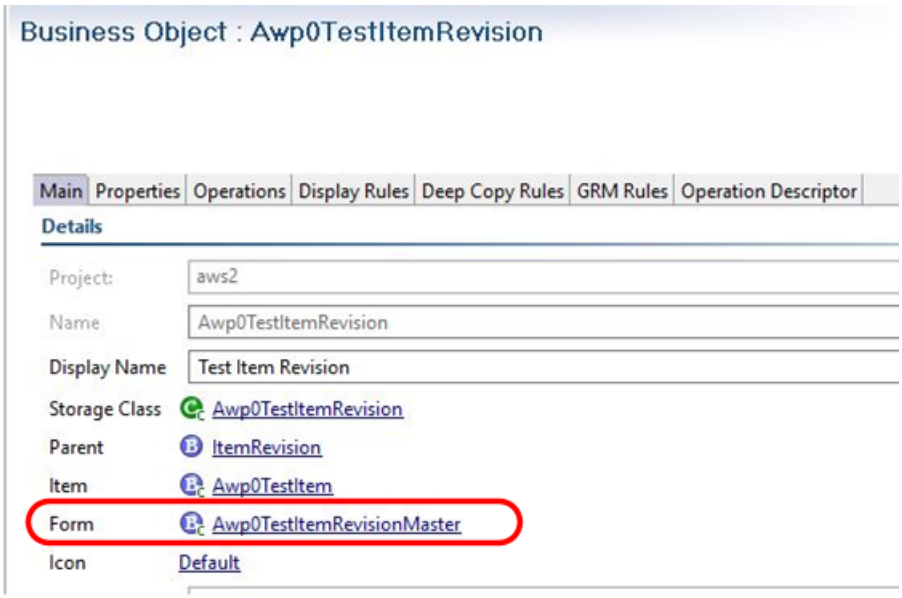
Awp0SearchFilterPriority

This property constant is optional. You can set a numeric value for priority. The lower the value, the higher the priority.

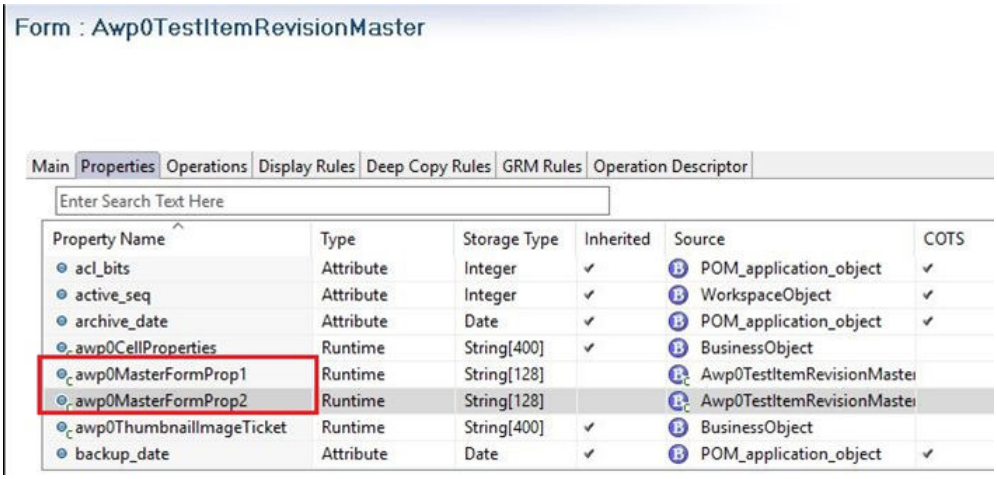
Example: Search properties of a related Master or custom form

Enable searching and filtering using the properties of a related Master or custom form. You need to add or update the property constants for the property of the related form. By default, the **awp0MasterFormStorageClass** compound property is configured for **ItemRevision**. The compound property references the data file on the Master form for **ItemRevision**.

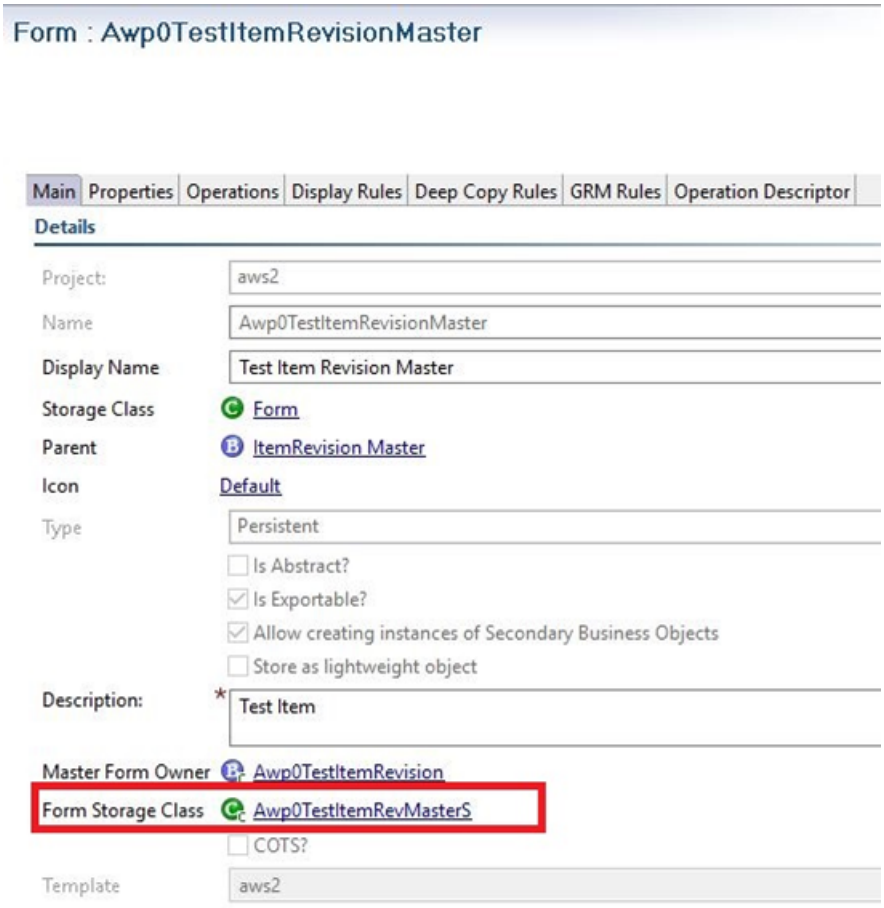
1. An **ItemRevision** has a subtype **Awp0TestItemRevision** with a Master form **Awp0TestItemRevisionMaster**:



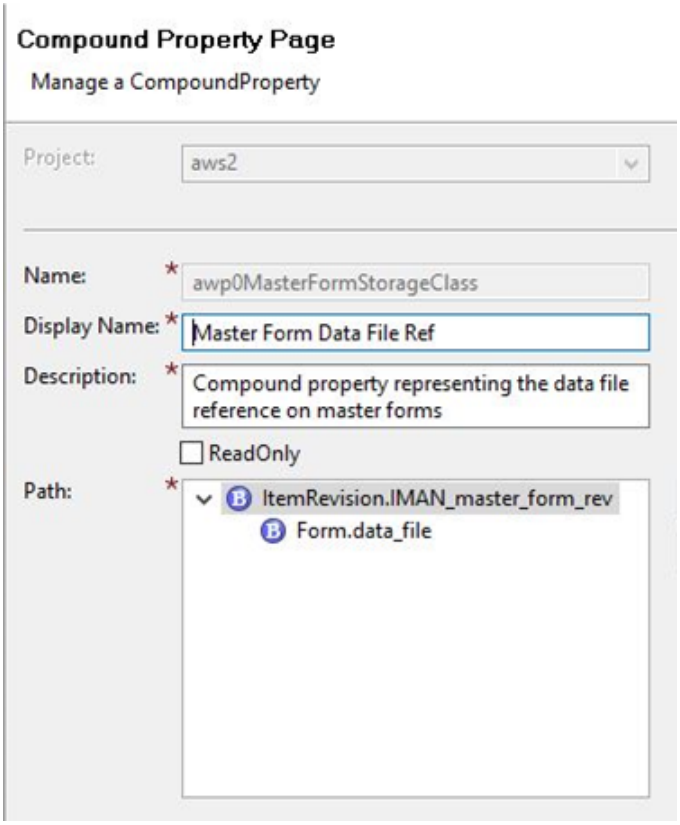
2. The Master form has two properties:



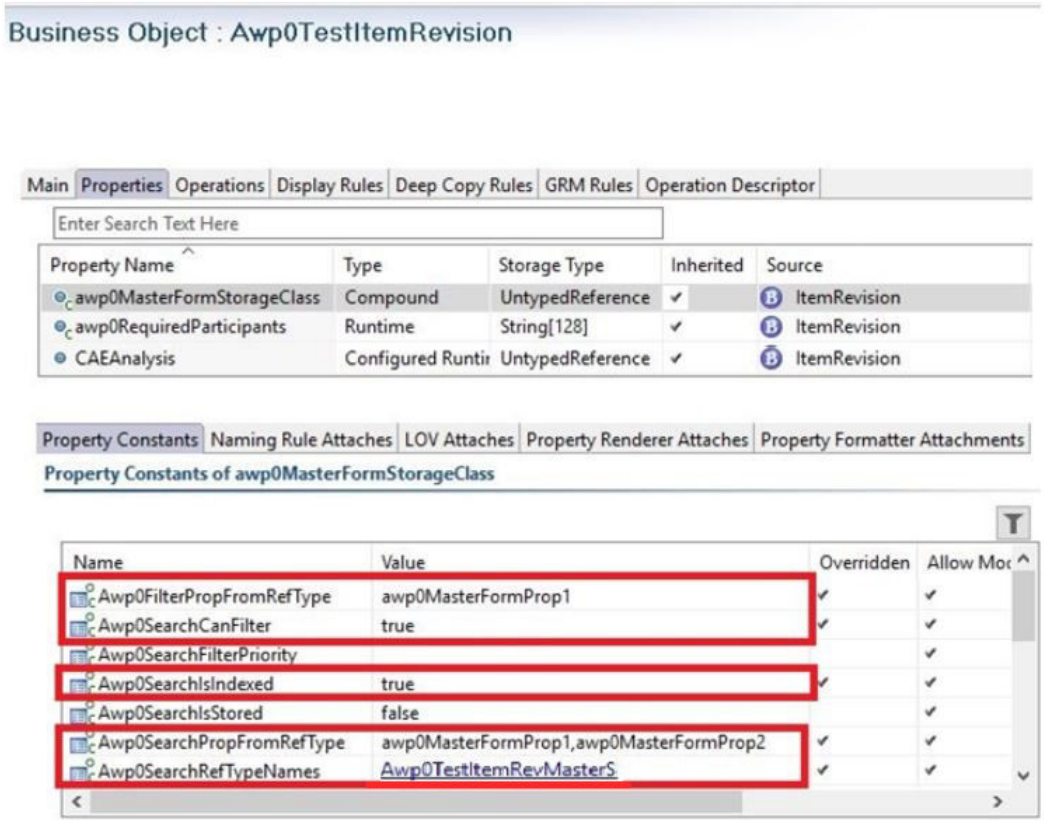
3. **Awp0TestItemRevMasterS** is the storage class name for the form.



4. **awp0MasterFormStorageClass** is a compound property that references the data file of the Master form.



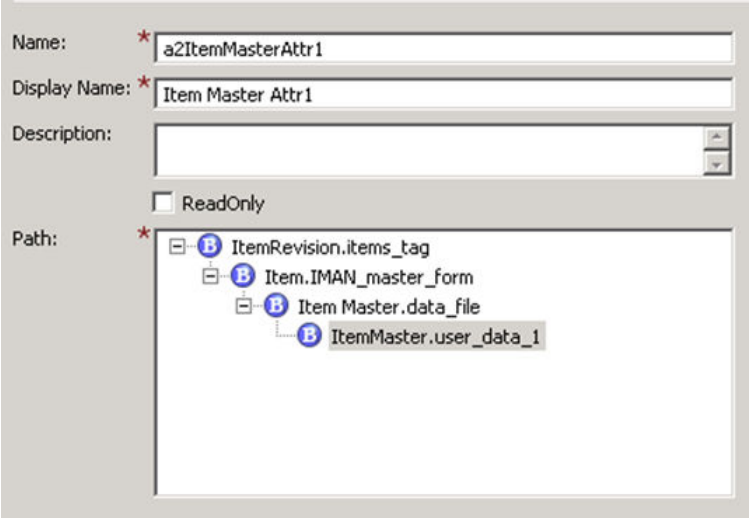
5. Configure the Master form storage class property **awp0MasterFormStorageClass** with the property constants that enable indexing, searching, and filtering.



Example: Search properties of an Item Master form

Enable searching and filtering of an Item Master form using a compound property. You need to create a compound property on a persistent attribute of the Item Master **data_file** storage class. The compound property references the data file for the Master form of the **Item**. You need to create a compound property for every attribute you want to search.

In the example, the compound property **a2ItemMasterAttr1** is created on **user_data1**, which is a persistent attribute on the Item Master **data_file** storage class.



Be sure to set the index, search and filter property constants on the new compound property.

Utilities

Using command-line utilities

In order to perform some administrative activities, you must run command-line utilities. Even if it's not the only option, sometimes using command-line utilities can also make some administrative tasks easier.

To run command-line utilities, you must have access to the Teamcenter platform command-line environment.

For information about working with command-line utilities, refer to the *Utilities Reference* in the Teamcenter documentation.

ac0_migrate_s2cldata

> Note:
>
> If you have used Active Collaboration for Retail or Active Collaboration prior to Active Workspace 5.1, you can perform a one-time migration using this utility to migrate your existing questions and comments to the new Active Collaboration discussions feature.

Migrates previous Active Collaboration questions and comments (**S2clSocial** objects) to the new Active Collaboration discussions feature that uses **Ac0ActiveCollaboration** objects.

> Caution:
>
> Perform this migration only once to prevent duplication of data.

SYNTAX

ac0_migrate_s2cldata [**-u**=*admin-user-id*] {[**-p**=*password* | **-pf**=*password-file*]} [**-g**=*group*] **-verbose** **-report**=*report-file-path* **-h**

ARGUMENTS

-u

Specifies the user ID.

A user with administration privileges is used as the value name for the user ID. If **-u** is used without a value, the operating system user name is automatically applied.

> Note:
>
> If Security Services single sign-on (SSO) is enabled for your server, the **-u** and **-p** arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-p

Specifies the password.

If used without a value, the system assumes a null value. If this argument is not used, the system assumes the *user-ID* value to be the password.

This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file.

-g

Specifies the group associated with the user, which must be **dba**.

-verbose

Outputs low-level processing information to log and report.

-report

Specifies the path where the report file should be stored.

-h

Displays help for this utility.

EXAMPLE

Migrate the existing **S2clSocial** objects to **Ac0ActiveCollaboration** objects:

```
ac0_migrate_s2cldata -u=admin -p=pwd -g=dba -verbose
-report=C:\temp\admin_data\active_collaboration_objects.xml
```

bomindex_admin

Adds structured content to the search index.

SYNTAX

bomindex_admin [**-u**=*user-id* {**-p**=*password* | **-pf**=*password-file*} **-g**=*group*] **-logfile**=*location_of_logfile* **-function**=[**create** | **delete** | **list** | **upgrade**] **-inputfile**=*location_of_inputfile*

ARGUMENTS

-u

Specifies the user ID. This is a user with administration privileges.

> Note:
>
> If Security Services single sign-on (SSO) is enabled for your server, the user and password arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-pf

Specifies the password file that holds the cleartext or encrypted password. For enhanced security, use a password file instead of the password. If the **-pf** argument is not used, the system uses the given password.

-p

Specifies the password.

This argument is mutually exclusive with the **-pf** argument.

-g

Specifies the group associated with the user.

If used without a value, the user's default group is assumed.

-logfile

Specifies the location of the log file written by the utilities. You can specify a different location for each utility.

-function=*function-name*

Performs the following functions:

create	Creates the **BOMIndexAdminData** objects based on the input file.

delete	Finds the **BOMIndexAdminData** objects in the input file and marks them as deleted.
list	Creates the input file for update or delete operations for existing **BOMIndexAdminData** business objects. The generated file also reports **BOMIndexAdminData** properties such as **window-uid**.
upgrade	Upgrades the definition of BOM index tables when the property set is modified.

-inputfile

Specifies the location of a file containing the list of structure objects to index. The input file line format is as follows:

item-query-string | *item-revision-ID* | *base-revision-rule* | *effectivity-unit* | *effectivity-end-item-query-string* | *effectivity-date (dd-mmm-yyyy hh:mm:ss)* | *variant-rules* | *subscribers* | *closure-rules*

An example of an input file (**bomindex_admin_input.txt**):

```
item_id=HDD-0527 | B | Any Status; Working | 5 | item_id=HDD-0527 |
31-May-2013 00:00:00 | vrule1:item_id=OwnItem1:B,vrule2:,vrule3:item_id=OwnItem3:A |
MMV | closurerule1
```

- **effectivity-unit**

  If you have multiple effectivity units, their numbers must be comma-separated. Also, you must repeat the effectivity end item query string for each effectivity unit, for example:

  ```
  | 5,10,12 | item_id=HDD-0527,item_id=HDD-0527,item_id=HDD-0527 |
  ```

  The maximum number of effectivity units you can specify is 960.

- **variant-rules**

  The variant rules (also known as saved variant rules) are comma-delimited, and follow this format:

  SVR-name:owning-item-query-string:owning-itemrevision-ID

  The topline item revision is the default owner.

  The maximum number of saved variant rules you can specify is 960.

- **subscribers**

  (Optional) You may specify:

  - **VDS**

Specifies that this product configuration is indexed for viewing using the Visualization Data Server. This makes the structure available faster in visualization. **VDS** requires deployment of the Visualization Data Server.

- **closure-rules**

  (Optional) If a closure rule is applied for a configuration, content in the structure (excluded by the closure rule) does not appear in **where used** query results for top-level contexts.

- **structure-type**

  (Defunct) The type of structure that the product represents. **OCC** is the only valid value.

- **owning-user**

  (Optional) If Visualization for MMV is enabled for the product, specify the user who owns the MMV delta collection dataset.

- **MMVIdxAccessControllers**

  (Optional) Specify the users that control access to MMV index files.

HOW TO SPECIFY OWNING USER AND MMVIDXACCESSCONTROLLERS

Each VDS site can be configured to run as a different user. **BOMIndexAdminData** table entries are returned according to the permission specified for the configured VDS user. This helps you implement export compliance using these attributes.

Example:

Site owners configured for each VDS site:

- **USA** is **VDSadmin**
- **Mexico** is **mex_VDSadmin**
- **Canada** is **can_VDSadmin**
- **China** is **chi_VDSadmin**

BOMIndexAdminData (BIAD) entries are defined as follows:

BIAD	Product	Revision Rule	Structure Type	MMV Owning User	MMV Access Users
Biad1	Ship	Latest Working	BVR	**VDSadmin**	**mex_VDSadmin** **can_VDSadmin**
Biad2	Truck	Latest Working	BVR	**VDSadmin**	**mex_VDSadmin** **can_VDSadmin** **chi_VDSadmin**
Biad3	Car	Latest Working	BVR	**VDSadmin**	**chi_VDSadmin**

To summarize the access for each VDS site:

- **USA** site user **VDSadmin**

  Access to **Biad1**, **Biad2**, and **Biad3** because it is specified as the MMV owning user.

- **Mexico** site user **mex_VDSadmin**

  Access to **Biad1** and **Biad2** only. No access to **Biad3**.

- **Canada** site user **can_VDSadmin** user

  Access to **Biad1** and **Biad2** only. No access to **Biad3**.

- **China** site user **chi_VDSadmin** user

  Access to **Biad2** and **Biad3** only. No access to **Biad1**.

EXAMPLE

The following command creates a search index of structures:

```
bomindex_admin -u=username -p=password -g=dba
-logfile=C:\Scratch\log\log1.txt
-function=create -inputfile=C:\Scratch\log\bomindex_admin_input.txt
```

OVERRIDING EFFECTIVITY

When you want to specify override effectivity, do not specify it in the input file containing the product configurations to index. The override effectivity in the input file is ignored during index generation, causing a discrepancy between the indexed BOM and the BOM in use.

To set override effectivity during index generation, add the effectivity data to a Revision Rule.

For example, the Revision Rule might contain:

Z_ACE_DateOverride_Rule23_10Jan2020

which includes entries for the effective date **10-Jan-2020 00:00:00**.

The corresponding input file entry for **bomindex_admin** would have this corresponding effectivity override entry:

item_id=ACE_KK_EC01 | A | Z_ACE_DateOverride_Rule23_10Jan2020 | | | | | |

data_report

Gathers data from participating Multi-Site sites in the federation and generates reports on data inconsistencies. Reports are generated for individual sites and for the overall Multi-Site federation. This data is presented in the Active Workspace Multi-Site Assistant. (When working with the **data_report** utility, sites in the federation are the sites defined by **MS_Dashboard_Supported_Sites**.)

SYNTAX

data_report -u=*user-ID* {**-p=***password* | **-pf=***password-file*} **-g=***group*
[**-site=***site-name*]
[**-dir=***report-directory*]
[**-format=***report-format*]
[**-sql_file=***sql-file-name*]
[**-include=***included-report-categories*]
[**-exclude=***excluded-report-categories*]
[**-date_format=***date-filter-type* [**-from=***start-date*] [**-to=***end-date*]]
[**-object_type=***type*]
[**-f=**{**collect_data** | **generate_report**}]
[**-h**]

ARGUMENTS

-u

Specifies the user ID. The user must have administrative privileges.

If Security Services single sign-on (SSO) is enabled for your server, the **-u** and **-p** arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-p

Specifies the user's password. This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file. This argument is mutually exclusive with the **-p** argument.

-g

Specifies the group associated with the user.

-site

Specifies the name of a specific site for which data is gathered and a report is generated. If no site is specified, reports are generated for all sites and the overall Multi-Site federation (as defined by **MS_Dashboard_Supported_Sites**).

-dir=

Specifies directory in which reports are saved. By default, reports are saved in the location specified by **TC_TMP_DIR**.

-format

Specifies the format for reports. Valid values are **csv** (the default) and **json**.

-sql_file

Specifies a JSON file containing custom SQL data queries or predefined filters.

-include

Specifies the categories of issues to include in reports. Valid values are **itemOwnershipReports**, **duplicateIDReports**, and **objectOwnershipReports**. By default, all listed categories are included. Multiple values must be separated by commas.

The **objectOwnershipReports** analysis uses the external closure rules defined in **MSA_ObjectOwnershipCR**. As the **objectOwnershipReports** analysis may take significant time, consider first running **data_report** excluding **objectOwnershipReports**, and then later running only the **objectOwnershipReports**.

-exclude

Specifies the categories of issues to be excluded from reports. Valid values are **itemOwnershipReports**, **duplicateIDReports**, and **objectOwnershipReports**. Multiple values must be separated by commas.

-date_format

When specifying a reporting date range, **-date_format** specifies the date type. Valid values are **creation** (the date the object was created) and **last_modified** (the date the object was last modified).

-from

Used with **-date_format** to specify, inclusively, the start date and time for reporting. The format of the date is *"YYYY-MM-DD HH:MM:SS"* and must be inside the double quotes due to the space between the year and the hour.

-to

(Optional) Used with **-date_format** to specify, inclusively, the end date and time for reporting. The format of the date is *"YYYY-MM-DD HH:MM:SS"* and must be inside the double quotes due to the space between the year and the hour. If not given, the current date and time is used.

-object_type

Specifies an object type to be included in the report. All item and item subtypes are included.

-f

Specifies the function that **data_report** should perform. Valid values are **collect_data** (gather updated data from sites) and **generate_report** (generate reports based on gathered data). By default, **data_report** performs both actions.

-h

Displays help for this utility.

EXAMPLES

Required log-in information is omitted from the following examples.

- Gather data and generate reports for all sites defined by **MS_Dashboard_Supported_Sites**:

```
data_report
```

- Gather data for a specific site:

```
data_report -site=site01 -f=collect_data
```

- Generate reports for all sites and the Multi-Site federation using data previously collected:

```
data_report -f=generate_reports
```

- Generate reports for all sites and the Multi-Site federation for only specific categories of issues:

```
data_report -include=itemOwnershipReports,duplicateIDReports
```

- Gather data and generate reports for a specific site for a specific time period:

```
data_report -site=site01 -date_format=creation -from="2020-06-01 00:00:00"
-to="2020-06-30 23:59:59"
```

- Gather data and generate reports for all sites and the Multi-Site federation using custom SQL data queries:

```
data_report -dir=d:\reports -sql_file=d\reports\msPredefinedSQLs.json
```

generate_admin_data_report

Generates a report showing the specified administration data for the site where you run the utility or for an export package. The export package can be from a remote site.

The report contains HTML pages for the administration data objects, showing their properties with hyperlinks to referenced objects. If an object is referenced by other objects, its HTML page contains a where-used table that indicates the categories and objects that have references to the current object.

The report has a summary showing all the administration data types included in the report and the instances of each element present within the category. The report also has a glossary page with descriptions of the administration data categories and the elements available in each of the categories.

SYNTAX

generate_admin_data_report -u=*user-ID* {**-p=***password* | **-pf=***password-file*}
-g=*group*
-adminDataTypes=*Admin-data1,Admin-data2,...,Admin-dataX* | **all**
[**-inputPackage=***input-package-path*]
-outputDir=*path-to-directory-for-report-files*
[**-listTypes**]
[**-h**]

ARGUMENTS

-u

Specifies the user ID. The user must have administrative privileges.

If Security Services single sign-on (SSO) is enabled for your server, the **-u** and **-p** arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-p

Specifies the user's password.

This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file.

For more information about managing password files, see *Utilities Reference* in Teamcenter help.

This argument is mutually exclusive with the **-p** argument.

-g

Specifies the group associated with the user.

-adminDataTypes

Specifies the types of administrate data to include in the compare report. You provide the data types as a comma-separated list (no spaces). You may also specify the **all** value to include all data types defined in the local system or the specified input package.

> Tip:
>
> Use the **-listTypes** argument to get a list of available administration data types.

If the report contains multiple data types, it includes a where used table showing where each object is referenced.

-inputPackage

Specifies the full path, including the file name, of the export administration data package from the site for which the report is generated. If you do not specify this argument, the utility generates a report for the local site.

-outputDir=

Specifies the path to directory where you want the report saved. You must specify this argument.

-listTypes

Displays a list of the available administration data types that you can include in the report.

-h

Displays help for this utility.

ENVIRONMENT

As specified in *Manually configure the Teamcenter environment* in *Utilities Reference* in Teamcenter help.

This is a Java utility that, by default, has the maximum Java heap size set to 1024M. For reports that contain a large number of objects, you may need to increase maximum Java heap size to avoid out-of-memory errors or poor performance. If possible, set the maximum heap to at least to 4096M for large reports. You can set this value using the **BMIDE_SCRIPT_ARGS** environment variable, for example:

```
set BMIDE_SCRIPT_ARGS=-Xmx4096M
```

> Note:
>
> Java standards require that no more than 25 percent of total RAM be allocated to virtual memory (VM). If the amount allocated to the Java VM exceeds this percentage, degradation of performance can occur.

FILES

As specified in *Log files produced by Teamcenter* in *Utilities Reference* in the Teamcenter help.

EXAMPLES

- Generate a list of the administration data types that you can export:

```
generate_admin_data_report -u=admin-username -p=admin-password -g=dba
-listTypes
```

- Generate a report containing the preferences and their values at the local site:

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

- Generate a report containing the Access Manager and Organization administration data from an export package of a remote site:

```
generate_admin_data_report -u=admin-username -p=admin-password -g=dba
-adminDataTypes=AccessManager,Organization
-inputPackage=C:\temp\admin_data\siteB\siteB.zip
-outputDir=C:\temp\admin_data\siteB\am_and_organization_report
```

log-level

Changes the log level of Teamcenter microservice framework components and compliant microservices. Among these are the service dispatcher and the microservices **configurator**, **filerepo**, and **MPS**. Administrators can change logging levels without having to stop and restart the services.

Syntax

Host operating system	Syntax
Linux	**./log-level** *operation [argument]* On Linux hosts, it is necessary to set permissions on the *log-level.sh* file. To do so, enter the command `chmod +x log-level.sh`
Windows	**log-level** *operation [argument]*

Arguments

get

Gets the current log level of a microservice.

```
log-level get MICROSERVICE_NAME
```

```
>log-level get filerepo
Microservice Name: filerepo
Current Log Level: WARN
Possible Values: [INFO, ERROR, DEBUG, WARN, TRACE]
```

Available log levels depend on the microservice. See Server manager logging levels in the Teamcenter help for a description of log levels.

getall

Gets the current log level of all running microservices.

```
log-level getall
```

```
>log-level getall
-----------------------------------
|  Microservice Name   | Log Level |
-----------------------------------
| filerepo             | WARN      |
| mps                  | ERROR     |
| servicedispatcher    | INFO      |
-----------------------------------
```

set

Changes the log level of a microservice. Possible values are INFO, ERROR, DEBUG, WARN, and TRACE.

```
log-level set MICROSERVICE_NAME LOG_LEVEL
```

```
>log-level set servicedispatcher DEBUG
INFO: Successfully updated log level for microservice servicedispatcher.
```

reset

Changes the current log level back to the default log level for a microservice.

```
log-level reset MICROSERVICE_NAME
```

```
>log-level reset servicedispatcher
INFO: Successfully reset log level for microservice  servicedispatcher.
```

help

Prints the instructions for using the log level command line interface.

```
log-level help
```

Environment

The utility works on the master microservice framework node for a Teamcenter environment, irrespective of whether the host is running a Linux or Windows operating system.

The utility is located in the *TC_ROOT*/*microservices*/*bin* folder and must be run from this location.

req_word_html_converter

As an administrator, you can selectively convert requirement content in HTML format to Microsoft Word format (or the reverse, depending on the option selected). You can perform a selective conversion by providing a criteria file or a comma separated file containing fullText UIDs or directory containing multiple such Fulltext UID files. In non-permanent selective conversion from rich text to Microsoft Word, the converted requirements have the necessary named reference attachments as **MSWordXPart**; however, the content type remains rich text. Similarly, in non-permanent conversions from Microsoft Word to rich text, the converted requirements have the named references attachments as **Arm0HTML** and **Arm0HTMLIMG**, but the content type is still rich text.

Note:

Before you run this utility, ensure that the Active Workspace Requirements Management feature is installed. Several files are created in the transient volume folder when you run the utility:

- *failed_ID.txt* contains failed UIDs separated by commas
- *invalidIDs.txt* contains invalid UIDs
- *validIDs.txt* contains valid UIDs
- *dumpLogs.log* if you use the **dumpLogs** option
- The utility performs conversion for the following objects only: **SpecElementRevision**, **SpecElement**, or **SpecificationRevision**.

SYNTAX

req_word_html_converter [**-u=***user-id* **-p=***password* | *password-file* **-g=***group*]
] [-path=*full file path of HtmlConverter01.exe*
] [-dumpLogs] [-forceUpdate] [-h][-htmlToWord] [-wordToHtml]
[-processObjectList=*full path of the text file containing FullTextUIDs* **-in=***full file path of criteria file*
][-permanentConvert] [-dryRun]

ARGUMENTS

-u=*user_id*

Specifies the user ID to be used for the upgrade.

This is a user with Teamcenter administration privileges.

-p=*password*

Specifies the password for the specified user ID.

-g=*group_name*

Specifies the group associated with the user.

-path=*full file path of WordHtmlConverter.exe (including the .exe extension)*

Specifies the full path to the **WordHtmlConverter.exe** utility, including the filename **WordHtmlConverter.exe**.

-dumpLogs

(Optional) Dumps a detailed debug log with more information about the point in the code the utility is failing or which full-text dataset is causing the error.

-forceUpdate

(Optional) Forces the update and repair of all requirements in database even if they were previously converted.

-h

Displays help for this utility.

-htmlToWord

Converts requirements from HTML format to Microsoft Word.

-wordToHtml

Converts requirements from Microsoft Word format to HTML.

-processObjectList=*<full file path of the process object list text file>*

Specifies the full path of the text file containing FullText UIDs. The text files must contain FullText IDs separated only by commas; no spaces allowed.

-in=*<full file path of the criteria file>*

Performs a selective conversion of an entire requirement specification structure to html. The input is a criteria file that defines this structure.

The schema for the file is as follows:

KEYWORD_SEPARATOR=*KWS*

KEY_VALUE_SEPARATOR=*KVS*

RULE_SEPARATOR=*RS*

keys *KWS key1=value1 KVS keyN=valueN RS* **rev_rule** *KWS revision-rule RS* **topline_rev** *KWS* **topline rev**

keys *KWS key1=value1 KVS keyN=valueN RS* **rev_rule** *KWS revision-rule RS*

keys *KWS key1=value1*

Note the following conditions:

- The **KEYWORD_SEPARATOR**, **KEY_VALUE_SEPARATOR**, and **RULE_SEPARATOR** entries are required and you must enter in the order indicated. These entries define the separators that segregate the key-value pairs and keywords from corresponding values. You cannot use the equal sign (**=**) as the value for these entries. For example, the entry **RULE_SEPARATOR= =** is invalid.

- Separate all entries with the new-line character (**\n**).

- Starting in the fourth row, define the entries as follows:

  - *Segment 1 (Required)*

    Consists of multi-field key-value (MFK) pairs. *Multifield keys* are IDs assigned to each object to ensure their uniqueness in the database. Based on the MFK, specifications/requirements are retrieved, and then further configuration is applied based on Segment 2 and Segment 3. This segment is required to uniquely identify the top object in the database.

    Syntax

    keys *KWS key1=value1 KVS key2=value2 KVS keyN=valueN*

    Example

    keys : item_id=REQ-000002 , object_type=Requirement

  - *Segment 2 (Optional unless Segment 3 is defined*)

    Denotes the revision rule to apply to the revision retrieved based on the MFK pairs in Segment 1.

    If you do not define this segment, then the defined revision rule as read from preference **TC_config_rule_name** is applied.

    Syntax

    rev_rule *KWS revision_rule_name*

    Example

    rev_rule : Latest Working

  - *Segment 3 (Optional)*

    Defines the revision of the item retrieved on the basis of the MFK pairs defined in Segment 1. You can use this segment to determine the structure of interest. If you do not define this segment, then the latest revision is considered for configuring structure. If this segment is defined then you must define Segment 2 also.

For example, if the MFK pairs in Segment 1 return a particular item such as **item_id=REQ-000002**, then there can be different structures for different revisions of this item. Revision A as a top line might contain 6 children items; revision B might contain 12 children items.

Syntax

topline_rev *KWS topline_revision*

Example

topline_rev : A

- *Example: valid input criteria file*

  KEYWORD_SEPARATOR=:

  KEY_VALUE_SEPARATOR=,

  RULE_SEPARATOR=|

  keys: item_id=REQ-000001

  keys: item_id=REQ-000001 , object_type=Requirement | rev_rule:Latest Working

  keys: item_id=REQ-000001 | rev_rule:Precise Only

  keys: item_id=REQ-000001 | rev_rule:Any Status; Working | topline_rev:A

- *Example: invalid input criteria file*

  KEYWORD_SEPARATOR= = (invalid because the equals sign (**=**) is not a valid separator)

  KEY_VALUE_SEPARTOR=, (invalid because **KEY_VALUE_SEPARATOR** is misspelled)

  RULE_SEPARATOR| (invalid because the equals sign (**=**) is missing)

  keys: item_id=REQ-000001 | rev_rule: | topline_rev:A (invalid because the revision rule name is not provided)

  rev_rule:Latest Working | keys: item_id=REQ-000002 , object_type=Requirement (Invalid because Segment 1, Segment 2, and Segment 3 must be defined in that order: Segment 1 is the MFK, Segment 2 is the revision rule, and Segment 3 is the topline revision)

  keys: item_id=REQ-000003 | topline_rev:A (Invalid because Segment2 is skipped and directly Segment3 is defined)

-permanentConvert

(Optional) Permanently converts requirements to one of the following formats:

- If you include the **-wordToHtml** switch, converts to HTML format, which is editable in the CK Editor in the **Documentation** tab.
- If you include the **-htmlToWord** switch, converts to Word format, which is not editable in the CK Editor in the **Documentation** tab.

-dryRun

These files are created: failed_ID.txt with failed UIDs separated by comma, invalidIDs.txt with the invalid UIDs, and validIDs.txt with the valid. The conversion does not take place.

The files are described below:

1. invalidIDs.txt: any UID not present in the database or has a blank content_type property.
2. failed_ID.txt : any UID having corrupted data, cannot be opened in Word, the user does not have write access on it, or is checked out by another user or a replica object.
3. validIDs.txt : All UIDs are valid.
4. alreadyConvertedIDs.txt : UIDs that are already HTML for wordTOHtml conversion case or already Word for HtmlToWord conversion, is contained in this file.

EXAMPLES

req_word_html_converter -u=*user_id* -p=*password* -g=*group* -path=*full file path of WordHtmlConverter.exe* -forceUpdate -htmlToWord

req_word_html_converter -u=*user_id* -p=*password* -g=*group* -path=*full file path of WordHtmlConverter.exe* -dryrun -htmlToWord

req_word_html_converter -u=*user_id* -p=*password* -g=*group* -path=*full file path of WordHtmlConverter.exe* -dumpLogs -htmlToWord

req_word_html_converter -u=*user_id* -p=*password* -g=*group* -path=*full file path of WordHtmlConverter.exe* -in=*full path of the criteria file for selective conversion* -wordToHtml

req_word_html_converter -u=*user_id* -p=*password* -g=*group* -path=*full file path of WordHtmlConverter.exe* -processObjectList=*full path of the process uidst text file* -wordToHtml

req_word_html_converter -u=*user_id* -p=*password* -g=*group* -path=*full file path of WordHtmlConverter.exe* -dir=*full path of the folder that contains text files with process uids* -htmlToWord

req_word_html_converter -u=*user_id* -p=*password* -g=*group* -path=*full file path of WordHtmlConverter.exe* -permanentConvert -htmlToWord

Caution:

The following conditions are not supported:

- Creating a requirement in Teamcenter Rich Client and modifying it in Active Workspace (and vice-versa).
- Creating a requirement in Teamcenter Rich Client and creating a sibling in Active Workspace and exporting to Word. The sibling cannot be edited.
- Creating a requirement in Teamcenter Rich Client and exporting it using microservices.

To create a specification that can be edited in Active Workspace, use **IMPORT SPECIFICATION** with the **Enable Editing** checkbox selected, or use the microservice-based import.