SIEMENS

Active Workspace 5.2

Active Workspace Administration

AW058 - 5.2

Contents

Settings and performance

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.
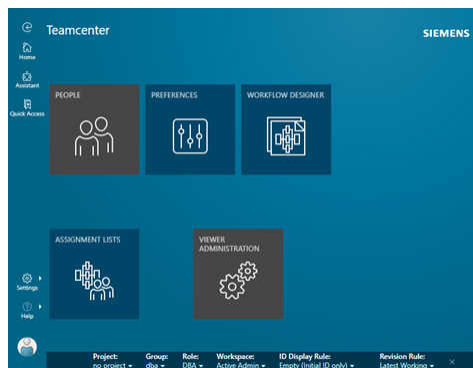
How do I enable it?

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, modify, and remove groups, roles, and users.

- **Preferences**

  Manage your Teamcenter preferences from within Active Workspace.

- 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. 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.
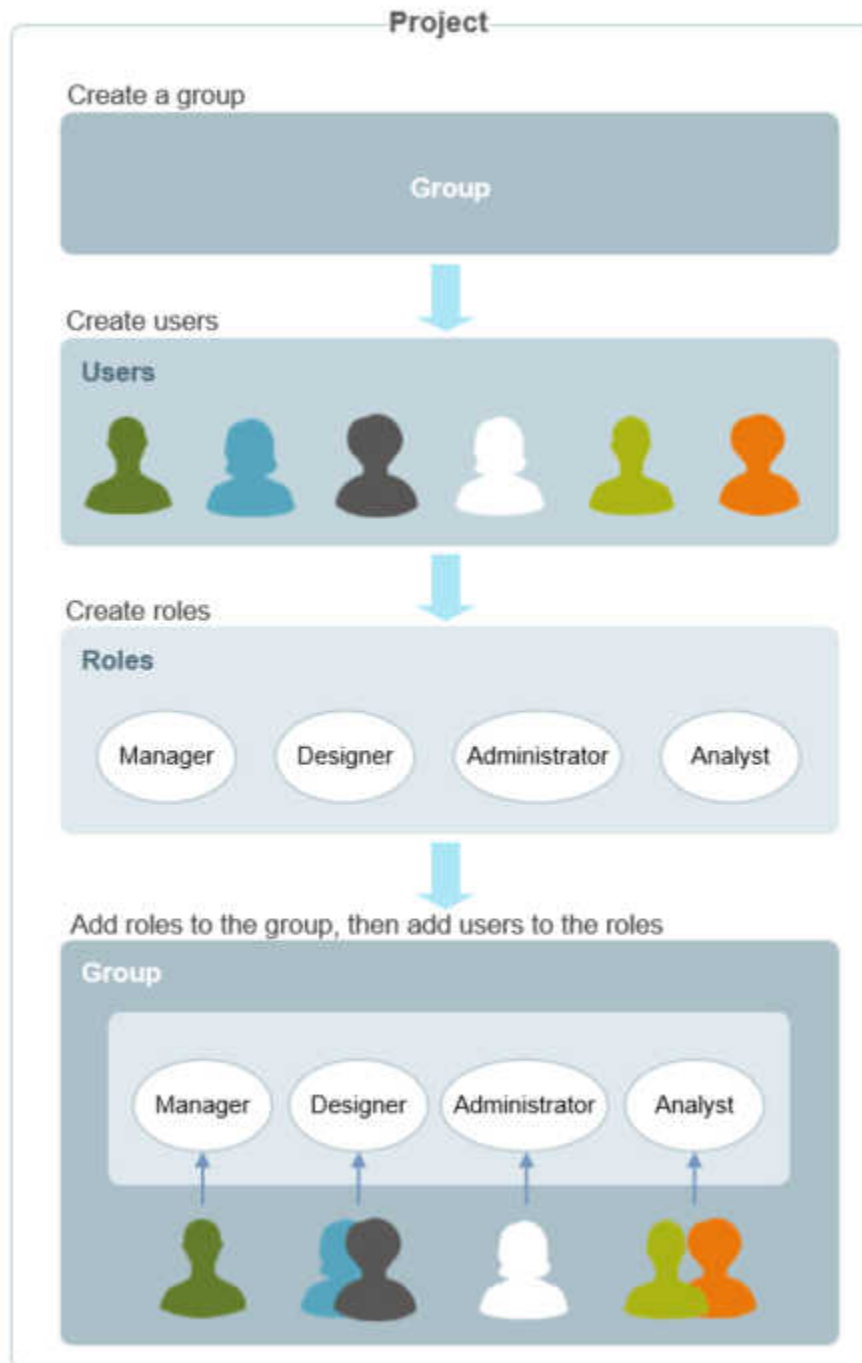
Managing users, groups, and roles

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**, **modify**, and delete groups.

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.
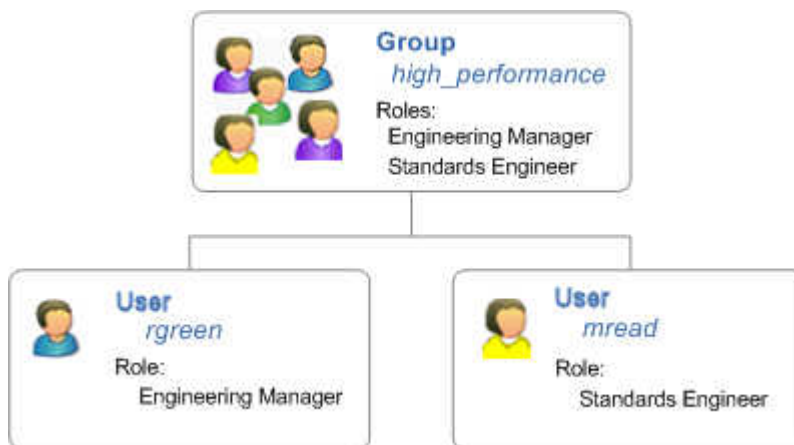
- Assign authorized data access privileges to a group.

- 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**.
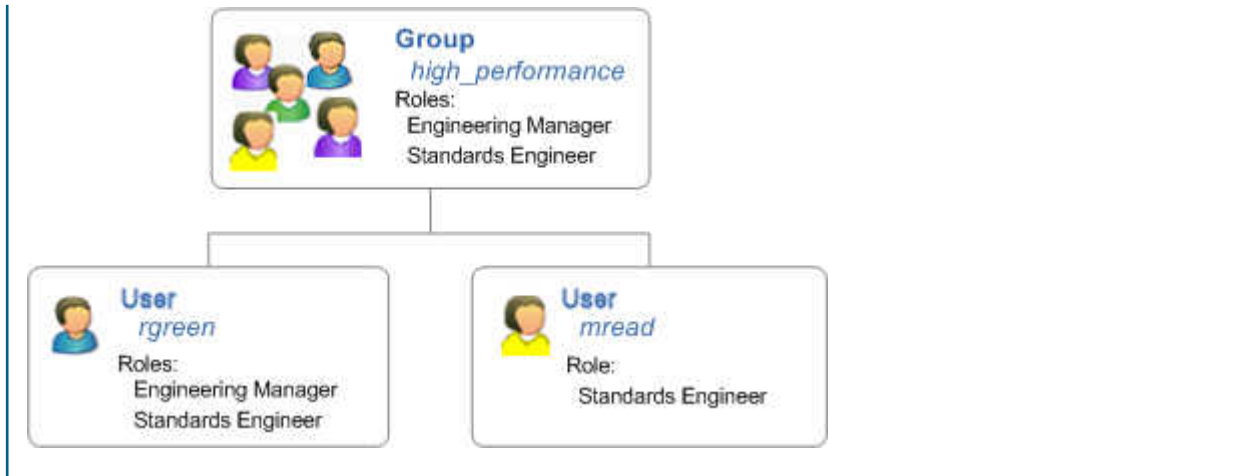
Users

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**.

User
rgreen
Default group:
   high_performance
Role:
   Standards Engineer
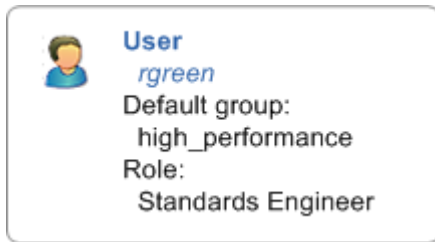
How to manage groups, roles, and users in Active Workspace

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.
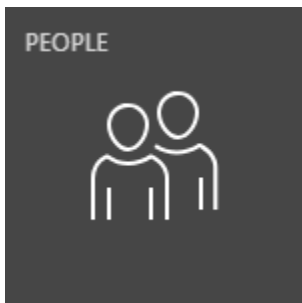
> Note:
>
> The **PEOPLE** tile is visible in both the **Active Admin** and **Default** workspaces. It *may* be visible in the **General User** workspace.
>
> You can create your own workspace mapped to a special group of non-**dba** group users and add the **PEOPLE** tile to it. This allows users to 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.
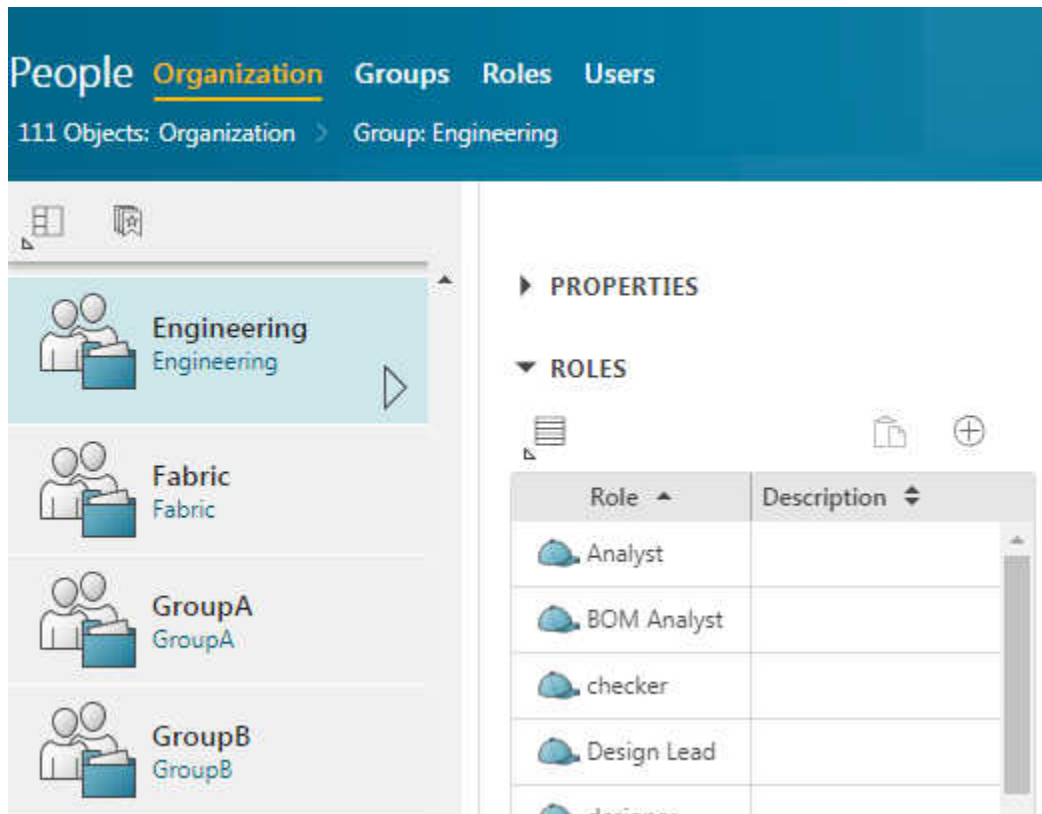
Creating groups, roles, and users

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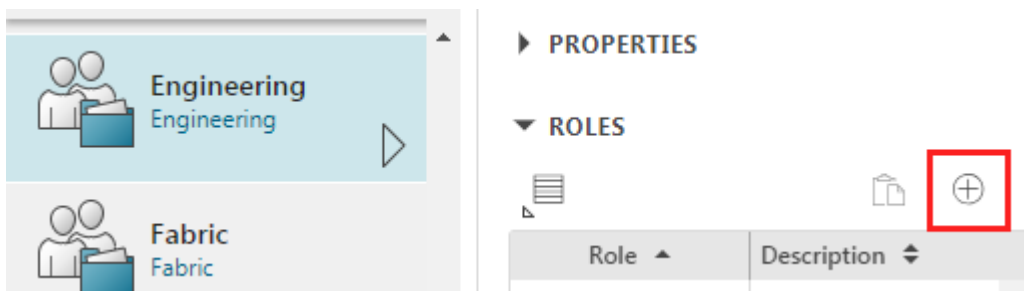
3. In the **Add** panel, do one of the following:

- In **New**, enter a role and description for the new role.

- In **Search**, 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**.
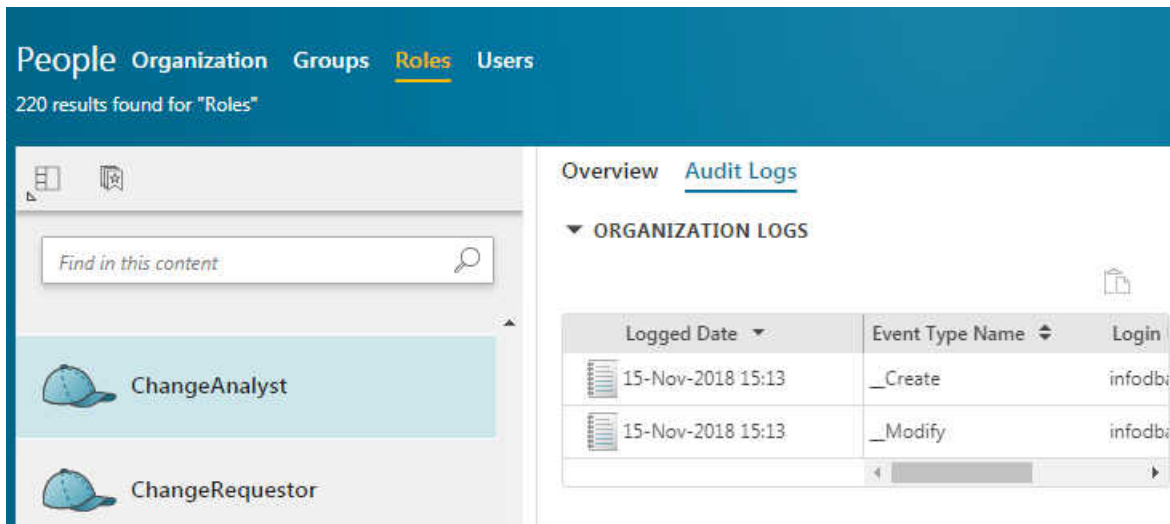
Adding the Access tab to view user access rights

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"/>
```
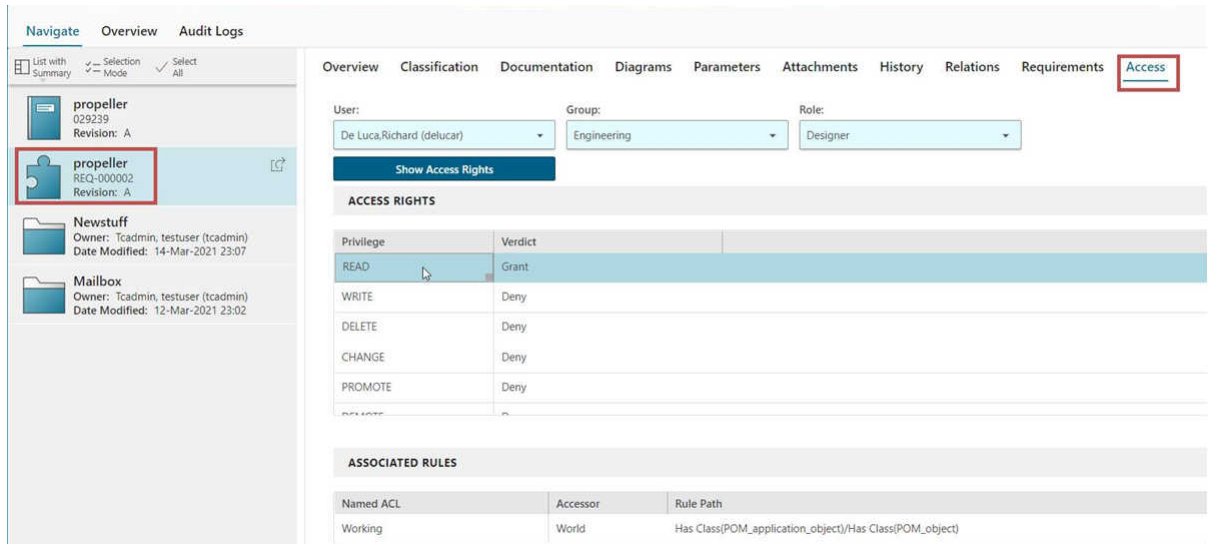

Add or change a user password

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**.
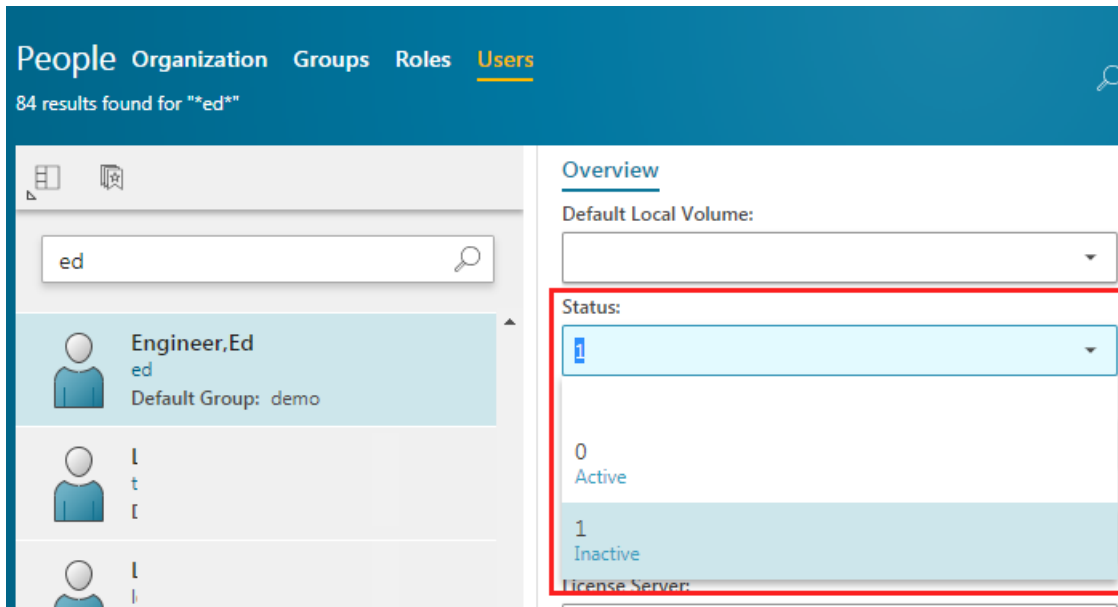
Delete a user from a group

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.

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.
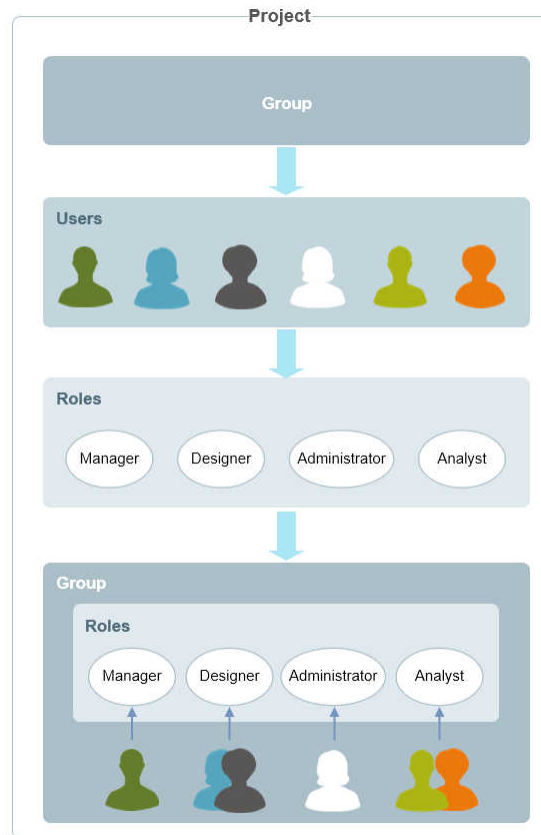
Control access to your project data

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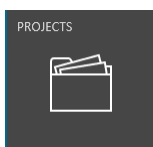
Depending on your role, you can perform the following project-related tasks in Active Workspace:

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.
	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**.
    >
    >
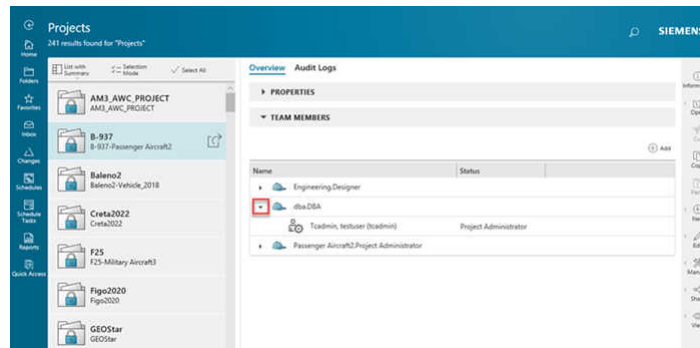
Add a user to a project

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

2. From **TEAM MEMBERS**, 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**.
>
>
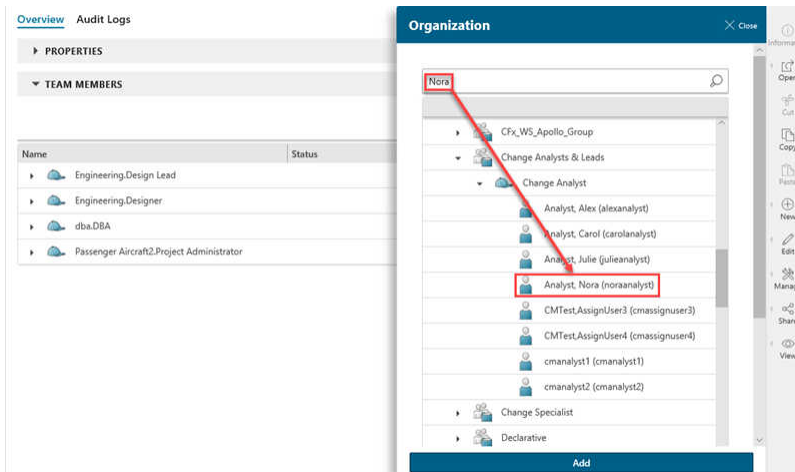
Add a role to a project

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

2.   From **TEAM MEMBERS**, 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.

> **Note:**
>
> You cannot remove a user from a role. You must remove the role.
>
> To remove a role from the project, select the role and click **Remove** ⊖.

> **Example:**
>
> From **Organization**, filter on **Change Analyst**. Then, select the role and click **Add**.
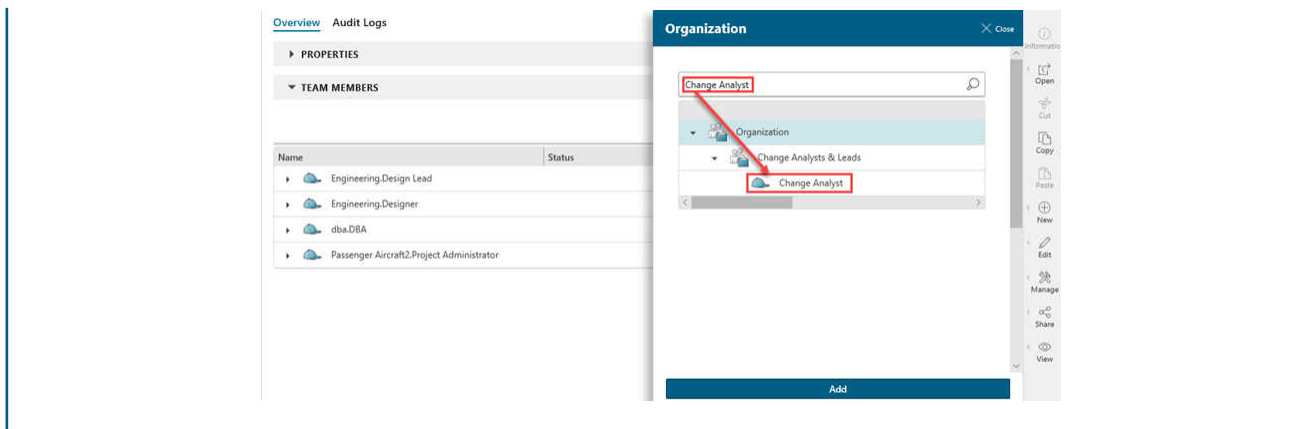
Add a group to a project

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

2.   From **TEAM MEMBERS**, 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 role and click **Add**.
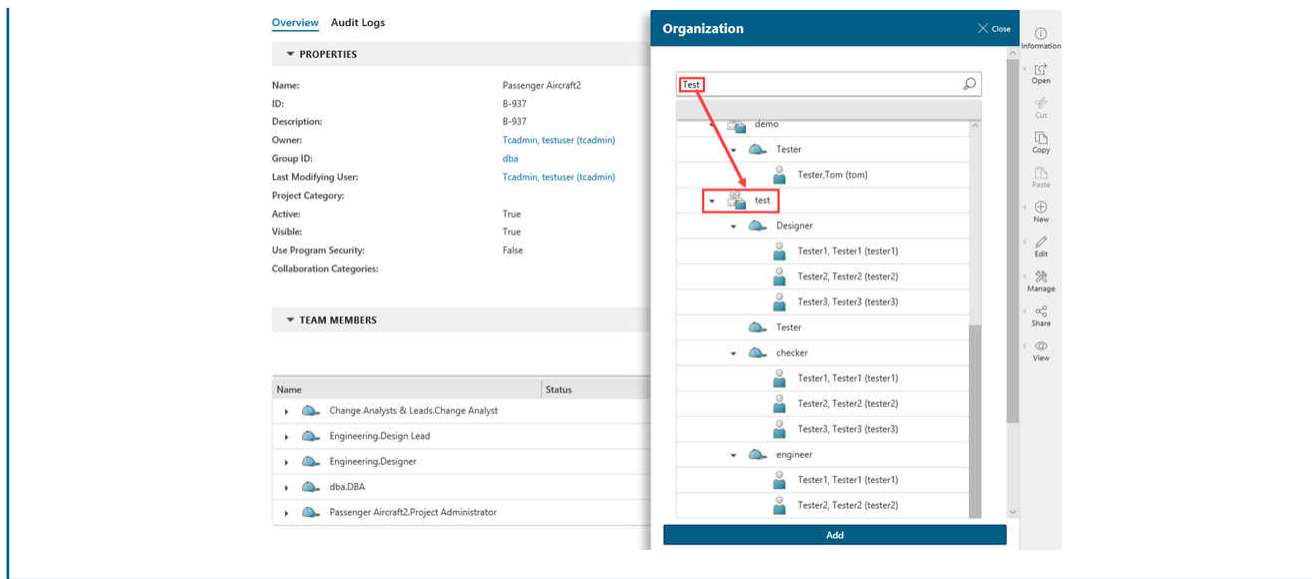
Configuring owning program

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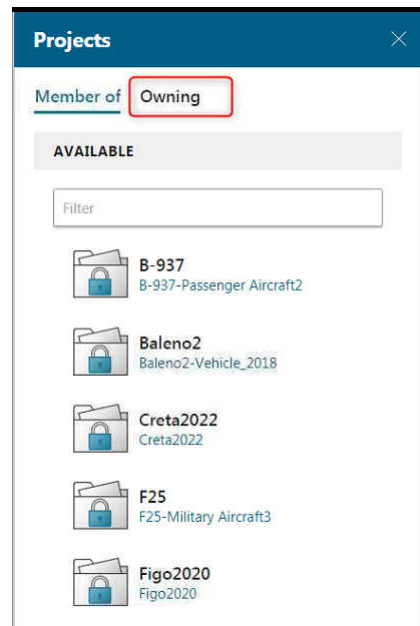
To view the **Owning** program tab, you must set the **AWC_Project_showOwningProgramTab** preference to **true**. Owning program can be set on the object only if the **autoAssignToProject** extension is enabled on the object type.

> 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.
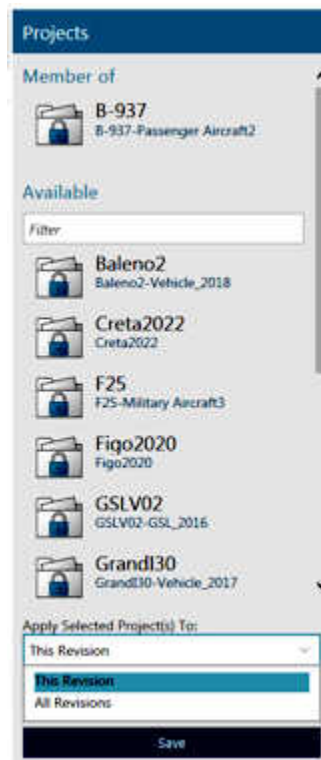
Also, you can hide the project section from the **Add** panel for items. To do this, modify your data model configuration in Teamcenter using the Business Modeler IDE and set the **Fnd0EnableAssignProjects** constant to **False**.
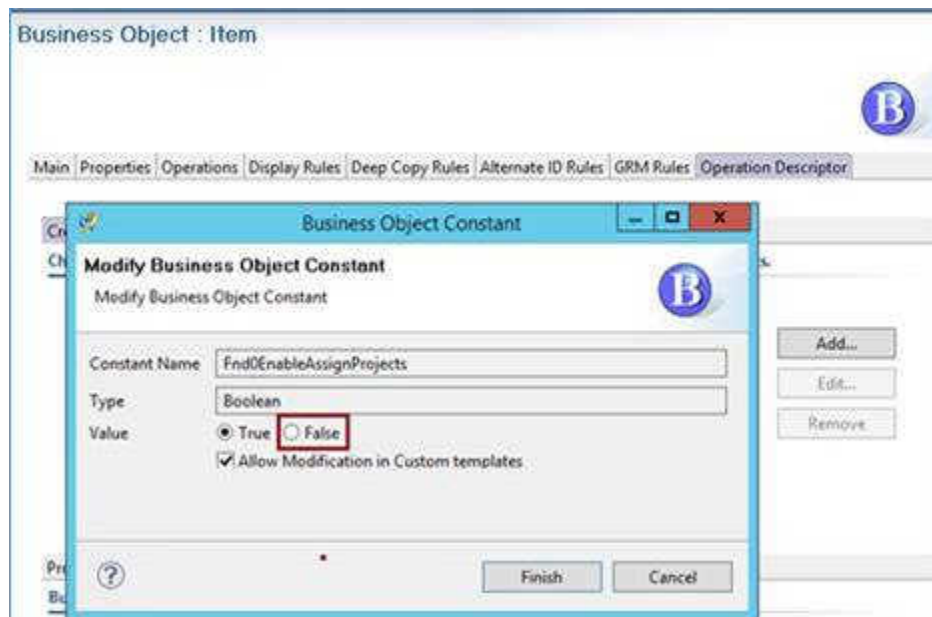
For more information about modifying business object constants, see *Configure your business data model in BMIDE*.

3. Managing data sharing

Configure Briefcase file sharing

Briefcase file exchange settings

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 report layout settings

Briefcase 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 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.

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
```

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**
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 login 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: `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,

Problem	Solution
	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
``` |

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.

Bulk extract and copy tools are not available when you select items from a product structure.

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. (Bulk loading is not available when you select objects from a product structure.)

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.

4. Logging

Monitoring system logging

You can configure two main sources of logging.

Configure the audit logs

These logs record activities performed on selected data model objects. This provides a tracking mechanism for any changes made to those objects for historical record.

Aggregate the gateway logs

This collects and combines the logs from several Active Workspace gateways. If your Active Workspace microservices are distributed, you should 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 following preference to activate the **Audit Log** tab in Active Workspace.

- **AWC_show_audit_logs**
Activates the visibility of the **Audit Log** tab in Active Workspace. By default, the value is **true** for the **dba** group. As a **DBA** user, you can make the **Audit Log** page available to other users using:

  - The rich client **Options** dialog box **Preferences By Organization** pane, which allows a **DBA** user to set the **AWC_show_audit_logs** preference for specific groups, roles, and users.

  For more information, see the *Environment Variables Reference* and 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:

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.

General Logs

ER ID	CHANGE ID	REASON	GROUP NAME	ROLE NAME	SECONDARY OBJECT DISPLAY NAME
dba			dba	DBA	
dba			dba	DBA	

Using audit logs

> 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.

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

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**

Object type	Audit dataset
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.   Insert an **inject** statement for the audit log you want to add.

3.   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 log entries of certain error levels or for entries with a matching stable correlation ID value.

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.

For this property	Do this
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.
	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 version 3.8.0 is included with the microservice framework kit version 5.0.

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
```

> 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
> ```

---

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`

```
        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.

5. 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** ⑦ > **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:
	
	<pre><!-- 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></pre>
	   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. For example, in Internet Explorer, perform the following:
	
	   1. Choose **Tools→Internet Options** and click the **Advanced** tab.
	
	   2. In the **Security** section, clear the selection of **Use TLS 1.0**.
	
	   3. Click **OK**.

Issue	Possible resolution
	4. Restart the browser. The steps for other browsers are similar to those described.
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. 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.

Use PLStats to see performance data

Use the PLStats functionality of Active Workspace to view performance telemetry data.

When you use PLStats, it reports to the browser console information about memory usage, overhead times, DOM node count, and so on.

To use it, modify the URL to insert **?usePLStats** before the **#**.

Example:

`host:port/awc/#/showHome`

Becomes:

`host:port/awc/`**?usePLStats**`#/showHome`

Once you add this to the URL, Active Workspace will maintain it, printing out performance data for each page. To stop using PLStats, remove the **?usePLStats** from the URL.

1. Modify the URL.

2. View the performance summary table.

3. Investigate detailed telemetry information

What else should I know?

In the detailed telemetry section, 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-1.1.0/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.

Windows

On Windows, all of the gateway services and microservices on a given machine are managed by a single multi-threaded 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"
```

Linux

On Linux, the gateway services and microservices are manged by a **Docker** swarm. Force a rolling restart on the gateway node. The others will restart in turn.

Visualization monitoring and troubleshooting

Troubleshoot a new installation of Visualization

Intent

The following Visualization troubleshooting diagnostic sequence is:

- For new installations where visualization is non-functional.

- Tailored for clean systems that have never had a previous installation of visualization.

- Intended for use when the Visualization Pool Assigner is deployed on a Java server on Windows.

Usage notes

- Document all changes made during this process so that all unnecessary changes can be reverted once the system finally works.

- If a problem is identified and fixed during the diagnostic sequence below, but visualization still does not work, return to the beginning of the diagnostic sequence.

Sequence

Use the following steps when troubleshooting a new installation of Visualization.

1. Verify that the servers are installed on computers that are running supported operating systems. For example, Windows 7 Professional is unsupported.

2. Verify that the Visualization Server Manager is launched using the **run_visservermgr.cmd** script. Do NOT run the Visualization Server Manager as a Windows Service, as doing so significantly reduces stability and performance.

3. Verify that the Visualization Pool Assigner is launched using the **run_visassigner.cmd** script. Do NOT run the Visualization Pool Assigner as a Windows Service, as doing so significantly reduces stability and performance.

4. If the Visualization Data Server is installed and running, terminate the Visualization Data Server. It is not required for loading small to medium sized models.

5. Turn off all firewalls. If this is not possible, verify that all ports and port-ranges declared through TEM have been opened through firewalls.

6. Restart the visualization system. The following sequence yields the cleanest startup:

   a. Terminate the Visualization Server Manager.

   b. Terminate the Visualization Pool Assigner.

   c. Start the Visualization Pool Assigner.

   d. Start the Visualization Server Manager.

7. Attempt to view 3D content in Active Workspace. A failure is expected.

8. Does the 3D window waiting cursor (rotating circle) show for a long time and the 3D model does not display?

   - Yes -

     - Logout and login as the **admin** user. Navigate to Viewer Administration and verify that at least one Visualization Pool Assigner and one Visualization Server Manager is listed.
       If no Visualization Pool Assigner and Visualization Server Manager are listed, do the following.

       a. Navigate to the Gateway installation.

       b. Verify that Gateway forwarding is correctly pointing to the deployed Visualization Pool Assigner by verifying that the following entry is correct in the **config.json** file.

       ```
       "vis": {

       "path": "/VisProxyServlet",
       ```

```
    "target": "http://
    <VisAssignerHostname>:<VisAssignerHostPort>>
    /VisProxyServlet"

    }
```

Where **VisAssignerHostname** and **VisAssignerHostPort** are the host and port where the Visualization Pool Assigner was configured.

- No - Continue.

9. Does the message "Vis Server Manager is ready!" appear in the Visualization Server Manager console within two minutes of startup?

- Yes – Continue.

- No –

  - Does a "JVM_Bind" error appear in the Visualization Pool Assigner or Visualization Server Manager console/log?

    - Yes – The server's Socket Cache port is already in use by another process. Either use TEM to alter the port, or terminate the process that is presently using the port. Then, restart the visualization system.

    - No – Continue.

  - Does a "Trouble connecting to cold visualization server on port <PORT> with PID <PID> due to 'The VisView's reported system CPU usage (-1.0) is less than 0'. Retrying ..." error appear in the Visualization Server Manager console?

    - Yes –

      a. Verify that the Visualization Server Manager is installed on a computer that is running a supported operating system.

      b. On the machine hosting the Visualization Server Manager, execute the following Windows commands:
      ```
      cd C:\Windows\SysWOW64
      lodctr /r
      winmgmt /resyncper
      ```

      c. Restart the Visualization Server Manager.

      d. If the problem persists, contact vendor.

    - No – Continue.

- Does a "Error reading 'begin' notification" error appear in the Visualization Server Manager console?

  ▪ Yes – You are likely pointing your Visualization Server Manager at an incorrect server or port. For example, you may be pointing it at the Visualization Pool Assigner's HTTP server instead of the Visualization Pool Assigner's Socket Cache server. If not, contact vendor.

  ▪ No – Continue.

- Verify that the appropriate Microsoft Visual Studio Redistributables are installed. (They are typically installed automatically).

  a.   Launch **VisServerFV\Products\FoundationViewer\visview.exe**.

  b.   Does VisView appear?

     ▪ Yes – Continue.

     ▪ No –

        ◊ Does an error message appear that complains of a missing MFC DLL?

           • Yes – Download and install the appropriate redistributables.

           • No – A different warning or error message is observed. Continue.

- Is the Visualization Server Manager repeatedly reporting an error beginning with "Could not connect to VisPoolAssigner"?

  ▪ Yes –

     ◊ The Visualization Pool Assigner is running a server called the "Socket Cache", but the Visualization Server Manager is reporting that it cannot connect to that server. Verify that the **VisPoolProxy.peerNodes** property in the Visualization Server Manager's **jetty/jettyservice.properties** file will enable the Visualization Server Manager to contact the Visualization Pool Assigner's Socket Cache server.

     ◊ If the problem persists, contact vendor.

  ▪ No – Continue.

- Purge VisView's registry areas.

  a.   Terminate the Visualization Server Manager.

  b.   Run Windows' Registry Editor (*regedit.exe*).

   c.   Using the Registry Editor, delete the following folders in the registry:

```
HKEY_CURRENT_USER/Software/Siemens/AW/<<AW_RELEASE_VERSION>
HKEY_CURRENT_USER/Software/Siemens/AW_Retained/
<<AW_RELEASE_VERSION
```

   d.   Restart the Visualization Server Manager and retest.

   e.   Continue.

- Contact vendor.

10. Does a "The visualization servers are busy" error message appear in Active Workspace when trying to view 3D content?

- Yes –

  - Does a "All Pool Managers are full" error message appear in the Visualization Pool Assigner console?

    - Yes –

      a.   Open the Visualization Server Manager's *jetty/jettyservice.properties* file and note the value of **VisPoolProxy.hostName**.

      b.   From the Visualization Pool Assigner computer, open a command prompt and run the command
      `ping <VisPoolProxy.hostName>`
      where **<VisPoolProxy.hostName>** is the value found in the *jetty/jettyservice.properties* file.

      c.   Was a "Reply" observed?

          ◇ Yes – Continue.

          ◇ No –

            - The Visualization Pool Assigner initiates communications with the Visualization Server Manager using the **VisPoolProxy.hostName** and **VisPoolProxy.poolUrl** values found in the *jetty/jettyservice.properties* file. If the Visualization Pool Assigner cannot reach the Visualization Server Manager using these values, then the system will not work.

      d.   If the problem persists, contact vendor.

    - No – Contact vendor.

- No – Continue.

11. Is a new VisView process started when you attempt to load a model into Active Workspace?

   - Yes –

      - Did the new process terminate a few seconds after starting?

         ▪ Yes – Contact vendor.

         ▪ No – Continue.

   - No –

      - Ensure that the**VisPoolProxy.peerNodes** in the **jetty/jettyservice.properties** file is pointing at the correct Visualization Pool Assigner.

      - If the problem persists, contact vendor.

12. Configure the Visualization Server Manager to be in debug mode.

   a. Make a backup of the **jetty/jettyservice.properties** file.

   b. Open the **jetty/jettyservice.properties** file and change the following parameters:

      - Set "VisPoolProxy.warmServers=1"

      - Set "VisPoolProxy.maxServers=1". (This prevents more than one VisView process from starting.)

      - Enable "VisPoolProxy.envset.TCVIS_DA_DEBUG_LOG=True"

      - Enable "VisPoolProxy.envset.TCVIS_LOGGING_LEVEL=DEBUG"

   c. Shut down the Visualization Server Manager.

   d. Delete the contents of the **jetty/TEMP** directory.

   e. Start the Visualization Server Manager.

   f. You are now in debug mode. Continue.

13. Check for FCC problems.

   a. Configure the Visualization Server Manager to be in debug mode. (Procedure described in previous step.)

   b. Stop the Visualization Server Manager.

c.   Verify that your **FMS_HOME** environment variable specifies the FCC installation area.

d.   Purge FCC temporary files.

    A.   Run the following commands:
```
%FMS_HOME%/startfcc.bat
%FMS_HOME%/bin/fccstat -purge
%FMS_HOME%/bin/fccstat -kill
```

    B.   Delete the following:

- *C:\Users\%USERNAME%\FCCcache**

- *C:\Users\%USERNAME%\Teamcenter\SOA*

- *C:\Users\%USERNAME%\vendor\logs*

- *C:\Users\%USERNAME%\fcc.**

- *VisDataServer/Program/scratch/*.*

    C.   Start FCC manually using the command "**%FMS_HOME%/startfcc.bat**" and verify that there are no errors.

e.   Clear the contents of the Visualization Server Manager's **jetty/TEMP** area.

f.   Restart the visualization system.

g.   Attempt to view 3D content in Active Workspace.

h.   Examine the **jetty/TEMP/VisProd*/tcvis_da_dbglog*.txt** and address any suspicious error messages.

i.   Open the **jetty/TEMP/Visview<PID>.log** file.

j.   Does the log file contain any of these messages:
```
"ERROR: MkGetFileByFMSTicket"
"ERROR: MkCreateMoniker"
"ERROR: OpenDocumentByMoniker"
```

- Yes –

    A.   Open your FCC's **fcc.xml** file and verify that it is pointing at correct locations and that it is it free of typos.

    B.   If your FCC's **fcc.xml** parentfsc is using HTTPS, verify the involved certificates.

        C.   Review the FCC console for errors.

        D.   Review the **jetty/TEMP/VisProd\<PID\>/*/tcvis_da_debug*.txt** for errors.

        E.   If the problem persists, contact vendor.

- No – Continue.

14. Verify that the Visualization Server Manager has access to graphics hardware.

   a. See the section "Configure the Visualization Server Manager to be in debug mode" earlier in this procedure.

   b. Open the **jetty/TEMP/Visview\<PID\>.log** file.

   c. Does the log file contain the message: "System Supports OpenGL Version"?

   - Yes –
     - Is the value of "System Supports OpenGL Version" 1.2 or greater?
       - Yes – Continue
       - No –
         ◇ Are you using supported graphics hardware?
         - Yes –
           A. Verify that your NVIDIA graphics driver is version 340.66 or later
           B. Verify that the computer is recognizing the graphics card.
           C. If the problem persists, contact vendor.
         - No – No solution.
   - No – Contact vendor.

15. Contact vendor.

Troubleshooting Visualization

The following list of issues and possible resolutions addresses situations that are outside the scope of the visualization troubleshooting **diagnostic sequence for new installations**.

1. **Graphics in the viewer tab display extraneous geometry.**
2. **Measurement label dragging does not work with a touch screen.**
3. **The assembly appears to be very small on the screen.**
4. **Indexing fails while using the MMV option.**
5. **Lifecycle Visualization may display a structure differently than it is shown in Active Workspace.**
6. **You encounter an error when using Internet Explorer 11 to run Active Workspace hosted in stand-alone visualization.**
7. **The Visualization Pool Assigner repeatedly adds the error message "Could not connect to <HOST>:<PORT>. Retrying..." to the console/log.**
8. **The Visualization Server Manager displays message "Trouble connecting to cold visualization server on port XXXX with PID YYYYY due to "The VisView's reported system CPU usage (-1.0) is less than 0". Retrying ..." .**
9. **After a user inactivity exceeds the time out value, the Active Workspace viewer tries to reconnect but fails with the following error: "Visualization was not loaded because communication was lost."**
10. **When initializing the Viewer, you see a spinning circle, but the Viewer never loads.**

Issue	Possible resolution
1) Graphics in the viewer tab display extraneous geometry.	This is an indication that the graphics driver on the Visualization Server Manager machine is not up-to-date. **Verification** 1. On your video card manufacturer's web site, make note of the latest driver version for your card. 2. Open the Windows Control Panel. 3. Click **Device Manager**. 4. Expand **Display adapters**. 5. Right-click the entry for your display adapter, and choose **Properties**. 6. Click the **Driver** tab. The driver version on your machine is listed. If the installed driver is not the latest available, update it. **Solution** If the driver for the graphics adapter is not the latest version, update the driver and reboot.

Issue	Possible resolution
2) Measurement label dragging does not work with a touch screen.	**Solution** You can use Internet Explorer to drag measurement labels by pressing and holding the label. In other browsers on the Microsoft Surface, you may need to disable the "press and hold" setting if you see a translucent square appear when performing the press and hold gesture. 1. Open Windows search and type **Pen and Touch** to find the settings dialog box. 2. In the **Touch** tab, select the **Press and Hold** action and click **Settings**. 3. Uncheck **Enable press and hold for right-clicking** and click **OK**. 4. In the **Pen and Touch settings** dialog box, click **OK**.

3) The assembly appears to be very small on the screen.	**Verification**
	
	The existence of bad data from a single part in a large assembly may cause noticeable visualization artifacts when the whole assembly is viewed in MMV mode. For example, if one part has a very large bounding box caused by bad data, the assembly may appear to be very small on the screen.
	
	Review the **vds_console.log** for this line:
	
	`Suspected bad bounding box encountered`
	
	VDS provides this warning if it encounters parts with suspicious bounding boxes. Keep in mind the following items:
	
	• VDS flags nodes with an unusually large bounding box.
	
	• VDS flags nodes that are isolated from other parts.
	
	• You need at least 1000 nodes in a structure for these calculations to be made. (Otherwise it would not be statistically meaningful.)
	
	To log additional information on boundary box error reporting, create a log for bounding box validation by adding the following to the **VisDataServer.properties** file:
	
	`# This channel is meant to capture the output from BBoxValidator logger.`

Issue	Possible resolution

```
# This will log any invalid Bounding Boxes found in the
structure.
logging.channels.BBoxValidatorChannel.class=FileChannel
logging.channels.BBoxValidatorChannel.flush=false
logging.channels.BBoxValidatorChannel.path=$
{system.tempDir}/BBoxValidator.log
logging.channels.BBoxValidatorChannel.rotateOnOpen=true
logging.channels.BBoxValidatorChannel.purgeAge=0 seconds
logging.channels.BBoxValidatorChannel.formatter=FileFormatt
er

# BBoxValidator logger
logging.loggers.BBoxValidator.name=BBoxValidator
logging.loggers.BBoxValidator.level=Debug
logging.loggers.BBoxValidator.channel=BBoxValidatorChannel
```

Use the bounding box validator to define the appropriate bounding box for your assemblies.

4) Indexing fails while using the MMV option.

Verification

When running the FTS Indexer with the Massive Model Visualization (MMV) option, a folder is automatically generated in case there is a failure:

FTS_INDEXER_HOME**working\TcFtsIndexer_structure\ MMV_Failure**

Solution

If you notice the **MMV_Failure** folder is created and contains content, contact Support Center to investigate the issues.

5) Lifecycle Visualization may display a structure differently than it is shown in Active Workspace.

This may occur when Active Workspace configures its structures using a saved variant rule (SVR) and then interoperates the configured structure to Lifecycle Visualization.

Solution

The **PSEShowUnconfigdVarPref** preference must be set to **false** for Lifecycle Visualization to show the same structure as Active Workspace when variants are applied. This can be done using the **Edit→Options** menu command in the rich client.

The issue can occur depending on the value of the **PSEShowUnconfigdVarPref** preference. The Structure Manager application within the rich client allows for setting a **Show Unconfigured Variants** flag. When this flag is **true**, BOM lines that would normally be removed given the current variant configuration are shown. The value of the **PSEShowUnconfigdVarPref** preference is modified each time the state of this flag is modified. Active Workspace does not currently present this **Show Unconfigured Variants** flag as a configurable option. However, the **PSEShowUnconfigdVarPref**

Issue	Possible resolution
	preference is still used by the BOM window to set its own state regarding whether it shows unconfigured BOM lines.

Setting the **PSEShowUnconfigdVarPref** preference to **false** causes BOM lines for configurations (other than the current one) to be removed, displaying (in Lifecycle Visualization) the same configuration data that is displayed in Active Workspace.

6) You encounter an error when using Internet Explorer 11 to run Active Workspace hosted in stand-alone visualization.

Verification

You see the following error:

```
You are using an unsupported browser.
In order to use Teamcenter Active Workspace, you must use
a browser that
supports HTML5.
If you are running Internet Explorer 11 (or later) and
seeing this message,
you may be running in compatibility mode.
You must turn it off to have the HTML5 support that is
required.
```

Solution

1. Clear the cache in Internet Explorer by choosing **Tools→Delete Browsing History** on the menu bar.

2. Choose **Tools→Compatibility View Settings** and check **Display intranet sites in Compatibility View**.

3. In the registry, add the following browser emulation settings for the executables **visview.exe** and **visview_ng.exe**:

```
HKEY_CURRENT_USER
        SOFTWARE
            Microsoft
                Internet Explorer
                    Main
                        FeatureControl
                            FEATURE_BROWSER_EMULATION
```
visview.exe = (DWORD) 00011000
visview_ng.exe = (DWORD) 00011000

For detailed information about browser emulation and registry settings, see:

https://msdn.microsoft.com/en-us/library/ ee330730(v=vs.85).aspx

Issue	Possible resolution
	4. Reboot your machine.
7) The Visualization Pool Assigner repeatedly adds the error message "Could not connect to <HOST>:<PORT>. Retrying..." to the console/log.	The Visualization Pool Assigner was likely mistakenly configured to have a peer Visualization Pool Assigner. Peer Visualization Pool Assigners are intended for load balanced configurations where there is more than one Visualization Pool Assigner in the system for improved load handling and/or failover. Open the Visualization Pool Assigner configuration page in TEM and remove the Visualization Pool Assigner's peer assigner entry.
8) The Visualization Server Manager displays the message "Trouble connecting to cold visualization server on port XXXX with PID YYYYY due to "The VisView's reported system CPU usage (-1.0) is less than 0". Retrying ..."	The Visualization Server Manager process uses Windows performance counters to read the current CPU usage of the computer. Windows performance counters can become broken, resulting in invalid values for the CPU usage, for example: -1. **Solution** 1. Open a command prompt or PowerShell as an administrator. 2. Change the directory to *C:\Windows\SysWOW64*. 3. Run the command **lodctr /R**. 4. Restart the Visualization Server Manager.
9) After a user exceeds the time out value, the Active Workspace viewer tries to reconnect but fails with the following error: " Visualization was not loaded because communication was lost."	The Visualization deployment was likely mistakenly configured with the Teamcenter Load Balancer URL. Refer to Configure Visualization where Teamcenter is deployed behind a load balancer. In the developer tools console the following error will display if the deployment was configured with the Load Balancer URL: error "Failed to connect to server: The TCLoginverifier likely refused this visualization-specifc request due a missing connection to Teamcenter."
10) The Viewer doesn't load during initialization and you see a spinning circle.	There is a startup preference for Active Workspace that contains the list of all preferences that are loaded at startup. It must contain the full list of preferences required by the viewer. If some of the preferences are missing from this preference or from the database, the viewer may not load properly. You will see a spinning circle over the graphics area, but the viewer will not load. It is especially important to check this if Active Workspace preferences were installed or upgraded without using the install scripts provided by Active Workspace or were modified after the install.

Issue	Possible resolution
	• All of the viewer preferences must be in the database with valid values.
	• Check the value of the preferences: **AWC_startupPreferences**. It should contain the list of required viewer preferences.
	The full preference list and their default values can be found at:
	{ROOT}\src\solutions\awv0activeworkspacevis\businessdata \awv0activeworkspacevis\install\awv0_preference_skip.xml
	The full list is below.

AWC_visNavigationMode	AWC_visStdViewOrientationFront
AWC_vis3DNavigationMode	AWC_applyTrueShadingMaterial
AWC_visShading	AWC_visOverlayDisplayEffectivity
AWC_visMaterial	AWC_visSelectionDisplay
AWC_visTrihedronOn	AWV0SectionCapsEdgesInitialState
AWC_visFloorOn	AWV0HostAWInVisUponLaunch
AWC_visFloorPlaneOrientation	AWV02DViewerRenderOption
AWC_visFloorOffset	AWV0ViewerRenderOption
AWC_visGridOn	AWC_visExamineZoomIn
AWC_visShadowOn	AWC_visExposedBetaFeatures
AWC_visReflectionOn	AWC_visAllOn
AWC_visStdViewOrientationTop	AWC_3DViewerDisplayUnit
AWC_visStdViewOrientationLeft	

Monitor visualization components in Active Workspace

The Active Workspace **Viewer Administration** page provides information about active visualization components including the server pool assigner, server manager, processes, and connected clients.

1. Log on as a user with administrator privileges.

2. On the home page, click **VIEWER ADMINISTRATION**.

Tip:

To see the **VIEWER ADMINISTRATION** tile on the home page, make sure your organization group and role is mapped to the right workspace.

The **Viewer Administration** page appears. The initial view of the page includes a diagram of the server pool assigner, server manager, and the active processes and connected clients.

3. For details about an object included in the diagram, select the object, and click **Information** ⓘ.

The **Information** panel appears, providing detailed information on the selected visualization component.

> Note:
>
> To maintain a secure environment, sensitive information such as IP addresses and the session ID is not displayed.

4. To update the display of information, click **Refresh**.

Troubleshooting an MMV deployment

This troubleshooting topic assumes that you have already deployed the Active Workspace 3D viewer, Visualization Data Server (VDS), and indexed the structure with the MMV flag. If you do not have a working Active Workspace 3D viewer, review the other topics within **Visualization monitoring and troubleshooting**. If you have a working viewer but your structure is not loading with MMV, then use this checklist to troubleshoot your MMV deployment issues.

Use the following procedures to troubleshoot an Active Workspace MMV deployment.

Troubleshooting step	Comments
Ensure the **Active Workspace Visualization Server Extension** feature is installed.	This feature adds the **awv0activeworkspacevis_template.xml** template to the database.
Ensure that these licenses are installed.	• Vis_simp_rendering • Visualization Professional or Mockup service level
Ensure that **FCC** (File Client Cache) is installed and configured correctly.	The FCC should be large enough to load all the JT data that is needed for the indexed products.
Use the **VisView** process log files to determine if the viewer is using the **GPU**.	1. Enable logging through the **jettyservice.properties file**. 2. Uncomment this line: `#VisPoolProxy.envset.TCVIS_LOGGING_LEVEL=DEBUG` 3. Restart the **Visualization Server Manager**. 4. Log into any log file for any **VisView** process. The log output directory (defaults to TEMP) should look like the example below. The numbers will be different but the pattern Visview*.log will remain the same.

Troubleshooting step	Comments
	5. Search for **OpenGL** to find a block of text that looks like the example below. If the version of **OpenGL** is greater than 1.1.0 (110), then you are using the **GPU**.
Verify that the configuration that is indexed is the same as what you are trying to view (e.g., same revision, rule, effectivity, etc.).	For more information on using the FTSIndexer, review runTcFTSIndexer. Use the following command to get the FTSIndexer status. 1. In the Teamcenter **command prompt**, enter the following command: `runTcFTSIndexer –task=structure:show` 2. Confirm that the **State** field value = **8** (success) and the **Subscribers** field value = **MMV**. Another way to verify that the indexing is successful is to: 1. Log in as the Teamcenter administrative user. 2. Locate the **MMV Delta Collection - DO NOT DELETE** folder. 3. Inside the folder, locate the dataset with the **Awv0CompleteFile** named reference, indicating successful indexing.

Troubleshooting step	Comments
	If the structure is not MMV-indexed, review the bomindex_admin to make sure it is configured correctly.
If the indexing did not succeed, generate indexing logs for MMV.	1. Set the **TcFtsIndexer** logging to **TRACE**: `log4j.logger.com.siemens.teamcenter.ftsi=TRACE` 2. Modify the existing **%TcFtsIndexer.home%\conf\TcFtsIndexer.properties** parameter: This keeps generated mmp and tcxml files. 3. Cleanup the working directory and previously generated logs. 4. Restart the **TcFtsIndexer** service.
Review the **VDS** console to verify that there are no obvious error messages.	1. Start up the **VisDataServer.exe** process. 2. Look for ***FULL STRUCTURE IMPORT COMPLETE** output for the **BIAD**s (BOMIndexAdminData tables) that are MMV-indexed. You will not be able to view MMV until the import is complete. 3. Review the console for any obvious error messages.
Correct an **InvalidCredentialsException** error on **VDS** startup.	**VDS** independently logs into Teamcenter using a password file created by TEM. If this password is wrong or lost, you will see an InvalidCredentialsException error in the console on VDS startup. You can do the following to recreate the file.

Troubleshooting step	Comments

	1. From the command line, enter:
	`set TEM_SEENA=<password>`
	`VisDataServer.exe /encryptpwf /`
	`pwenv=TEM_SEENA /pwfile=d:\test.pwf`
	`set TEM_SEENA=`
	2. In the **VisDataServer.properties** file, ensure that these values are correctly set:
	
	• User name under which **VDS** accesses Teamcenter data for the population of indexed models in its memory and cache.
	`TeamcenterAccessManager.User1=`*Tc-admin-user*
	• Path to encrypted password file.
	`TeamcenterAccessManager.LoginFilePath1=C:/`
	`myfolder/test.pwf`

Verify that the URL is configured correctly and that the viewer can access the **VDS**.	1. In the **jetty.properties** file for the viewer (not the **VDS**), locate the line similar to the following example:
	`VisPoolProxy.envset.TCVIS_VISDATASERVERURL=h`
	`ttp://<hostname>`
	`:9990/ProductStructure`
	2. Copy and paste the URL into a browser window on the machine where the viewer is running.
	The **VDS** console should respond with an error message if the URL is configured correctly and the viewer is accessing the VDS.
	If the VDS console does not respond, it means either that this line in the jetty.properties file is misconfigured or that something in the network is preventing the viewer from contacting the VDS.

View the **VDS** logs if the viewer isn't behaving as expected.	If the viewer isn't behaving as expected, do the following to view the client communication logs to **VDS**. You should see FindRoot call to confirm that the viewer is attempting to load a structure with the **VDS**.
	
	1. Shut down **VDS**.
	2. In the **VDS.properties** file, uncomment the following lines to see the HTTP request from the client.
	`#logging.loggers.ProductStructure.name=Produ`
	`ctStructure`
	`#logging.loggers.ProductStructure.level=Debu`
	`g`
	`#logging.loggers.ProductStructure.channel=Co`
	`nsoleChannel1`
	This will show client communication from the viewer to **VDS**.

Troubleshooting step	Comments

> Note:
>
> This will generate a lot of logs, so we don't recommend doing this until you have reached this step in the troubleshooting process.

3. Locate the FindRoot call to confirm that the viewer is attempting to load a structure with the **VDS**.
4. If there is no communication between the viewer and **VDS** when a structure is loaded, turn on the SOADebug library from the viewer:

   - In the **jetty.properties** file, add the following line:
     ```
     VisPoolProxy.envset.TC_SOACLIENT_LOGGING=DEBUG
     ```
     The soa_client log will be created in the TEMP directory.

   - In the soa_client log, look for a GetStructureIDFromRecipe call being made to Teamcenter from the viewer.

Monitoring Visualization server components using JMX

Overview of monitoring Visualization Server components using JMX

You can monitor the Active Workspace Visualization Server system, including the Visualization Server Manager, Visualization Servers, and the Visualization Pool Assigner, using a freeware Java Management Extensions (JMX) client, such as Oracle Java Mission Control or JConsole. Monitoring these server components with JMX is useful for identifying performance bottlenecks or other problems.

A JMX client installed on the same computer as the Visualization Server components automatically detects all servers running on the machine. The information exposed by the visualization components is presented using MXBeans.

To enable remote access for JMX clients, on the server you must configure authentication (users and passwords) and encryption for the server process. Once remote access is enabled and configured, JMX clients from remote machines can connect to the server.

For information about configuring remote JMX monitoring of server processes, see *Monitoring and Management Using JMX Technology* in the Oracle Java SE Documentation.

> Note:
>
> JMX metrics can include the following composite data types with multiple values:

CurrentMaxTotal: This object includes these values:

- The current value

- The highest the value has been since startup

- The total value since startup

▲ ■ #clientCount	CompositeData, size 3
■ #current	26.0
■ #max	30.0
■ #total	66.0

CurrentMaxMin : This object includes these values:

- The current value

- The highest the value has been since startup

- The smallest the value has been since startup

▲ ■ #computerCpuUsageRatio	CompositeData, size 3
■ #current	0.0014545454
■ #max	0.122
■ #min	0.0

Visualization Server Manager

Each Visualization Server Manager hosts two MXBeans that contain information about its current state: **<poolName>** and **<poolName> monitoring**. They are located in the **Administer-<poolName>-manager** folder.

The **<poolName>** MXBean for the Visualization Server Manager provides the following information:

- **CacheConfiguration**
  The configuration parameters used to connect the Visualization Server Manager to the Visualization Pool Assigner.

- **Language**
  The language within which the Visualization Server Manager is running.

- **Load**
  A single ratio that represents how much of the computer's capacity is currently in use. When this ratio is greater than or equal to 1.0, the system is completely full and new clients are rejected.

- **NumberOfAssignedServers**
  The number of Visualization Server processes in use or recently in use by client users.

- **NumberOfColdServers**
  The number of Visualization Server processes in the process of starting up, although not yet ready for use.

- **NumberOfServers**
  The total number of Visualization Server processes (cold, warm, and assigned).

- **NumberOfWarmServers**
  The number of Visualization Server processes ready for use by new client users.

- **PoolID**
  The name of this Visualization Server Manager.

- **PoolSpecificConfiguration**
  The configuration parameters passed in at startup to this Visualization Server Manager.

- **StartupDate**
  The data and time that this Visualization Server Manager was last started.

The **<poolName> monitoring** MXBean for the Visualization Server Manager provides the following information:

- **accepting**
  Whether or not this server is currently accepting new incoming users.

- **assignedServerCount**
  The number of VisView processes that are currently serving users with visualization functionality.

- **assignedVisViews**
  Specific information about each of the VisView processes that are currently assigned to users.

- **assignedVisViewsCount**
  The number of VisView processes that are currently assigned to users.

- **computerCpuUsageRatio**
  A ratio indicating how much CPU usage is consumed or unavailable on this computer.

  > Note:
  >
  > A *ratio* for Active Workspace MXBeans refers to a current usage value divided by the maximum usage value. For example, a CPU usage of 30% is divided by the maximum of 100% to compute a ratio of 0.3. All ratios in Active Workspace are between 0 and 1, unless the capacity of the visualization system is exceeded, in which case the ratio is greater than 1.

- **computerMemUsageRatio**
  A ratio indicating how much system memory is consumed or unavailable on this computer.

- **computerNetworkUsageRatio**
  A ratio indicating how much network usage is consumed or unavailable on this computer.

- **config**
  The configuration parameters passed in at startup to this server.

- **dateCreated**
  The date and time that this Visualization Pool Assigner was last started.

- **gpus**
  Specific information about each of the GPUs currently used by VisView processes.

- **hostName**
  The name or IP address of the computer that this server is hosted on.

- **languageID**
  The language that the server is currently running in. The default is English.

- **loadRatioAbsolute**
  A ratio indicating how much of the computer's resources is consumed or unavailable on this computer.

- **loadRatioRelative**
  A ratio indicating how much of the computer's resources is consumed or unavailable on this computer when compared to the maximum allowed resource-consumption-level (default of 0.7) of this server.

- **maxBandwidthBytesPerSec**
  The maximum allowed bandwidth (in bytes-per-second) that this server is allowed to consume.

- **numAssignmentsSinceStartup**
  The number of models that have used visualization system resources on this server.

- **numGpus**
  The number of GPUs that the computer has.

- **poolName**
  The alias defined by the administrator to identify this particular Visualization Server Manager.

- **Prefers**
  The models preferred by this server.

- **serverTooFullExceptions**
  When clients are refused visualization services, this contains the reason.

- **serverTooFullExceptionsCount**
  How many clients were refused visualization services.

- **serves**
  The models that this server has currently in memory due to requests from users.

- **totalGpuMemMB**
  The total amount of system GPU memory on this computer.

- **upTimeSec**
  How many seconds have elapsed since this server was last started.

- **visSysCpuUsageRatio**
  A ratio indicating the CPU usage of this server on the computer.

- **visSysGpuUsageRatio**
  A ratio indicating the GPU usage of this server on the computer.

- **visSysMemUsageRatio**
  A ratio indicating the amount of system memory consumption of this server on the computer.

- **visSysNetworkUsageRatio**
  A ratio indicating the amount of network usage of this server on the computer.

- **warmServerCount**
  The number of VisView processes that do not yet have users but are ready to host visualization services for new users.

- **warmVisViews**
  Specific information about the VisView processes that do not yet have users but are ready to host visualization services for new users.

- **warmVisViewsCount**
  The number of VisView processes that do not yet have users but are ready to host visualization services for new users.

Visualization Server

Each Visualization Server owned by the Visualization Server Manager hosts one MXBean that contains information about its current state. The MXBeans for the Visualization Servers are called **VisView@PID_<processID>@Port_<port>**. They are located in a folder called **VisServers**.

An MXBean for a Visualization Server provides the following information:

- **ClientConnections**
  Information about each client user connected to this Visualization Server.

- **DateCreated**
  The date and time that this Visualization Server entered a state where it was first made available to client users (warm).

- **Models**
  The IDs for the models that this Visualization Server is currently hosting.

- **MsSinceLastEMM**
  The number of milliseconds since this Visualization Server last received a message from a client.

- **Port**
  The port that this Visualization Server is currently hosting its socket server on for connections from the Visualization Pool Assigner.

- **ProcessCpuUsageRatio**
  The average amount of CPU usage that this Visualization Server has consumed on the Visualization Server Manager computer over the last 20 seconds.

- **ProcessGpu**
  General information about the GPU that the Visualization Server is using.

- **ProcessID**
  Also known as the PID, this is the identifier that the operating system uses to denote this particular Visualization Server.

- **ProcessMemUsageRatio**
  The average amount of memory usage that this Visualization Server has consumed on the Visualization Server Manager computer over the last 20 seconds.

- **ProcessMyGpuMemUsageRatio**
  The average amount of GPU memory usage that this Visualization Server has consumed (of the particular GPU that this Visualization Server is assigned to) over the last 20 seconds.

- **ProcessNetworkUsageRatio**
  The average amount of network usage that this Visualization Server has consumed on the Visualization Server Manager computer over the last 20 seconds.

- **ProcessTotalBytesTransfered**
  The number of bytes that have been received and sent by this Visualization Server process (discounts data downloaded from Teamcenter servers).

- **ServletConnections**
  Information about each connection from the Visualization Pool Assigner.

- **TotalNumEMMs**
  The number of client requests handled by this Visualization Server.

- **UpTimeSec**
  The number of seconds that have elapsed since this Visualization Server was created.

Visualization pool assigner

Each Visualization Pool Assigner hosts two MXBeans that contain information about its current state: **Assigner** and **Assigner monitoring**. The MXBeans are located in the **Administer Assigner manager** folder.

> Note:
>
> You must configure the Visualization Pool Assigner to populate some of the JMX metrics with meaningful information. For more information, see Configure the Visualization Pool Assigner for JMX metrics.

The **Assigner** MXBean for the Visualization Pool Assigner provides the following information:

- **AssignerSpecificConfiguration**
  The configuration parameters passed in at startup to this Visualization Pool Assigner.

- **CacheConfiguration**
  The configuration parameters used to connect this Visualization Pool Assigner to any other Visualization Pool Assigners in the Visualization Server system, and the configuration parameters used to identify this Visualization Pool Assigner such that other nodes in the Visualization Server system can connect to it.

- **Load**
  A single ratio that represents how much of the computer's capacity is currently in use. When this ratio is greater than or equal to 1.0, the system is completely full and new clients are rejected.

- **NumberOfPools**
  The number of Visualization Server Managers that this Visualization Pool Assigner is currently connected to.

- **NumberOfUsers**
  The number of client users who are currently connected to Visualization Server processes through this Visualization Pool Assigner.

- **StartupDate**
  The data and time that this Visualization Pool Assigner was last started.

The **Assigner monitoring** MXBean for the Visualization Pool Assigner provides the following information:

- **clientCount**
  The number of users that are connected to this server.

- **clients**
  Specific information about the clients that have active sessions with this server.

- **computerCpuUsageRatio**
  A ratio indicating how much CPU usage is consumed or unavailable on this computer.

- **computerMaxBandwidthBytesPerSec**
  The maximum allowed bandwidth (in bytes-per-second) that this server is allowed to consume.

- **computerMemUsageRatio**
  A ratio indicating how much system memory is consumed or unavailable on this computer.

- **computerNetworkUsageRatio**
  A ratio indicating how much network usage is consumed or unavailable on this computer.

- **computerTotalMemMB**
  The total amount of system memory on this computer.

- **config**
  The configuration parameters passed in at startup to this server.

- **dateCreated**
  The date and time that this Visualization Pool Assigner was last started.

- **loadRatioAbsolute**
  A ratio indicating how much of the computer's resources is consumed/unavailable on this computer.

- **loadRatioRelative**
  A ratio indicating how much of the computer's resources is consumed or unavailable on this computer when compared to the maximum allowed resource-consumption-level (default of 0.7) of this server.

- **poolCount**
  The number of Visualization Server Managers known to this server.

- **poolManagers**
  Specific information about the Visualization Server Managers known to this server.

- **serverTooFullExceptions**
  When clients are refused visualization services, this contains the reason.

- **serverTooFullExceptionsCount**
  How many clients were refused visualization services.

- **upTimeSec**
  How many seconds have elapsed since this server was last started.

- **visSysCpuUsageRatio**

A ratio indicating the CPU usage of this server on the computer.

- **visSysMemUsageRatio**
A ratio indicating the amount of system memory consumption of this server on the computer.

- **visSysNetworkUsageRatio**
A ratio indicating the amount of network usage of this server on the computer.

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 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 supercede 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 supercede 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 supercede 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.

Alice
Engineering / Manager

DocumentRevision

Summary view

DocumentRevision.SUMMARYRENDERING

Manager role: "DocRevSumMgr

Site: "DefaultDocRevSum"

Manager's custom view

DocRevSumMgr

DefautDocRevSum

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 supercede 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 supercedes 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	*.dot*	*.mdb*	*.sxc*	*.xls*
.aw	*.dotm*	*.mif*	*.txt*	*.xlsm*
.csv	*.dotx*	*.msg*	*.various*	*.xlt*
.dat	*.eml*	*.ods*	*.vdx*	*.xltm*
.dc	*.epub*	*.pdf*	*.wo*	*.xltx*
.dif	*.fff*	*.ppt*	*.wpd*	*.xlw*
.doc	*.htm*	*.pptx*	*.xml*	*.xlsx*
.docm	*.html*	*.rtf*	*.xla*	
.docx	*.ip*	*.stc*	*.xlam*	

- **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. **Awp0TestItemRevMasterS** 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.

Business Object : Awp0TestItemRevision

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 in a non-retail industry solution in previous versions of Active Workspace, you can perform a one-time migration using this utility to migrate your existing questions and comments data to the new Active Collaboration discussions feature.

Migrates previous Active Collaboration questions and comments data (**S2clSocial** objects) to the new Active Collaboration discussions feature that uses **Ac0ActiveCollaboration** objects.

> **Caution:**
>
> Perform this migration only once to prevent a 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

To 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
```

awindexerutil

Refreshes indexed objects if you make changes to them and you want the synchronization flow to refresh the index for those objects. The **awindexerutil** utility marks those objects to be picked up during the next synchronization flow batch. This allows you to update the index without the downtime of a full index flow.

You can refresh your index for only the delta of changes since the last completed synchronization. You can index changes for types and properties that have been added, modified, or removed, by performing a delta update when you remerge Solr and Teamcenter schemas and update the index.

Running **awindexerutil** does not interfere with current synchronization flows.

Run the utility from the *TC_ROOT\bin* directory (*TC_BIN* if it's set).

SYNTAX

awindexerutil -u=user-id -p=password -g=group [**-refresh**] [**-delta** [**-dryrun**] [**-daterange**]] **-h**

ARGUMENTS

-u

Specifies the user ID. The user needs 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 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.

-g

Specifies the group associated with the user.

-refresh

Starts the synchronization flow according to the batch size.

-delta

Updates the index for the delta of changes to object types and properties since the last completed synchronization. Be sure to run **-delta -dryrun** to evaluate the changes before running the **-delta** index update.

Use this approach to remerge Solr and Teamcenter schemas and to update the index.

-dryrun

Use with **-delta** to compare the changes in object types and properties for delta reindexing. No indexing is performed. The differences are output to the command window and a log file. The *.log* file path is returned after the operation is complete.

-daterange

Use with **-delta** or **-delta -dryrun** to set a date range for object types and properties that can be indexed in the updated schema. To set the date range, use the following year-month-day form:

YYYY/mm/dd HH:MM:SS-YYYY/mm/dd HH:MM:SS

The time (**HH:MM:SS**) is optional. You can specify multiple ranges in a comma-separated list. If the specified date range contains spaces, enclose the entire specification in quotation marks.

-classification

Used together with the **-delta** argument, evaluates the schema files and marks the changes in classification data for indexing in the next scheduled indexing synchronization run. Run the utility with the **-classification -delta -dryrun** arguments to receive a list of changes that will be marked for indexing when the **awindexerutil** is run.

-h

Displays help for this utility.

EXAMPLES

- Start the synchronization flow to refresh data objects:

```
awindexerutil -u=admin -p=pwd -g=group -refresh
```

- Start the dry run comparison of the delta of indexing changes. All instances of new, modified, and deleted types and properties are identified. For newly indexed types, only those instances that were changed during the specified date range (2012/12/12 - 2016/12/31) are included. Only a report is returned. No indexing changes are made.

```
awindexerutil -u=admin -p=pwd -g=group -delta -dryrun
    -daterange=2012/12/12-2016/12/31
```

- Start reindexing the delta of changes. Updates all new, modified, and deleted types and properties.

```
awindexerutil -u=admin -p=pwd -g=group -delta
```

- Start reindexing the delta of changes. Updates all new, modified, and deleted types and properties. For types that are newly added, only those objects last modified in the specified date range are indexed.

```
awindexerutil -u=admin -p=pwd -g=group -delta -daterange=
    "2015/12/12 15:30:00 - 2015/12/31 22:00:00, 2016/02/01 07:00:00
    - 2016/12/31 14:00:00"
```

• Mark changes in classification data for indexing:

```
awindexerutil -u=admin -p=pwd -g=group -delta -classification
```

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**

BIAD	Product	Revision Rule	Structure Type	MMV Owning User	MMV Access Users
					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 | | | | | |

csv2tcxml.perl utility

> Note:
>
> The *TC_DATA\csv2tcxml_perl\csv2tcxml.perl* utility described here is deprecated and support will be removed in a future release.
>
> The replacement utility is *TC_DATA\csv2tcxml\csv2tcxml.perl* (named the same, but stored in a different directory). This replacement utility is recommended for new data migrations. Refer to the *CSV2TCXML Converter Guide* in the *TC_DATA\csv2tcxml* directory for instructions on its use.
>
> See *Choosing a CSV to TC XML converter version* in Teamcenter help.

Converts a file formatted similar to a CSV file into a TC XML file that can be imported into a Teamcenter site. You use this utility to migrate data from a legacy system into Teamcenter using the bulk load function of the **tcxml_import** utility. For more information, see Teamcenter help.

The *csv2tcxml_config.txt* file contains default values for many of the arguments. You can override any of the variable values in this file temporarily by adding them into the command line arguments when you type the command. Use the format *argument-name=argument-value*.

Syntax

perl csv2tcxml.perl [**split**] {*file-name* | **reports** *input-directory*}
[*split-file-integer*]

Arguments

split

Indicates that the input file is processed as a set of subfiles. The converter processes the number of lines indicated by the *split-file-integer* argument as a subfile. The next set of lines are then processed until it has processed all lines in the indicated file. This allows more efficient use of memory for very large files and can prevent memory limit errors.

file-name

Defines the name of the TC XML output file that you use to import the legacy data into the target Teamcenter site. This argument is required unless you are generating reports.

reports

Generates the HTML report from the log files in the indicated directory. This report shows summary information, breakup of the objects created, performance of the conversion with time taken for

each step, and the number of errors and warnings the converter generated. It also includes a link to the log file.

input-directory

Indicates the directory containing the log files used to generate the HTML report.

split-file-integer

Indicates the number of lines to process as a subfile when you specify the **split** argument. If you do not specify a split value, the converter uses 100,000 as the default value.

Examples

- To read the input CSV file and generate a puid-based TC XML file for items:

```
perl csv2tcxml.perl items.csv
```

- To read the input CSV file and generate a puid-based TC XML file for datasets that does not contain item or revision information in the file:

```
perl csv2tcxml.perl dataset.csv item=exist
```

- To read the input CSV file and generate a puid-based TC XML file for datasets that does not contain BOM or GRM information in the file:

```
perl csv2tcxml.perl bom.csv item=exist
```

- The following is an example of the converter's progress indicator output:

```
D:\tcxml> perl D:\scripts\csv2tcxml.perl D:\scripts\samples\items.csv source_site=10000
   -> 0 of 5 : Processing
      [D:\scripts\samples\items.csv] in [puid] with item-exists=[0] ...
   -> 1 of 5 : Generating GSids
            !
   -> 2 of 5 : Converting GSids to Puids
   -> 3 of 5 : Converting CSV to TCXML
            !
   -> 4 of 5 : Creating tcxml file
   -> 5 of 5 : Printing & Validating tcxml stats
            NOTE: *** 3 errors 0 warnings 0 duplicates logged in
      [D:\scripts\samples\items.csv.log] ***
   -> Total time = 0 seconds
```

- To import a custom form that is attached to an item revision, in *csv2tcxml_mapping.txt* add the following line file to the `#CREATE_OBJECT_COLUMNS` section and replace `CostDataForm` with the custom form type name.

```
CustomFormName|CostDataForm:object_name<-IMAN_reference<-ItemRevision
```

In the *.csv* file, add the following column name and provide a value in each row to create the custom form.

```
!Item:item_id|ItemRevision:item_revision_id|CustomFormName
100223|A|cost-frm-1
100778|A|cost-frm-2
```

- To process multiple imports for an assembly, include the occurrence ID (**occ_id**) property. A unique **occ-id** column must be provided if the BOM data is updated multiple times as shown in the following example:

```
!parent_item|parent_rev|child_item|child_rev|occ_id
car|A|wheel|A|front-left
car|A|wheel|A|front-right
car|A|wheel|A|rear-left
car|A|wheel|A|rear-right
```

Errors and warnings

The converter generates the following error messages:

- `Required input (source_site) missing in config file and command line.`
- `Column count in Header is different than columns in a row.`
- `Item id value length is less than 1.`
- `Custom Item type used in csv file is missing in csv2tcxml_datamodel.txt file.`
- `Island 0 (admin) objects are not on top of xml file.`
- `Class/type in item, itemrevision, form, psbomview objects is not valid.`
- `Dataset type, tool/format and volume/sdpath definition is missing.`
- `Puid value of BO is invalid in itemrevision, form, dataset, bvr, psocc, relation and generic BO.`
- `Unsupported secondary object during generic BO creation with GRM.`
- `Primary object missing during generic BO creation thru attribute reference.`
- `Duplicate Puid generated.`
- `Business object/attribute name(s) used in column name is missing in Teamcenter schema.`
- `Item helper classes/types defined in csv2tcxml_datamodel.txt is missing in Teamcenter schema.`
- `Dataset/ImanRelation types used in csv file is missing in Teamcenter schema.`
- `Category defined in mapping is unknown or unsupported.`

The converter generates the following warning messages:

- `Unsupported command line parameters.`
- `Certain column in csv file is not mapped in mapping file.`
- `Required attribute is empty.`

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.

runTcFTSIndexer

Indexes data into the Solr indexing engine. Run this command from the *FTS_INDEXER_HOME* directory, for example, *TC_ROOT***\TcFTSIndexer\bin**.

SYNTAX

runTcFTSIndexer -debug -maxconnections -status -stop -service -shutdown -task=[objdata | multisite | structure | fourgd]:*flow-action* **-h**

Operating system considerations:

Linux	A *.sh* extension is required, for example, **./runTcFTSIndexer.sh**.
	If a UID contains a special character, you must enclose it in straight, single quotation marks. UIDs can contain **A-Z**, **a-z**, **0-9**, **$**, and **_**.
Windows	The *.bat* extension is not required for **runTcFTSIndexer**.
	For UIDs on Windows, do not enclose in straight, single quotation marks.

ARGUMENTS

-debug

Reports a summary of the flow in progress, including connections and the logs associated with them, to the command window and to the TcFtsIndexer logs in **TcFTSIndexer\logs**. Run **-debug** in a separate command window.

```
runTcFTSIndexer -debug
```

-maxconnections

Sets a new value for maximum **tcserver** connections to use at any given time, for example:

```
runTcFTSIndexer -maxconnections=5
```

-status

Checks the status of the indexer and reports the flows running in the indexer. For example, the following shows the status for all the flows:

```
runTcFTSIndexer  -status
```

This argument can also be used with the **-task** argument. For example, the following command shows the status of the **objdata:index** flow:

```
runTcFTSIndexer -status -task=objdata:index
```

-stop

Stops indexing flows that use an interval.

```
runTcFTSIndexer -stop
```

This argument can also be used with the **-task** argument. For example, the following command stops the **objdata:sync** flow with intervals:

```
runTcFTSIndexer -stop -task=objdata:sync
```

-service

Starts the indexer as a Java Remote Method Invocation (RMI) service in a console, for example:

```
runTcFTSIndexer -service
```

This argument can also be used with the **-task** argument to run a flow when starting the service, for example:

```
runTcFTSIndexer -service -task=objdata:index
```

-shutdown

Shuts down the service after stopping all the flows.

```
runTcFTSIndexer -shutdown
```

-task

Runs an indexing task in this format:

```
-task=type:flow-action
```

Flow actions are specific to the type of task.

objdata	Indexing actions to support object data indexing
admin	Administrative actions to support clone and merge indexing
fourgd	Indexing actions to support 4GD
multisite	Indexing actions to support multi-site published records
structure	Indexing actions to support structured content indexing

-h

Displays the help for this utility.

OBJDATA FLOW ACTIONS

- **objdata:clear**
  Clears existing indexed data, records, and cached files. This option is most often used prior to running **objdata:index**. When you run **-task=objdata:clear**, specify one of these options when you are prompted:

    1 clears the indexer cache.

    2 clears the Solr index.

    3 clears the object data indexing records from the Accountability table.

    4 clears the data covered by options 1, 2, and 3.

    5 clears the UIDs passed in from the Accountability table.
    When you specify **5**, provide the full path to the text file containing the UIDs.

    6 cancels the clear flow.

    7 cleans up the scratch table records, where the last saved date precedes the last processed date of the subscription table.

  If you run **-task=objdata:clear** in an environment that is set to **Clone Ready**, it fails in order to prevent accidentally clearing the index.

  > Example:
  >
  > To clear a list of UIDs, run the command:
  >
  > ```
  > runTcFTSIndexer -task=objdata:clear
  > ```
  >
  > At the prompt:
  >
  > ```
  > Please provide a clear option from above list [1-7]:
  > ```
  >
  > Enter **5**. The prompt returns:
  >
  > ```
  > Provide full path to input uid text file.
  > ```
  >
  > Enter the full path and file name:
  >
  > ```
  > c:\my_uid_directory\uids.txt
  > ```

- **objdata:errors**

Returns the errors for indexing failures to a specified directory. The directory must be empty. You can optionally specify the number of errors to be returned. The default is 50 errors.
The error directory contains a directory for each UID of the failed object. Each UID directory contains the following information:

- Properties such as object name and type provide information on the failed objects.

- The TC XML and Solr XML files are generated and saved for debugging.

- Syslog information.

- TcFtsIndexer log files with the errors.

In this example, the first 100 errors are sent to the specified output directory:

```
runTcFTSIndexer -task=objdata:errors d:\TcFTSIndexer\errors 100
```

- **objdata:index**
  Performs indexing for the time period specified in *TC_ROOT\TcFTSIndexer\conf\TcFtsIndexer_objdata.properties* without clearing the existing index.
  For a clean start, first use **objdata:clear** to clear indexed data and cached files. However, if you run it in a **Clone Ready** environment, it fails in order to prevent accidentally clearing the index.

- **objdata: index clone**
  Indexes the specified time period without clearing the existing index. The start time is set to when the **Clone Ready** state was set. The end time is set in the *conf\objdata.properties* file.
  This indexing flow supports the clone and merge indexing approach, which is a method to manage upgrades and patches more efficiently by reindexing a cloned environment and then merging it to an updated production environment.
  The **objdata: index clone** task picks up the delta of indexing changes in the production environment that occurred while the cloned environment was being indexed. This flow depends on the administrative flow actions.

- **objdata:indexsyncfailures**
  Indexes synchronization failures that required manual intervention.

- **objdata:recover**
  Recovers failed indexed objects.
  If failures are reported during initial indexing, run the recover flow action after initial indexing completes. Recover failures from the initial index by running **objdata:recover** repeatedly until there are no failures reported or the failures are consistent and need to be fixed.
  You can choose to fix the errors or leave them for later and proceed with the synchronization flow. If you leave them, these errors are logged as failures during synchronization. You can return at a later time to fix them. The recover flow action operates by time slice. The recover flow action processes all failed objects together.

- **objdata:show**

Returns objects that are in a specified indexing state in two text files. Specify the state code and a directory for the output files using the form **-task=objdata:show** *n uid_file_dir*.
The **show** number to specify the state is **1**, **2**, or **3**:

> **1** returns objects in the replication pending state

> **2** returns objects in the indexing complete state

> **3** returns objects in the indexing failed state

In this example, the output files contain the objects that failed indexing:

```
runTcFTSIndexer -task=objdata:show 3 d:\TcFTSIndexer\uid_output
```

The output returns two text files:

- *uid.txt*
  Contains the UIDs of the objects that match the specified state. Each UID is on one line.
  You can synchronize the objects again using **objdata:sync** *uid_file_dir*. Specify the directory containing the *uid.txt* file, for example:

  ```
  runTcFTSIndexer.bat -task=objdata:sync d:\TcFTSIndexer\uid_output
  ```

- *uid_prop.txt*
  Contains UIDs in the output format *UID | object_string | object_type*, for example:

  ```
  TRa3S5qdSDyB | Breaker Panel Anchor Plate/AP02-A | Physical Part Revision
  ```

- **objdata:sync**
  Updates the index with changes to data between the previous run and the current run.

  - The **sync** action can take the **-interval=**seconds argument.
    For example, to synchronize object data using the stand-alone indexer every 300 seconds (5 minutes):

    ```
    runTcFTSIndexer -task=objdata:sync -interval=300
    ```

    The value must be greater than **0**.
    To run **sync** once, omit **-interval=**seconds.

  - The **sync** action can take a *file path* to a *uid.txt* file.
    You can synchronize the objects again using **objdata:sync** *filepath*. Specify the directory containing the *uid.txt* file, for example:

    ```
    runTcFTSIndexer.bat -task=objdata:sync d:\TcFTSIndexer\uid_output
    ```

- **objdata:test**

Verifies whether the environment is set up correctly prior to running the indexer.

ADMINISTRATIVE FLOW ACTIONS

- **admin:cloneready**
Sets the production environment to **Clone Ready** in preparation for creating a cloned environment.
After this action is applied, the cloned environment can be upgraded or patched and then indexed using **objdata:index**.

- **admin:clonevalidate**
Confirms that the indexing information in the upgraded production environment and the upgraded cloned environment are the same.
Run this flow action to determine whether the production environment is ready for the indexing system to be merged.
After the merge, pick up the delta of indexing changes in the upgraded production environment using **objdata:index clone**.

- **admin:clonecomplete**
Removes the **Clone Ready** setting on the indexing system in the upgraded production environment.
The environment must have been previously set to **Clone Ready**.

- **admin:status**
Provides the means to verify the current clone status of the production environment.

MULTI-SITE FLOW ACTIONS

- **multisite:clear**
Clear indexed data and cached files for existing multi-site published records.
Use prior to running **multisite:index**.

- **multisite:index**
Without clearing the existing indexed multi-site published records, index for the time period specified in the *TC_ROOT\TcFTSIndexer\conf\TcFtsIndexer_multisite.properties* file. For example:

```
runTcFTSIndexer –task:multisite:index
```

During indexing, duplicate published records are removed.
For a clean start, use **multisite:clear** to clear indexed data for multi-site published records and cached files.

- **multisite:indexuids**
Index the UIDs for a specific Object Directory Services (ODS) site.
Specify the ODS site name and the directory containing the *uid.txt* file, for example:

```
runTcFTSIndexer –task=multisite:indexuids ODS_Site_name D:\UID_dir
```

- **multisite:indexsyncfailures**

Index synchronization failures that required manual intervention.

- **multisite:sync**
  Updates the index with changes to published record data between the previous run and the current run.
  The **sync** action can take the **-interval=**_seconds_ argument to repeat the **sync** action at the specified interval. For example, to synchronize multi-site published record data every 300 seconds (5 minutes):

  ```
  runTcFTSIndexer -task=multisite:sync -interval=300
  ```

  The value must be greater than **0**.
  To run **multisite:sync** once, omit **-interval=**_seconds_.

- **multisite:recover**
  Recovers failed indexed published record objects.
  If some published records fail during indexing, run the recover flow action after multi-site indexing completes. Recover failures by running **multisite:recover** repeatedly until there are no failures reported or the failures are consistent and need to be fixed.

- **multisite:test**
  Verify whether the environment is set up correctly prior to running the multi-site indexer.

STRUCTURE FLOW ACTIONS

- **structure:recoverfailures**
  Changes all product configurations with failed states to the **ReadyToIndex** state or the **MarkedForDeletion** state. For example:

  ```
  runTcFTSIndexer -task=structure:recoverfailures
  ```

- **structure:reset** _product-configuration-UID_
  Resets the given product configuration UID setting to the **ReadyToIndex** state or the **MarkedForDeletion** state. For example:

  ```
  runTcFTSIndexer -task=structure:reset 'goZRkWxoqd$DyB'
  ```

- **structure:resetall**
  Downloads the latest transform and schema files, resets all active product configurations to the **ReadyToIndex** state, and resets all deleted product configurations back to the **MarkedForDeletion** state. For example:

  ```
  runTcFTSIndexer -task=structure:resetall
  ```

- **structure:show**
  Shows a summary of all configured product configurations, for example:

  ```
  runTcFTSIndexer -task=structure:show
  ```

- **structure:sync**
  Queues synchronization and delete actions for all product configurations, for example:

  ```
  runTcFTSIndexer -task=structure:sync
  ```

- **structure:syncone** *product-configuration-UID*
  Queues synchronization and delete actions for a single product configuration UID, for example:

  ```
  runTcFTSIndexer -task=structure:syncone goZRkWxoqd12DyB
  ```

- **structure:test**
  Verifies that the environment is set up correctly prior to running the indexer, for example:

  ```
  runTcFTSIndexer -task=structure:test
  ```

4GD FLOW ACTIONS

The 4GD product structure is initially indexed using the **bomindex_admin** utility.

- **fourgd:reset** *product-configuration-UID*
  Resets the given 4GD product configuration UID setting to the **ReadyToIndex** state. For example:

  ```
  runTcFTSIndexer -task=fourgd:reset goZRkWxoqd$DyB
  ```

- **fourgd:resetall**
  Downloads the latest transform and schema files, resets all active 4GD product configurations to the **ReadyToIndex** state. For example:

  ```
  runTcFTSIndexer -task=fourgd:resetall
  ```

- **fourgd:show**
  Shows a summary of all 4GD configured product configurations, for example:

  ```
  runTcFTSIndexer -task=fourgd:show
  ```

- **fourgd:sync**
  Queues synchronization and delete actions for all 4GD product configurations, for example:

  ```
  runTcFTSIndexer -task=fourgd:sync
  ```

- **fourgd:syncone** *product-configuration-UID*
  Queues synchronization and delete actions for a single 4GD product configuration UID, for example:

  ```
  runTcFTSIndexer -task=fourgd:syncone goZRkWxoqd12DyB
  ```

Siemens Digital Industries Software

Headquarters

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

Americas

Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

Europe

Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

Asia-Pacific

Suites 4301-4302, 43/F
AIA Kowloon Tower, Landmark East
100 How Ming Street
Kwun Tong, Kowloon
Hong Kong
+852 2230 3308

About Siemens Digital Industries Software

Siemens Digital Industries Software is a leading global provider of product life cycle management (PLM) software and services with 7 million licensed seats and 71,000 customers worldwide. Headquartered in Plano, Texas, Siemens Digital Industries Software works collaboratively with companies to deliver open solutions that help them turn more ideas into successful products. For more information on Siemens Digital Industries Software products and services, visit www.siemens.com/plm.

This software and related documentation are proprietary and confidential to Siemens.