TEAMCENTER

Supplier Connect — Deployment and Administration

Teamcenter 2412

SIEMENS

About Siemens Digital Industries Software

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

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

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

Contents

Configuration tasks to be performed by suppliers to work with Briefcases

1. About Supplier Connect in Teamcenter

Effective communication and frequent interaction between the OEMs and suppliers are critical. For product design, the Supplier Connect solution from Teamcenter enables and automates this interaction in a secure and traceable way. Specifically, development teams working on large products in various industries, such as the automotive, electronics, or machinery industry, can collaborate with suppliers, using data exchange packages.

Consider a scenario where a design engineer wants to share data with a supplier and receive updated data from the suppliers based on the requirements. You, as an administrator, can install and configure the Supplier Connect solution in the OEM Sponsor Site for the design engineer and in the OEM Supplier Site for the supplier.

Where do I go from here?

 Sponsor	See *Supplier Connect for Data Exchange*.
 Supplier	See *Supplier Connect for Suppliers*.
 Administrator	
In my existing Teamcenter environment, how do I add Supplier Connect?	**Install Supplier Connect using Deployment Center.**
If I have an earlier version of Supplier Connect, how do I get the latest version?	**Update Supplier Connect.**
After I install or update Supplier Connect, what should I do?	Configure Supplier Connect for the **OEM (OEM Sponsor Site)** and the **suppliers (OEM Supplier Site)**.
After my installation and configuration is done, what must be set up?	**Set up the vendors and their suppliers** who will use Supplier Connect.
If I have an existing Supplier Collaboration Foundation environment, what must be done?	**Migrate Supplier Collaboration Foundation users and data to Supplier Connect.**

2. Planning the Supplier Connect deployment

To use Supplier Connect to exchange data between OEMs and suppliers, you require two Teamcenter sites, one for the OEM (OEM Sponsor Site) and one for the suppliers (OEM Supplier Site). This improves data security by preventing suppliers from accessing the data in the OEM's Teamcenter database. Additionally, when a design engineer shares design data with a supplier, the suppliers work only on the shared data.

For a successful deployment, ensure that you keep the following ready:

- Hardware for two Teamcenter sites.

  For versions of system software and hardware certified for running Teamcenter on your platform, see the Hardware and Software Certifications knowledge base article on **Support Center**.

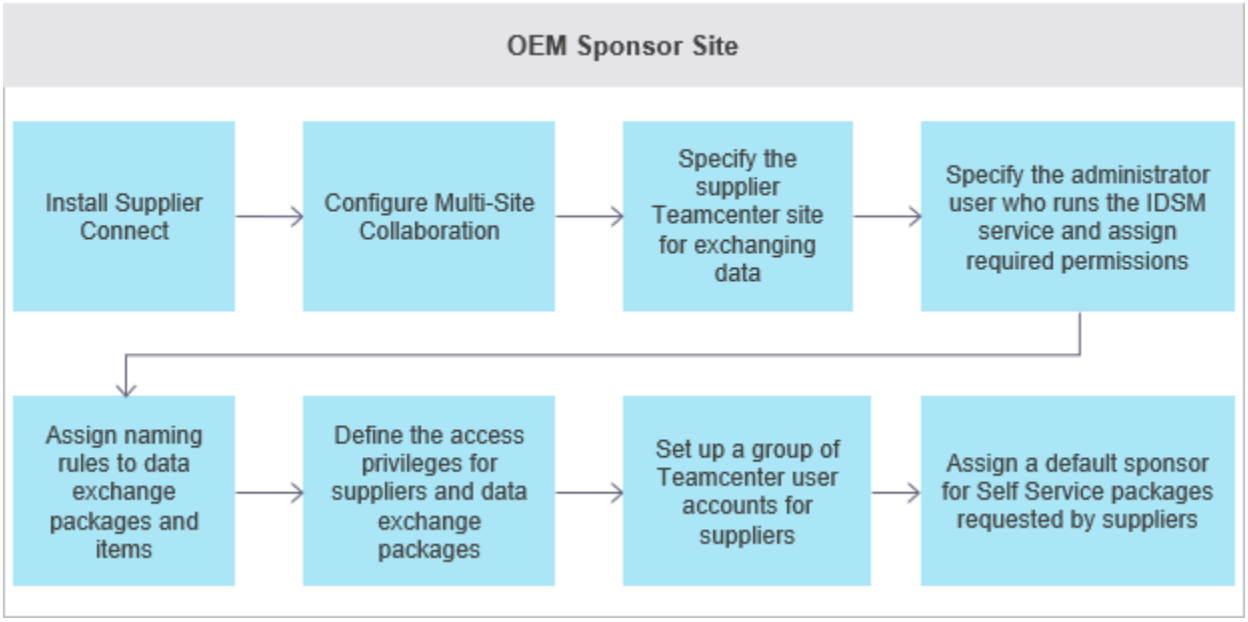
- Teamcenter is set up on the OEM Sponsor Site and OEM Supplier Site.

- Multi-Site Collaboration is configured and verified between the OEM Sponsor Site and the OEM Supplier Site. Supplier Connect uses Multi-Site Collaboration to exchange data between the OEM Sponsor Site and OEM Supplier Site.

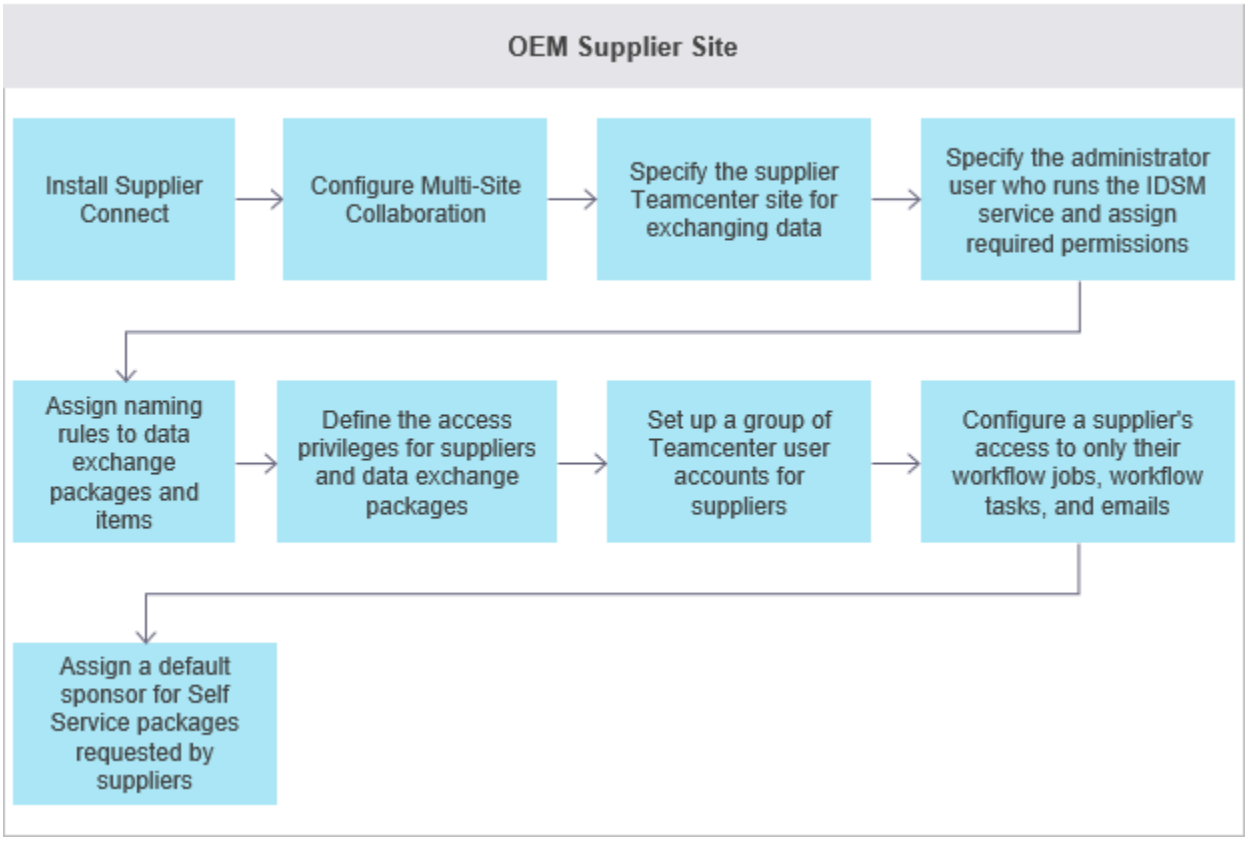
3. Task flow to deploy Supplier Connect

Deploy Supplier Connect on the OEM Sponsor Site and the OEM Supplier Site through a series of tasks.

The following graphic shows the sequence of tasks required to deploy Supplier Connect on the OEM Sponsor Site.



The following graphic shows the sequence of tasks required to deploy Supplier Connect on the OEM Supplier Site.



4. Install Supplier Connect using Deployment Center

Add the Supplier Connect application to your existing Teamcenter environment through a series of tasks from selecting the application and entering configuration parameters to generating and running deployment scripts.

> Note:
>
> You must install Supplier Connect on the OEM Sponsor Site and the OEM Supplier Site. You can install Supplier Connect only from Deployment Center.

> Caution:
>
> If you are already using Supplier Collaboration, and you install Supplier Connect on the same environment, you cannot revert to using Supplier Collaboration. Ensure that you install Supplier Connect only when you decide to stop using Supplier Collaboration.

Prerequisites

- Microservice framework is installed. For more information about the microservice framework, see *Microservices and the microservice framework* in *Teamcenter Installation Using Deployment Center* in the Teamcenter documentation.
- You must be familiar with using Deployment Center. For details, see *Deployment Center — Usage* in the Deployment Center documentation.

Procedure

1. Log on to Deployment Center and select the environment to which you want to add Supplier Connect.
2. Go to the **Applications** tab. Click **Add or Remove Selected Applications** .
3. In the **Available Applications** panel, use the web browser search to find the following applications, select the applications, and then click **Update Selected Applications**.

   - **Supplier Connect for Sponsor** when you are installing Supplier Connect on the OEM Sponsor Site

     OR

     Supplier Connect for Supplier when you are installing Supplier Connect on the OEM Supplier Site

- **Briefcase Browser**

  > Note:
  >
  > Supplier Connect works with only the latest version of **Briefcase Browser**. You must install the latest version for Supplier Connect.

Deployment Center automatically selects any additional dependent applications.

4. In the **Selected Components** list of the **Components** tab, configure the following components:

   - Components required for **Multi-Site Collaboration**

   - **Dispatcher Module**: Configure the **Async Service Translator** and **Supplier Connect Orchestration Translator** translators.

   Note any remaining components whose configuration status is not **100%**. Select each incomplete component, enter the required parameters, and save the component settings until all components in the environment show a configuration status of **100%**. When all the components are configured, the **Deploy** tab is enabled.

5. In the **Deploy** tab, to generate deployment scripts, click **Generate Install Scripts**.

   When script generation is complete, note any special instructions in the **Deploy Instructions** panel.

6. Locate the deployment scripts, copy each script to its target machine, and then run each script on the target machine.

   For more information about running deployment scripts, see *Run the deployment scripts* in the Deployment Center documentation.

   If you face any issues during the deployment, see *Troubleshoot the deployment script* in the Deployment Center documentation.

7. To use Supplier Connect in a single sign-on (SSO) deployment, you must install and configure SSO for both the OEM Sponsor Site and the OEM Supplier Site.

   For more information about configuring Teamcenter products in an SSO deployment, see *Security Services Configuration* in the Teamcenter documentation.

5. Update Supplier Connect

To use the latest version of Supplier Connect, update Supplier Connect in your existing Teamcenter environments for the OEM Sponsor Site and the OEM Supplier Site.

Prerequisites

- Supplier Connect must be installed on the OEM Sponsor Site and the OEM Supplier Site.
- You must be familiar with using Deployment Center. For details, see *Deployment Center — Usage* in the Deployment Center documentation.

Procedure

1. Log on to Deployment Center and select the environment where you want to update Supplier Connect.
2. Go to the **Applications** tab. Click **Add or Remove Selected Applications** .
3. In the **Available Applications** panel, use the web browser search to find the following applications, select the applications, and then click **Update Selected Applications**.

   - **Supplier Connect for Sponsor** when you are installing Supplier Connect on the OEM Sponsor Site

     OR

     Supplier Connect for Supplier when you are installing Supplier Connect on the OEM Supplier Site

   - **Briefcase Browser**

     > Note:
     >
     > Supplier Connect works with only the latest version of **Briefcase Browser**. You must install the latest version for Supplier Connect.

   Deployment Center automatically selects any additional dependent applications.
4. In the **Selected Components** list of the **Components** tab, configure the following components:

   - Components required for **Multi-Site Collaboration**
   - **Dispatcher Module**: Configure the **Async Service Translator** and **Supplier Connect Orchestration Translator** translators.

Note any remaining components whose configuration status is not **100%**. Select each incomplete component, enter the required parameters, and save the component settings until all components in the environment show a configuration status of **100%**. When all the components are configured, the **Deploy** tab is enabled.

5. In the **Deploy** tab, to generate deployment scripts, click **Generate Install Scripts**.

   When script generation is complete, note any special instructions in the **Deploy Instructions** panel.

6. Locate the deployment scripts, copy each script to its target machine, and then run each script on the target machine.

   For more information about running deployment scripts, see *Run the deployment scripts* in the Deployment Center documentation.

   If you face any issues during the deployment, see *Troubleshoot the deployment script* in the Deployment Center documentation.

6. Configure Supplier Connect on the OEM Sponsor Site

After installing Supplier Connect, you must configure the OEM Sponsor Site to connect with the OEM Supplier Site. When you complete the required configurations, the sponsors and suppliers can exchange data successfully.

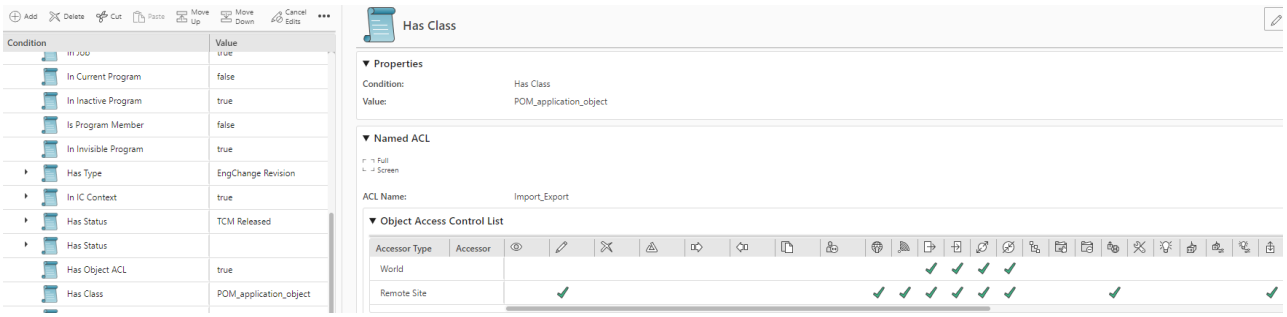
Prerequisites

- Supplier Connect must be installed at the OEM Sponsor Site and the OEM Supplier Site.
- Configure Multi-Site Collaboration between the OEM Sponsor Site and the OEM Supplier Site as specified in the Teamcenter documentation, specifically in:
  - *Prepare the Multi-Site Collaboration environment* in *Teamcenter Installation Using Deployment Center* in the Teamcenter documentation.
  - *Multi-Site Collaboration deployment options* in *Multi-Site Collaboration* in the Teamcenter documentation.
  - *Determining the setup process* in *Multi-Site Collaboration* in the Teamcenter documentation.
  - *Configure Multi-Site Collaboration sites* in *Multi-Site Collaboration* in the Teamcenter documentation.
- Verify that Multi-Site Collaboration is configured correctly on the OEM Sponsor Site and the OEM Supplier Site. Ensure that you have done the following:
  - In the OEM Sponsor Site and the OEM Supplier Site, configure the following preferences with the **Site Name** of the OEM Sponsor Site and the OEM Supplier Site:

Preference	Value
IDSM_permitted_sites	*<OEM Sponsor Site name>*, *<OEM Supplier Site name>*
IDSM_permitted_checkout_sites	*<OEM Sponsor Site name>*, *<OEM Supplier Site name>*
IDSM_permitted_transfer_sites	*<OEM Sponsor Site name>*, *<OEM Supplier Site name>*

  - Run the **dsa_util** utility to ensure that the OEM Sponsor Site and the OEM Supplier Site are connected. For more information, see *Multi-Site Collaboration* in the Teamcenter documentation.
  - Select the **Has Class (POM Object)** node from the Access Manager rule tree, and create the **Import/Export** access control list (ACL) with the following details:

Condition	Value	Accessor Type	Privileges
Has Class	**POM Application Object**	**World**	Grant these privileges: ■ **Export** ■ **Import** ■ **Transfer Out** ■ **Transfer In**
		Remote Site	Grant these privileges: ■ **Write** ■ **Publish** ■ **Subscribe** ■ **Export** ■ **Import** ■ **Transfer Out** ■ **Transfer In** ■ **Remote Check-Out** ■ **Check-In/Check-Out**



Procedure

1. To specify the OEM Supplier Site for exchanging data, set the **SUPPORTAL_share_site_names** preference to the Teamcenter site name specified for the OEM Supplier Site.

2. To send notification emails through the data exchange process, set up an email server with the following details:

   - Set the **Mail_server_name** preference to a valid SMTP mail server.
   - Set the **Mail_OSMail_activated** preference to **true** to enable operating system emails from Teamcenter.
   - Set the port used by the mail server to **25**.

   > Note:
   >
   > To disable notification emails from Supplier Connect, set the **SUPPORTAL_Enable_Mail_Notifications** preference to **False**.

3. If you have configured Multi-Site Collaboration to use remote procedure call (RPC) technology to communicate between the sites, do the following:

   a. For the Integrated Distributed Services Manager (IDSM) service in the OEM Sponsor Site and the OEM Supplier Site, ensure that you change the service's **Log on as** user from **infodba** to another user with database administrator privileges as follows:

      A. Edit the *TC_BIN***run_tc_idsm.bat** script file.

      B. Set the value of **TC_USER** from **infodba** to another user with database administrator privileges.

      C. Set the value of **TC_USER_PASSWD_FILE** from the password file of the **infodba** user to another user with database administrator privileges.

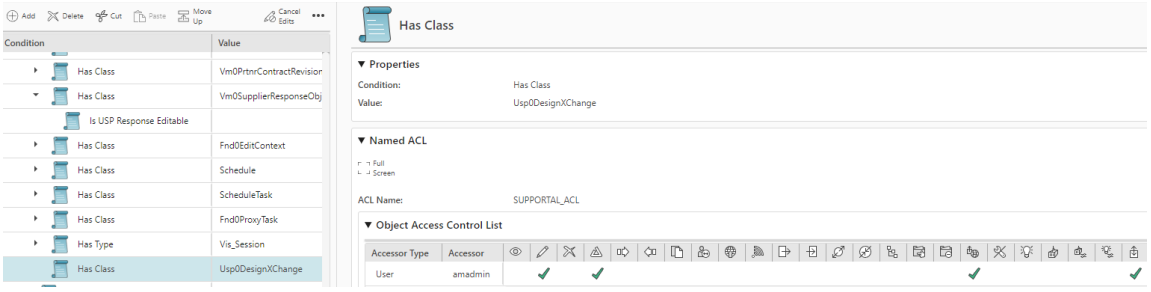
      D. Save the **run_tc_idsm.bat** file.

   b. For the IDSM service user with database administrator privileges, grant permissions to write, change, remotely check out an object, and override the checkout of an object by another user.

      A. In Teamcenter Access Manager, select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** node from the Access Manager (AM) rule tree, and create the **SUPPORTAL_ACL** ACL with the following details:

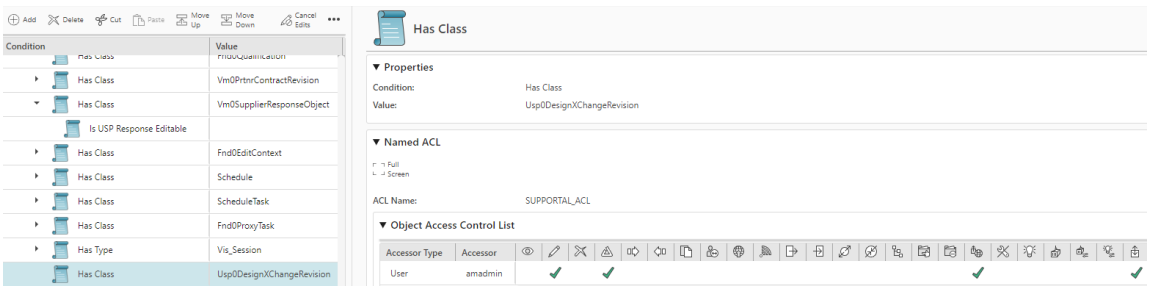
Condition	Value	Accessor Type	Accessor	Privileges
Has Class	**Usp0DesignXChange**	**User**	Administrator user specified as the IDSM administrator in the *run_tc_idsm.bat* script file	Grant these privileges: • **Write**

Condition	Value	Accessor Type	Accessor	Privileges
				• **Change** • **Remote Check-Out** • **Check-In/ Check-Out**



B. Select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** node from the AM rule tree, and create the **SUPPORTAL_ACL** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privileges
Has Class	**Usp0DesignXChangeRevision**	**User**	Administrator user specified as the IDSM administrator in the *run_tc_idsm.bat* script file	Grant these privileges: • **Write** • **Change** • **Remote Check-Out** • **Check-In/ Check-Out**



c. Restart the Pool Manager and the IDSM services on the OEM Sponsor Site and the OEM Supplier Site.

For more information about configuring Multi-Site Collaboration to use RPC, see *Methods for communicating through a firewall* in *Multi-Site Collaboration* in the Teamcenter documentation.

4. If you have configured Multi-Site Collaboration to use the HTTP/HTTPS protocol to communicate between the sites, do the following:

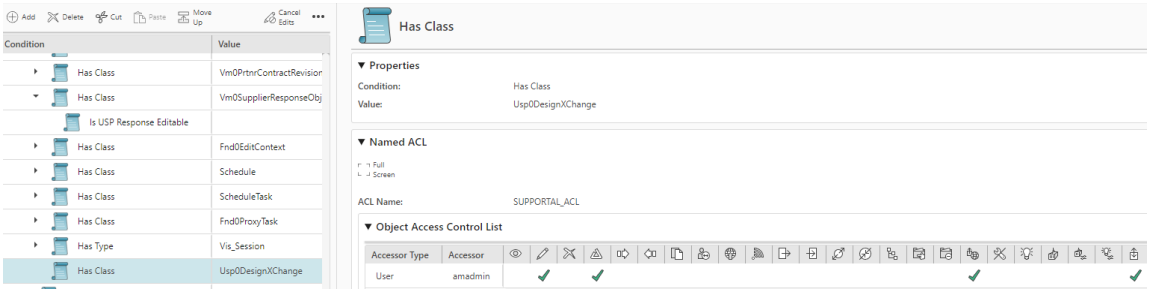
a. Define the **ASYNC_ALLOW_FALLBACK** environment variable, and set its value to **TRUE**.

```
ASYNC_ALLOW_FALLBACK=TRUE
```

b. For the administrator user configured as the remote proxy user, grant permissions to write, change, remotely check out an object, and override the checkout of an object by another user.

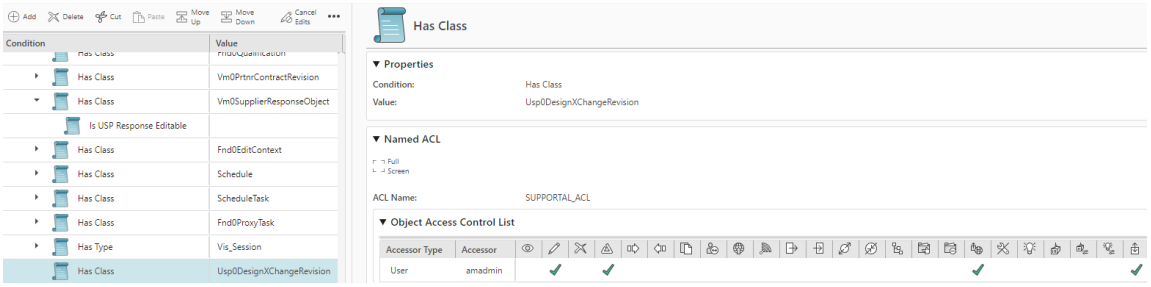
A. In Teamcenter Access Manager, select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** node from the Access Manager (AM) rule tree, and create the **SUPPORTAL_ACL** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privileges
Has Class	**Usp0DesignXChange**	**User**	Administrator user configured as the remote proxy user	Grant these privileges: • **Write** • **Change** • **Remote Check-Out** • **Check-In/Check-Out**



B. Select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** node from the AM rule tree, and create the **SUPPORTAL_ACL** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privileges
Has Class	**Usp0DesignXChangeRevision**	**User**	Administrator user configured as the remote proxy user	Grant these privileges: • **Write** • **Change** • **Remote Check-Out** • **Check-In/ Check-Out**



c. Restart the Pool Manager and the IDSM services on the OEM Sponsor Site and the OEM Supplier Site.

For more information about configuring Multi-Site Collaboration to use the HTTP/HTTPS protocol, see *Configure Multi-Site authentication using HTTP/HTTPS* in *Multi-Site Collaboration* in the Teamcenter documentation.

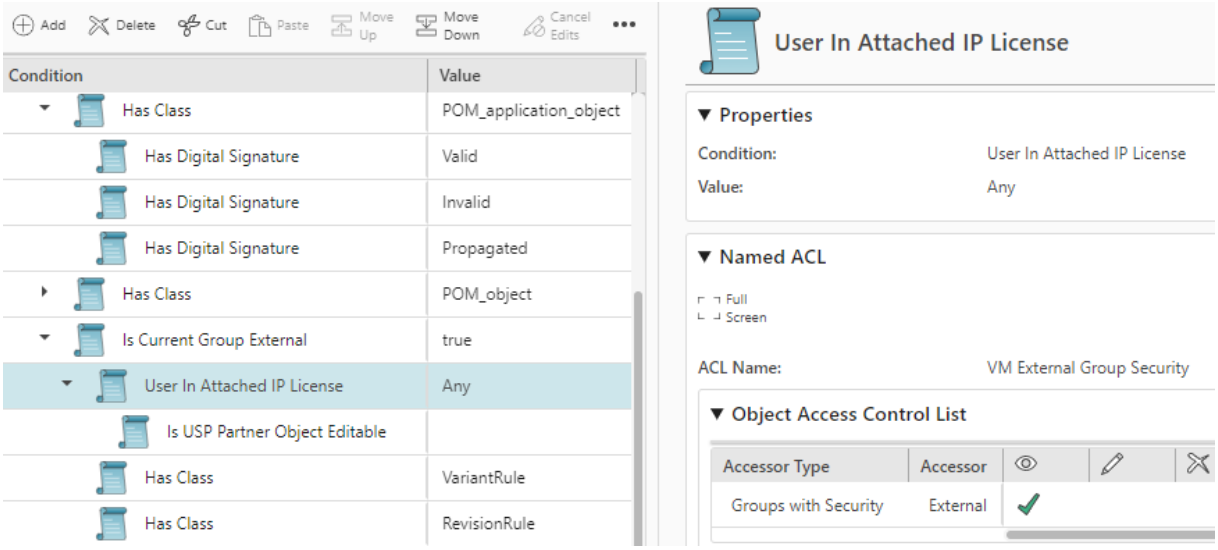
5. Create the following ACLs for Supplier Connect:

a. Log on to the web client as a user with Teamcenter administration privileges.

b. On the home page, click the **ACCESS MANAGER** tile.

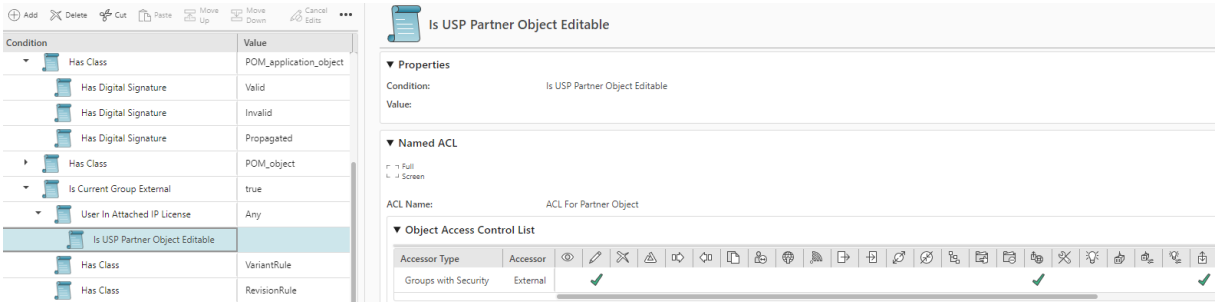
c. Select the **Has Class (POM Object)** > **Is Current Group External** node from the AM rule tree, and create the **VM External Group Security** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privilege
User In Attached IP License	**Any**	**Groups with Security**	**External**	Grant the **Read** privilege.



d. Select the **Has Class (POM Object)** > **Is Current Group External** >**User In Attached IP License** node from the AM rule tree, and create the **ACL For Partner Object** ACL with the following details:

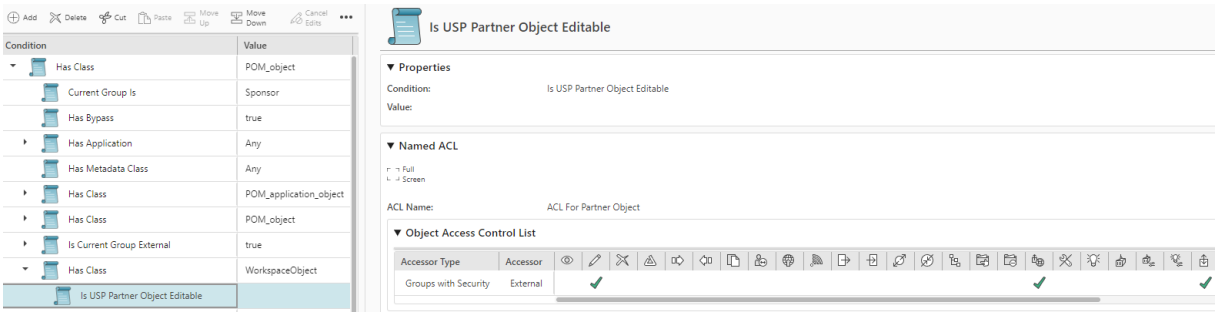
Condition	Value	Accessor Type	Accessor	Privileges
Is USP Partner Object Editable		**Groups with Security**	**External**	Grant these privileges: • **Write** • **Remote Check-Out** • **Check-In Check-Out**



e. Select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** node from the AM rule tree, and create the **ACL For Partner Object** ACL with the following details:

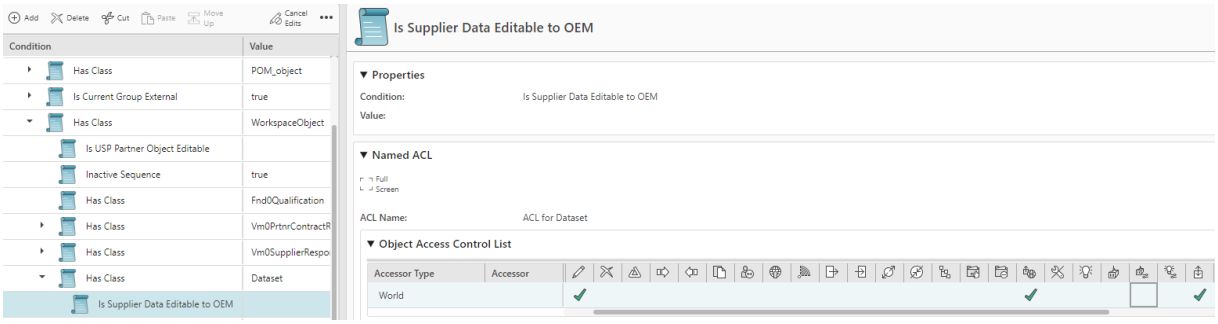
Condition	Value	Accessor Type	Accessor	Privilege
Is USP Partner Object Editable		**Groups with Security**	**External**	Grant these privileges: • **Write**

Condition	Value	Accessor Type	Accessor	Privilege
				• **Remote Check-Out** • **Check-In/Check-Out**



f. Select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** > **Has Class (Dataset)** node from the AM rule tree, and create the **ACL for Dataset** ACL with the following details:

Condition	Accessor Type	Privileges
Is Supplier Data Editable to OEM	**World**	Grant these privileges: • **Write** • **Remote Check-Out** • **Check-In/Check-Out**



6. Set up naming rules for data exchange packages.

> Caution:
>
> If you do not set up naming rules, it will result in data conflicts when suppliers submit their responses. Create separate naming rules for the OEM Sponsor Site and the OEM Supplier Site.

Naming rules define the data entry format for a business object property. A naming rule consists of rule patterns and a counter. After you create a naming rule, you must attach it to the business object property. You can also attach it to a property on all the business objects that use that property. Create a package in Business Modeler Integrated Development Environment (Business Modeler IDE) with the required naming rules, and deploy the package.

a. In Business Modeler IDE, create a new Business Modeler IDE template project.

b. Search for and select the following templates:

- **Supplier Connect**
- **Supplier Connect for AW**
- **Active Workspace**
- **Vendor Management**
- **Vendor Management Active Workspace**
- **Active Content Structure**

c. Click **Finish**.

d. Search for and open the **Usp0designXChangeRevision** business object.

e. Click the **Usp0DesignXchange** Item to open the item revision associated with it.

f. In the **Usp0DesignXchange** business object, click the **Properties** tab.

g. Select the **item_id** property in the properties table, and click the **Add** button in the **Naming Rule Attaches** tab.

h. In the **Naming Rule** dialog box, in **Name**, type the name for the new naming rule. The name must begin with the project prefix.

i. To add a naming rule pattern in the **Patterns** list, click **Add**.

j. In the **Pattern** dialog box, enter information for the new rule pattern.

For this parameter	Do this
Pattern	Enter a naming pattern. You can add pattern characters in three ways: • Type characters using the keyboard. • Click **Insert LOV** and add an LOV.

For this parameter	Do this
	• Click **Insert Rule** and add an existing naming rule. Example: For a three-digit numeric pattern from 001 to 999, type **nnn**. For a two-character alphabetic pattern from aa to zz, type **aa**. For a two-character pattern from AA to ZZ, type **AA**. For an alphanumeric pattern, for example, from A001 to Z999, type **Annn**. The following dynamic characters can be used in naming rule patterns: **U** Uppercase dynamic character **u** Lowercase dynamic character **D** Mixed-case dynamic character When you use a dynamic character in a pattern and select the **Generate Counter** ☑ check box, the corresponding characters typed in the **Initial Value** box are used in all subsequent IDs. Example: If the pattern is **UUU"-"NNNNN** and you type **REQ-00000** in the **Initial Value** box, then all IDs automatically generated using this pattern begin with **REQ** (**REQ-00000**, **REQ-00001**, **REQ-00002**, and so on). However, end users can override the generated text on the user interface. For example, they can either click **Assign**, or they can replace the **REQ** in the ID with some other text. Therefore, the pattern is dynamic, allowing it to be changed by end users.
Description	Type a brief description of the naming rule.
Generate counters?	Select the check box if you want to generate counters from the pattern. When a naming rule includes multiple patterns that generate counters, a selection list of the patterns will be available in the Teamcenter client for use with **Assign**. Patterns that include an inserted LOV, an inserted naming rule, a system variable that is not enclosed in quotation marks, or a regular expression cannot be used to generate counters.
Is Decrement?	Select the check box if the counter is to be reduced by the step amount.
Initial Value and **Maximum Value**	If you selected the **Generate counters?** check box, then type characters that match the pattern to set the initial and maximum values.

For this parameter	Do this
	For example, if you entered **nnn** for the pattern, type a three-digit number in the **Initial Value** box and the **Maximum Value** box, such as **100** and **899**. Alternatively, if you entered a pattern of **Annn**, then you might type **A001** and **Z999**.
Step	Type the amount by which the generated counters are to be incremented. The default is **1**, meaning that each additional number that is generated is to be increased by one.
Offset	Type a number by which the generated counter is increased the first time the rule is used. The default is **0**, implying that there is no offset.

k. Click **Finish**.

l. On the main toolbar click **Save Data Model**.

m. Generate a software package for distribution and deploy the package using Deployment Center.

For more information about generating a software package for distribution, see *BMIDE for Data Model Design* in the Teamcenter documentation. For more information about deploying a package using Deployment Center, see *Deployment Center — Usage Guide* in the Teamcenter documentation.

7. For the **Supplier Connect Orchestration Translator**, update the administrator credentials for the translator.

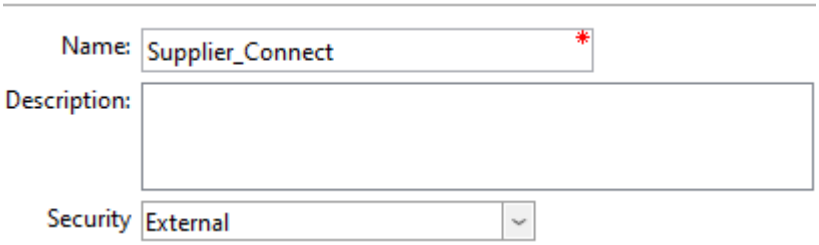
a. Navigate to the *DISPATCHER_ROOT\Module\Translators\supportalorchestrationservice\supportalorchestrationservice.bat* file.

b. Update the `-u` and `-pf` parameters with the required administrator credentials in the following line:

```
"%TC_ROOT%\bin\supportal_orchestration.exe" -u="CHANGE_ME"
-pf="CHANGE_ME" -g="CHANGE_ME" %arg1%=%arg2%
```

8. Set up a group of Teamcenter user accounts for the suppliers as follows:

a. In Teamcenter Organization, create a group with its security set to **External**.



b. In this group, create subgroups for each vendor, and set the security of each group to **External**.

c. Add the Teamcenter user accounts for the suppliers to their respective vendor group.

9. Assign a default sponsor for the Self Service packages requested by suppliers as follows:

a. Log on as a user with Teamcenter administration privileges.

b. On the home page, click the **PREFERENCES** tile.

c. In the **Search** box, type **SUPPORTAL_SelfServiceSponsor**.

d. Specify the User ID of the default sponsor for the Self Service packages.

e. Click **Save** to save your changes.

10. To ensure that suppliers have access only to the objects assigned to their specific project, do the following:

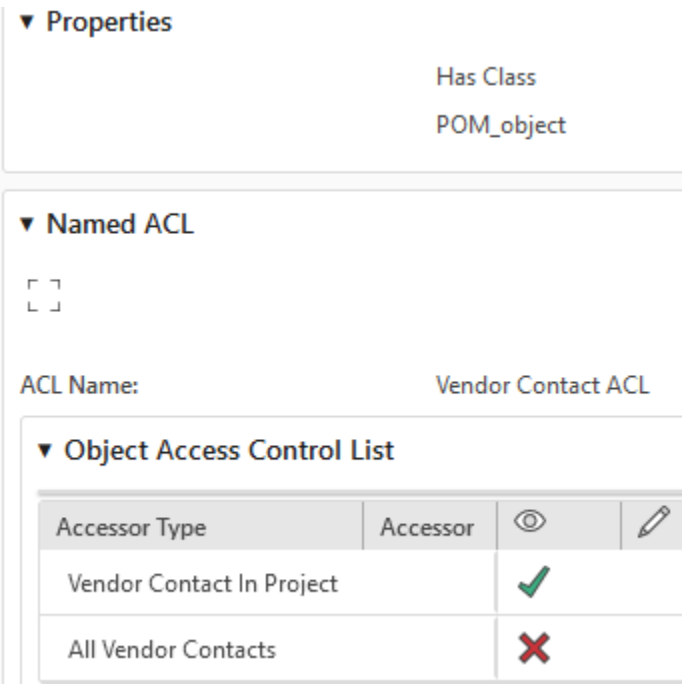
a. Create the following ACL:

A. Log on to the web client as a user with Teamcenter administration privileges.

B. On the home page, click the **ACCESS MANAGER** tile.

C. Select the **Has Class (POM Object)** > **Has Class (POM_object)** node from the AM rule tree, and create the **Vendor Contact** ACL with the following details:

Condition	Value	Accessor Type	Privilege
Has Class	**POM_object**	**Vendor Contact in Project**	Grant the **Read** privilege.
Has Class	**POM_object**	**All Vendor Contacts**	Deny the **Read** privilege.



b. Create the required projects.

c. Assign or remove assemblies to or from projects.

d. Assign suppliers to their associated projects.

e. Export the projects to the OEM Supplier Site by using the **admin_data_export** utility. For more information about using the **admin_data_export** utility, see *Teamcenter Utilities* in the Teamcenter documentation.

   Copy the generated ZIP file to the OEM Supplier Site. The location of this file is specified in the **-outputPackage** argument.

> Note:
>
> You must run this utility whenever you create a new project to keep the data synchronized.

11. By default, inaccessible assembly components are displayed with **<<UNREADABLE>>**. To prevent the display of **<<UNREADABLE>>** in an assembly, set the **BOM_hide_unreadable_lines** preference to **All** in the OEM Supplier Site.

12. To use subtypes of Supplier Connect objects, you must configure the following preferences with the names of the subtype objects:

    - **SUPPORTAL_Usp0OEMDeXChange_type_name**

- **SUPPORTAL_Usp0SupDeXChange_type_name**

13. If you are working with multiple OEM Sponsor Sites, do the following additional configurations:

    a. Create separate naming rules for each of the multiple OEM Sponsor Sites.

    b. Ensure that the encryption keys are the same on all the sites.

7. Configure Supplier Connect on the OEM Supplier Site

After installing Supplier Connect, you must configure the OEM Supplier Site to connect with the OEM Sponsor Site. When you complete the required configurations, the sponsors and suppliers can exchange data successfully.

> Note:
>
> Siemens Digital Industries Software recommends that you define the site name of the OEM Supplier Site in this format: **Supplier_Connect_Site_Name**. This allows you to quickly identify the OEM Supplier Site.

Prerequisites

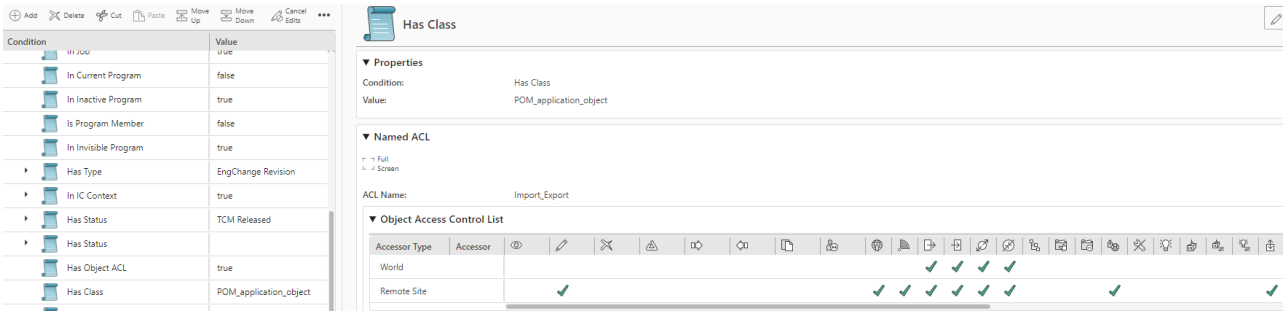
- Supplier Connect must be installed at the OEM Sponsor Site and the OEM Supplier Site.
- Configure Multi-Site Collaboration between the OEM Sponsor Site and the OEM Supplier Site as specified in the Teamcenter documentation, specifically in:
  - *Prepare the Multi-Site Collaboration environment* in *Teamcenter Installation Using Deployment Center* in the Teamcenter documentation.
  - *Multi-Site Collaboration deployment options* in *Multi-Site Collaboration* in the Teamcenter documentation.
  - *Determining the setup process* in *Multi-Site Collaboration* in the Teamcenter documentation.
  - *Configure Multi-Site Collaboration sites* in *Multi-Site Collaboration* in the Teamcenter documentation.
- Verify that Multi-Site Collaboration is configured correctly on the OEM Sponsor Site and the OEM Supplier Site. Ensure that you have done the following:
  - In the OEM Sponsor Site and the OEM Supplier Site, configure the following preferences with the **Site Name** of the OEM Sponsor Site and the OEM Supplier Site:

Preference	Value
IDSM_permitted_sites	*<OEM Sponsor Site name>*, *<OEM Supplier Site name>*
IDSM_permitted_checkout_sites	*<OEM Sponsor Site name>*, *<OEM Supplier Site name>*
IDSM_permitted_transfer_sites	*<OEM Sponsor Site name>*, *<OEM Supplier Site name>*

- Run the **dsa_util** utility to ensure that the OEM Sponsor Site and the OEM Supplier Site are connected. For more information, see *Multi-Site Collaboration* in the Teamcenter documentation.

- Select the **Has Class (POM Object)** node from the Access Manager rule tree, and create the **Import/Export** access control list (ACL) with the following details:

Condition	Value	Accessor Type	Privileges
Has Class	**POM Application Object**	**World**	Grant these privileges: ■ **Export** ■ **Import** ■ **Transfer Out** ■ **Transfer In**
		Remote Site	Grant these privileges: ■ **Write** ■ **Publish** ■ **Subscribe** ■ **Export** ■ **Import** ■ **Transfer Out** ■ **Transfer In** ■ **Remote Check-Out** ■ **Check-In/Check-Out**



Procedure

1. To specify the OEM Sponsor Site for exchanging data, set the **SUPPORTAL_share_site_names** preference to the Teamcenter site name specified for the OEM Sponsor Sites.

2. To send notification emails through the data exchange process, set up an email server with the following details:

   - Set the **Mail_server_name** preference to a valid SMTP mail server.
   - Set the **Mail_OSMail_activated** preference to **true** to enable operating system emails from Teamcenter.
   - Set the port used by the mail server to **25**.

   > Note:
   >
   > To disable notification emails from Supplier Connect, set the **SUPPORTAL_Enable_Mail_Notifications** preference to **False**.

3. To set up a confidentiality agreement between the OEM and the supplier, configure the following preferences:

   - Set the **LoginCountry_selection_enabled** preference to **True** to display the **Country Selection** dialog box for suppliers to select the country from which they are logging in.
   - Set the **LoginCountry_save_previous_selection** preference to **True** to allow suppliers to save the previous country selection in the **Country Selection** dialog box.
   - To modify the text in the confidentiality agreement statement, do the following:

     a. Create an untranslatable resource file, *custom-name*_**text.xml**.

     b. Add the existing key (**LoginCountry_confidentiality_statement**) located in the **tc_text_locale.xml** file to the *custom-name*_**text.xml** file.

     c. Add the custom file to the **TC_USER_MSG_DIR***language_locale* directory.

     > Note:
     >
     > *language_locale* is the JAVA standard language name. For example, **fr_FR**.

     d. Modify the **LoginCountry_confidentiality_statement** in the **TC_USER_MSG_DIR***language_locale**custom-name*_**text.xml** file.

> Note:
>
> For tips about creating a confidentiality statement, see *Configure confidentiality agreement* in *Teamcenter Security* in the Teamcenter documentation.

4. If you have configured Multi-Site Collaboration to use remote procedure call (RPC) technology to communicate between the sites, do the following:

   a. For the Integrated Distributed Services Manager (IDSM) service in the OEM Sponsor Site and the OEM Supplier Site, ensure that you change the service's **Log on as** user from **infodba** to another user with database administrator privileges as follows:

      A. Edit the *TC_BIN***run_tc_idsm.bat** script file.

      B. Set the value of **TC_USER** from **infodba** to another user with database administrator privileges.

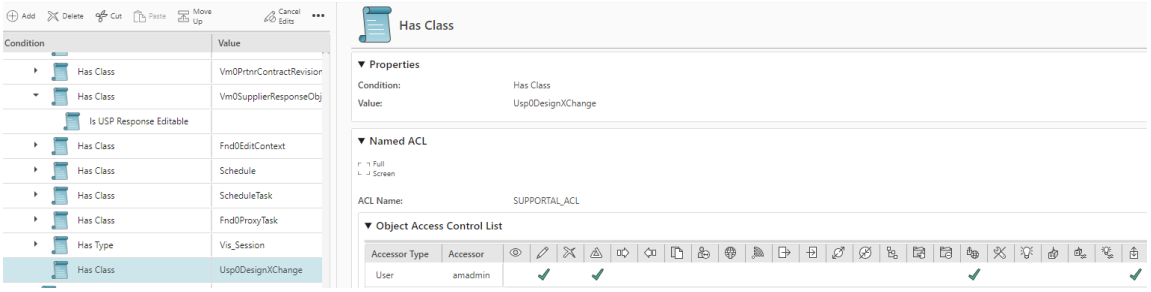
      C. Set the value of **TC_USER_PASSWD_FILE** from the password file of the **infodba** user to another user with database administrator privileges.

      D. Save the **run_tc_idsm.bat** file.

   b. For the IDSM service user with database administrator privileges, grant permissions to write, change, remotely check out an object, and override the checkout of an object by another user.

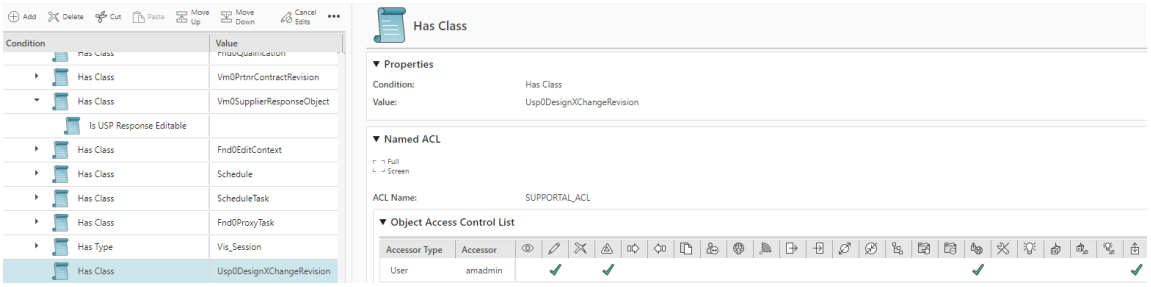
      A. In Teamcenter Access Manager, select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** node from the Access Manager (AM) rule tree, and create the **SUPPORTAL_ACL** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privileges
Has Class	**Usp0DesignXChange**	**User**	Administrator user specified as the IDSM administrator in the *run_tc_idsm.bat* script file	Grant these privileges: • **Write** • **Change** • **Remote Check-Out** • **Check-In/ Check-Out**



B. Select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** node from the AM rule tree, and create the **SUPPORTAL_ACL** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privileges
Has Class	**Usp0DesignXChangeRevision**	**User**	Administrator user specified as the IDSM administrator in the *run_tc_idsm.bat* script file	Grant these privileges: • **Write** • **Change** • **Remote Check-Out** • **Check-In/ Check-Out**



c. Restart the Pool Manager and the IDSM services on the OEM Sponsor Site and the OEM Supplier Site.

For more information about configuring Multi-Site Collaboration to use RPC, see *Methods for communicating through a firewall* in *Multi-Site Collaboration* in the Teamcenter documentation.

5. If you have configured Multi-Site Collaboration to use the HTTP/HTTPS protocol to communicate between the sites, do the following:

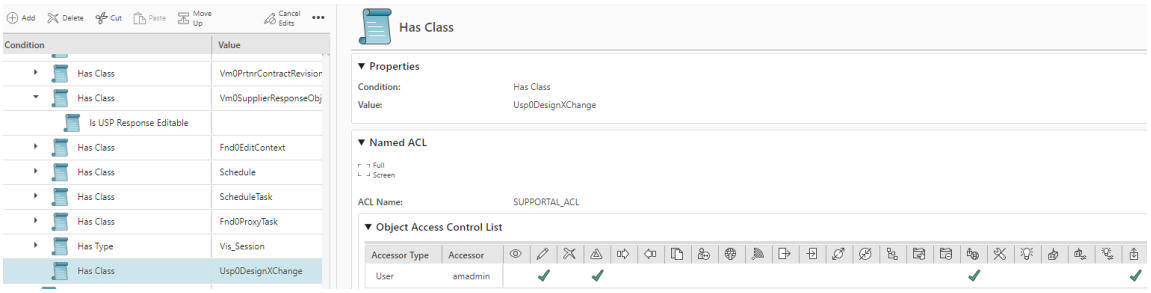
a. Define the **ASYNC_ALLOW_FALLBACK** environment variable, and set its value to **TRUE**.

```
ASYNC_ALLOW_FALLBACK=TRUE
```

b. For the administrator user configured as the remote proxy user, grant permissions to write, change, remotely check out an object, and override the checkout of an object by another user.

A. In Teamcenter Access Manager, select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** node from the Access Manager (AM) rule tree, and create the **SUPPORTAL_ACL** ACL with the following details:

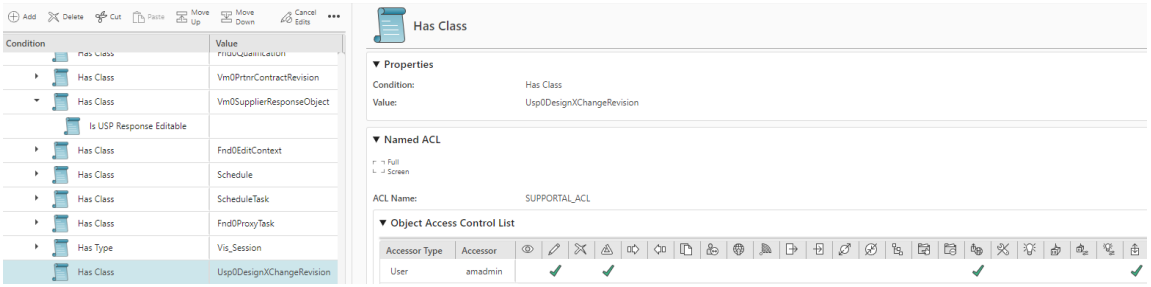
Condition	Value	Accessor Type	Accessor	Privileges
Has Class	**Usp0DesignXChange**	**User**	Administrator user configured as the remote proxy user	Grant these privileges: • **Write** • **Change** • **Remote Check-Out** • **Check-In/Check-Out**



B. Select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** node from the AM rule tree, and create the **SUPPORTAL_ACL** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privileges
Has Class	**Usp0DesignXChangeRevision**	**User**	Administrator user configured as the remote proxy user	Grant these privileges: • **Write** • **Change**

Condition	Value	Accessor Type	Accessor	Privileges
				• **Remote Check-Out** • **Check-In/ Check-Out**



c. Restart the Pool Manager and the IDSM services on the OEM Sponsor Site and the OEM Supplier Site.

For more information about configuring Multi-Site Collaboration to use the HTTP/HTTPS protocol, see *Configure Multi-Site authentication using HTTP/HTTPS* in *Multi-Site Collaboration* in the Teamcenter documentation.

6. Set up naming rules for data exchange packages.

> Caution:
>
> If you do not set up naming rules, it will result in data conflicts when suppliers submit their responses. Create separate naming rules for the OEM Sponsor Site and the OEM Supplier Site.

Naming rules define the data entry format for a business object property. A naming rule consists of rule patterns and a counter. After you create a naming rule, you must attach it to the business object property. You can also attach it to a property on all the business objects that use that property. Create a package in Business Modeler Integrated Development Environment (Business Modeler IDE) with the required naming rules, and deploy the package.

a. In Business Modeler IDE, create a new Business Modeler IDE template project.

b. Search for and select the following templates:

- **Supplier Connect**
- **Supplier Connect for AW**
- **Active Workspace**

- **Vendor Management**
- **Vendor Management Active Workspace**
- **Active Content Structure**

c. Click **Finish**.

d. Search for and open the **Usp0designXChangeRevision** business object.

e. Click the **Usp0DesignXchange** Item to open the item revision associated with it.

f. In the **Usp0DesignXchange** business object, click the **Properties** tab.

g. Select the **item_id** property in the properties table, and click the **Add** button in the **Naming Rule Attaches** tab.

h. In the **Naming Rule** dialog box, in **Name**, type the name for the new naming rule. The name must begin with the project prefix.

i. To add a naming rule pattern in the **Patterns** list, click **Add**.

j. In the **Pattern** dialog box, enter information for the new rule pattern.

For this parameter	Do this
Pattern	Enter a naming pattern. You can add pattern characters in three ways: • Type characters using the keyboard. • Click **Insert LOV** and add an LOV. • Click **Insert Rule** and add an existing naming rule. Example: For a three-digit numeric pattern from 001 to 999, type **nnn**. For a two-character alphabetic pattern from aa to zz, type **aa**. For a two-character pattern from AA to ZZ, type **AA**. For an alphanumeric pattern, for example, from A001 to Z999, type **Annn**. The following dynamic characters can be used in naming rule patterns: **U** Uppercase dynamic character **u** Lowercase dynamic character **D** Mixed-case dynamic character

For this parameter	Do this
	When you use a dynamic character in a pattern and select the **Generate Counter** ☑ check box, the corresponding characters typed in the **Initial Value** box are used in all subsequent IDs. Example: If the pattern is **UUU"-"NNNNN** and you type **REQ-00000** in the **Initial Value** box, then all IDs automatically generated using this pattern begin with **REQ** (**REQ-00000**, **REQ-00001**, **REQ-00002**, and so on). However, end users can override the generated text on the user interface. For example, they can either click **Assign**, or they can replace the **REQ** in the ID with some other text. Therefore, the pattern is dynamic, allowing it to be changed by end users.
Description	Type a brief description of the naming rule.
Generate counters?	Select the check box if you want to generate counters from the pattern. When a naming rule includes multiple patterns that generate counters, a selection list of the patterns will be available in the Teamcenter client for use with **Assign**. Patterns that include an inserted LOV, an inserted naming rule, a system variable that is not enclosed in quotation marks, or a regular expression cannot be used to generate counters.
Is Decrement?	Select the check box if the counter is to be reduced by the step amount.
Initial Value and **Maximum Value**	If you selected the **Generate counters?** check box, then type characters that match the pattern to set the initial and maximum values. For example, if you entered **nnn** for the pattern, type a three-digit number in the **Initial Value** box and the **Maximum Value** box, such as **100** and **899**. Alternatively, if you entered a pattern of **Annn**, then you might type **A001** and **Z999**.
Step	Type the amount by which the generated counters are to be incremented. The default is **1**, meaning that each additional number that is generated is to be increased by one.
Offset	Type a number by which the generated counter is increased the first time the rule is used. The default is **0**, implying that there is no offset.

k. Click **Finish**.

l. On the main toolbar click **Save Data Model**.

m. Generate a software package for distribution and deploy the package using Deployment Center.

For more information about generating a software package for distribution, see *BMIDE for Data Model Design* in the Teamcenter documentation. For more information about deploying a package using Deployment Center, see *Deployment Center — Usage Guide* in the Teamcenter documentation.

7. For the **Supplier Connect Orchestration Translator**, update the administrator credentials for the translator.

   a. Navigate to the *DISPATCHER_ROOT\Module\Translators\supportalorchestrationservice\supportalorchestrationservice.bat* file.

   b. Update the `-u` and `-pf` parameters with the required administrator credentials in the following line:

```
"%TC_ROOT%\bin\supportal_orchestration.exe" -u="CHANGE_ME"
-pf="CHANGE_ME" -g="CHANGE_ME" %arg1%=%arg2%
```

8. Configure the roles that can access the **Supplier** workspace as follows:

   a. Use the *export_wsconfig* utility to export workspace definitions from the Teamcenter command prompt.

   This is a Teamcenter platform command, and it must be run in a Teamcenter command-line environment. Information on how to *manually configure the Teamcenter environment* can be found in the Teamcenter *Utilities Reference* documentation.

   In the following example, all existing workspace definitions are exported.

```
export_wsconfig -u=<username> -p=<password> -g=<groupname>
-file="c:/exportedWorkspacesConfig.xml"
```

   b. In the exported file, search for **Usp1Supplier** to edit the available roles for the **Supplier** workspace.

   c. Add the roles that can access the **Supplier** workspace.

```
<Workspace id="Usp1Supplier">
    <WorkspaceMapping  group="" role="External Designer"
default="true"/>
    <WorkspaceMapping  group="" role="Supplier" default="true"/>
</Workspace>
```

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<Import>
<Workspace id="Usp1Supplier">
        <WorkspaceMapping  group="" role="External Designer" default="true"/>
        <WorkspaceMapping  group="" role="Supplier" default="true"/>
</Workspace>
</Import>
```

By default, **External Designer** roles can access the **Supplier** workspace.

d. Use the *import_wsconfig* utility to import the **Supplier** workspace definition.

In the following example, you import the *exportedWorkspacesConfig.xml* custom file, which contains the **Supplier** workspace definition.

```
import_wsconfig -u=<username> -p=<password> -g=<groupname>
-file="c:/exportedWorkspacesConfig.xml"
```

9. Ensure that you have set up the Partner Connect ACLs on the OEM Supplier Site before configuring the Supplier Connect ACLs on this site.

For more information, see *Partner Connect — Deployment and Administration* in the Teamcenter documentation.

10. If you have installed Supplier Connect in a new Teamcenter environment, set up the ACLs as follows:

a. Define the access privileges for the suppliers by running the **vm_install_am_rule** utility. For more information, see *Define the access privileges for the partner representatives* in *Partner Connect Administration* in the Teamcenter documentation.

b. Define the access privileges for the data exchange packages by running the **supportal_install_am_rules** utility.

supportal_install_am_rules [**-u=***user-id*] [**-p=***password*] [**-g=***group*] [**-output=***path to the log file*]

-u

Specifies the user ID.

This is generally a user with administration privileges.

-p

Specifies the password.

-g

Specifies the group associated with the user.

If used without a value, the user's default group is considered.

-output

Specifies the absolute path to the generated log file. If no path is specified, the report is generated in the current working directory of the application.

-h

Displays the help for this utility.

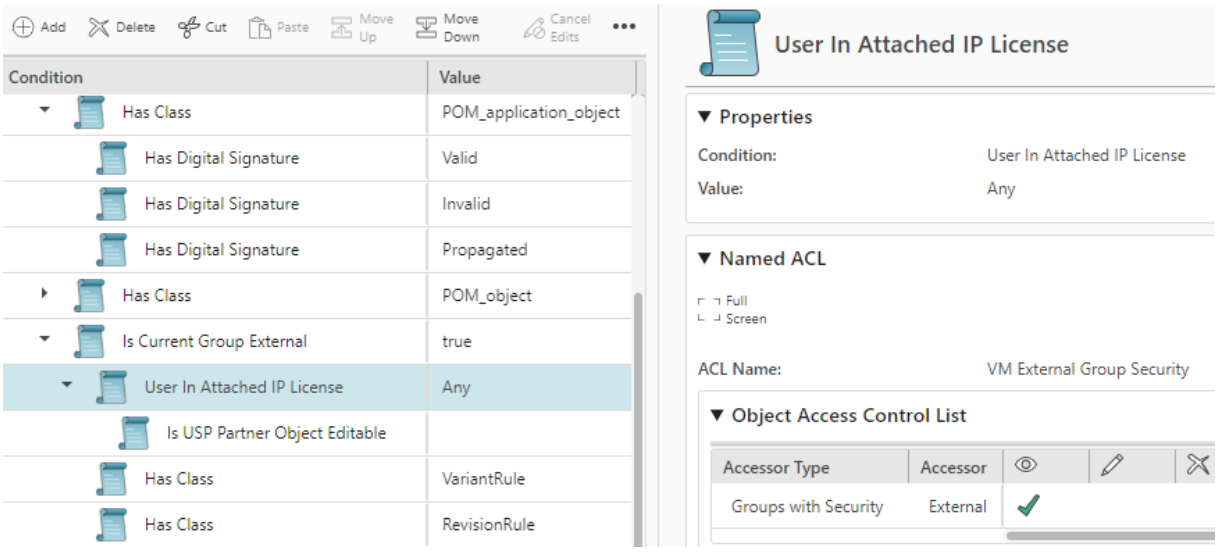
11. If you have installed Supplier Connect in an existing Teamcenter environment, create the following ACLs for Supplier Connect:

    a. Log on to the web client as a user with Teamcenter administration privileges.

    b. On the home page, click the **ACCESS MANAGER** tile.

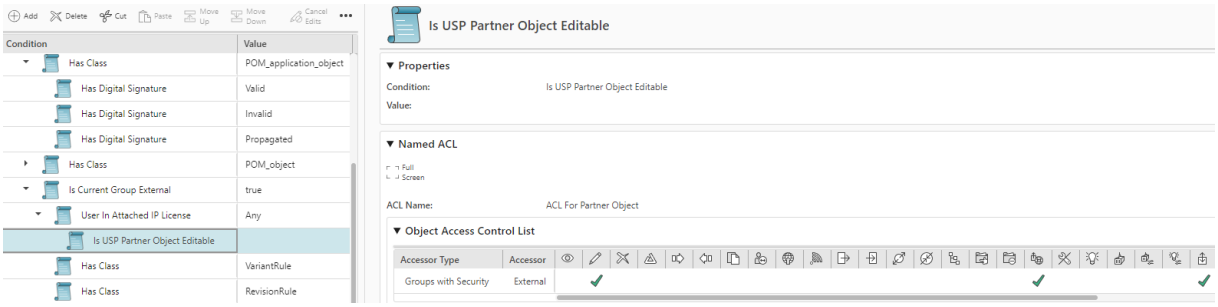
    c. Select the **Has Class (POM Object)** > **Is Current Group External** node from the AM rule tree, and create the **VM External Group Security** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privilege
User In Attached IP License	**Any**	**Groups with Security**	**External**	Grant the **Read** privilege.



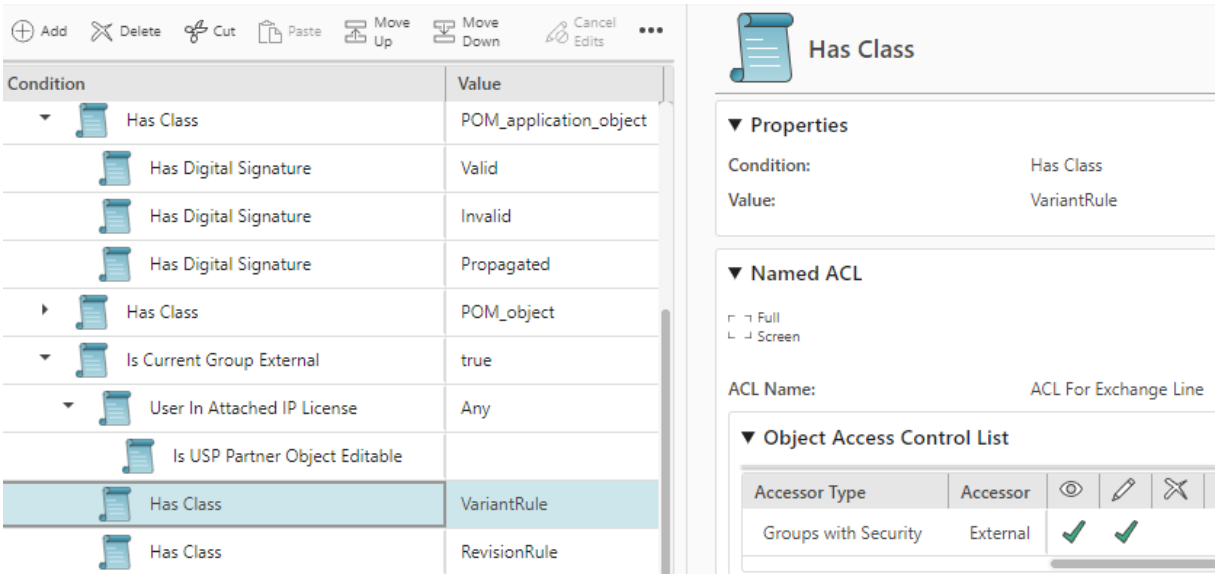
    d. Select the **Has Class (POM Object)** > **Is Current Group External** > **User In Attached IP License** node from the AM rule tree, and create the **ACL For Partner Object** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privileges
Is USP Partner Object Editable		**Groups with Security**	**External**	Grant these privileges: • **Write** • **Remote Check-Out** • **Check-In Check-Out**



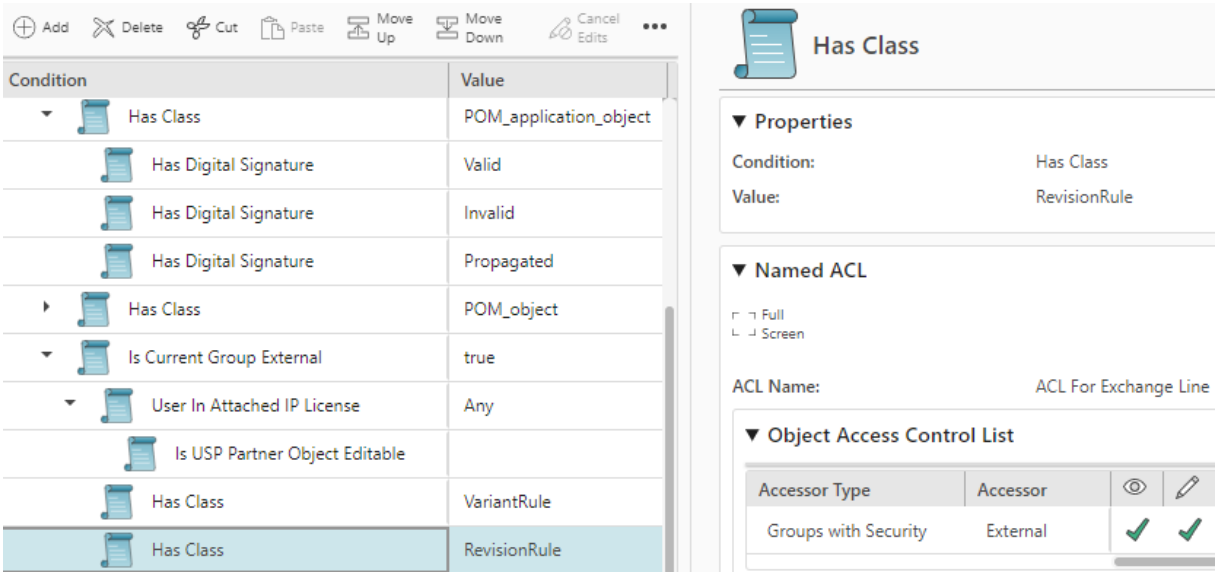
e. Select the **Has Class (POM Object)** > **Is Current Group External** node from the AM rule tree, and create the **ACL For Exchange Line** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privileges
Has Class	**VariantRule**	**Groups with Security**	**External**	Grant these privileges: • **Read** • **Write**



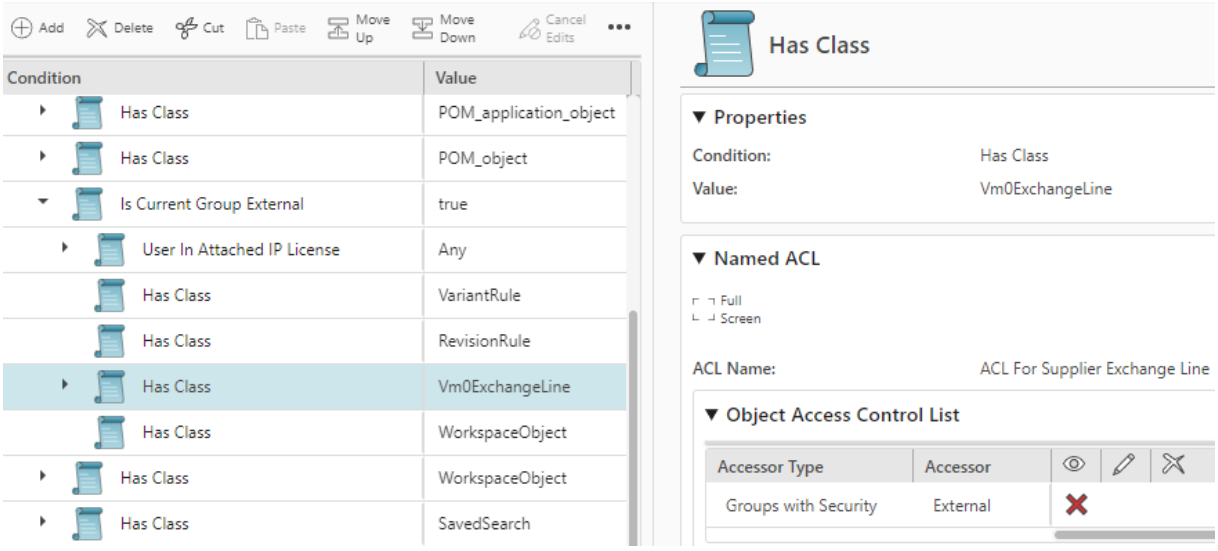
f. In the **Has Class (POM Object)** > **Is Current Group External** node, create the **ACL For Exchange Line** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privileges
Has Class	**RevisionRule**	**Groups with Security**	**External**	Grant these privileges: • **Read** • **Write**



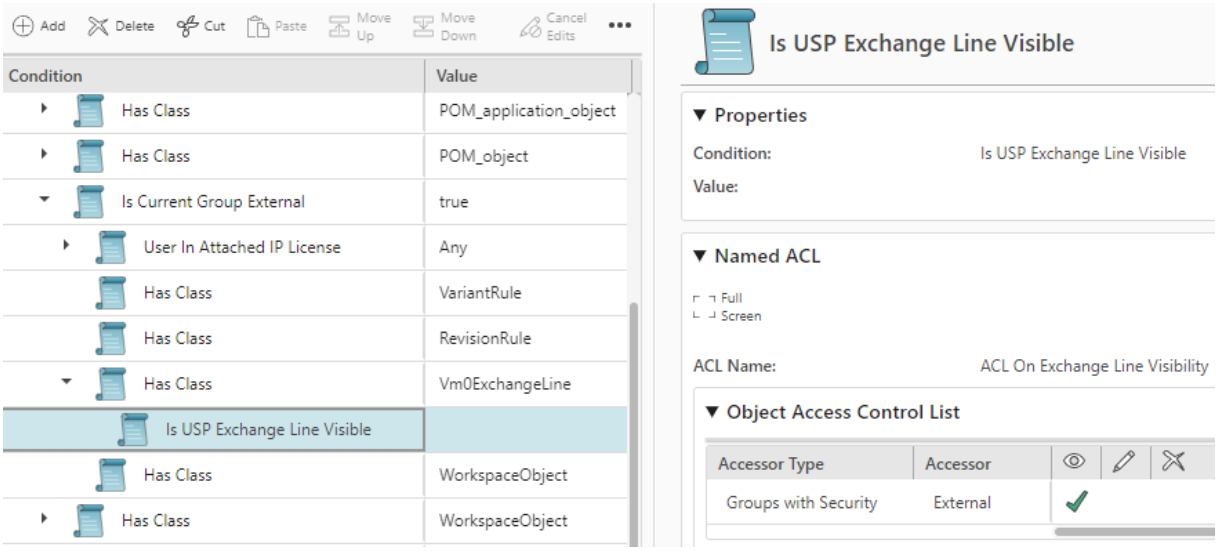
g. In the **Has Class (POM Object)** > **Is Current Group External** node, create the **ACL For Supplier Exchange Line** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privilege
Has Class	**Vm0ExchangeLine**	**Groups with Security**	**External**	Deny the **Read** privilege.



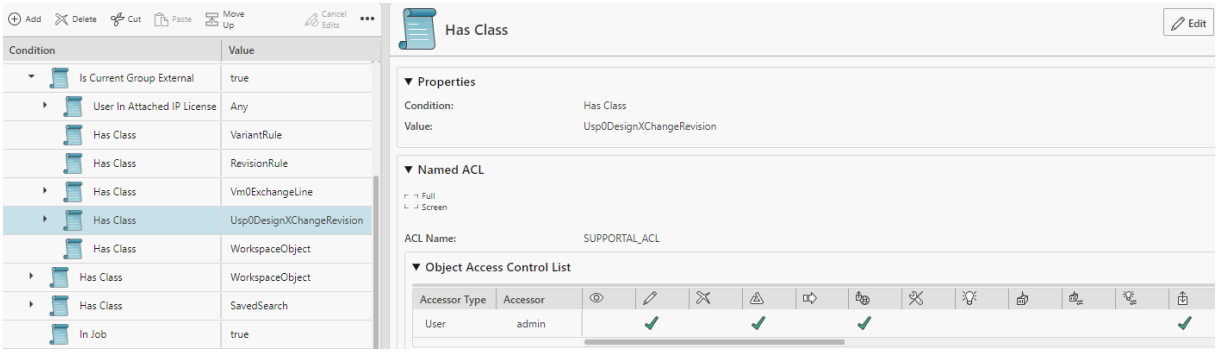
h. Select the **Has Class (POM Object)** > **Is Current Group External** > **Has Class (Vm0ExchangeLine)** node from the AM rule tree, and create the **ACL On Exchange Line Visibility** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privilege
Is USP Exchange Line Visible		**Groups with Security**	**External**	Deny the **Read** privilege.



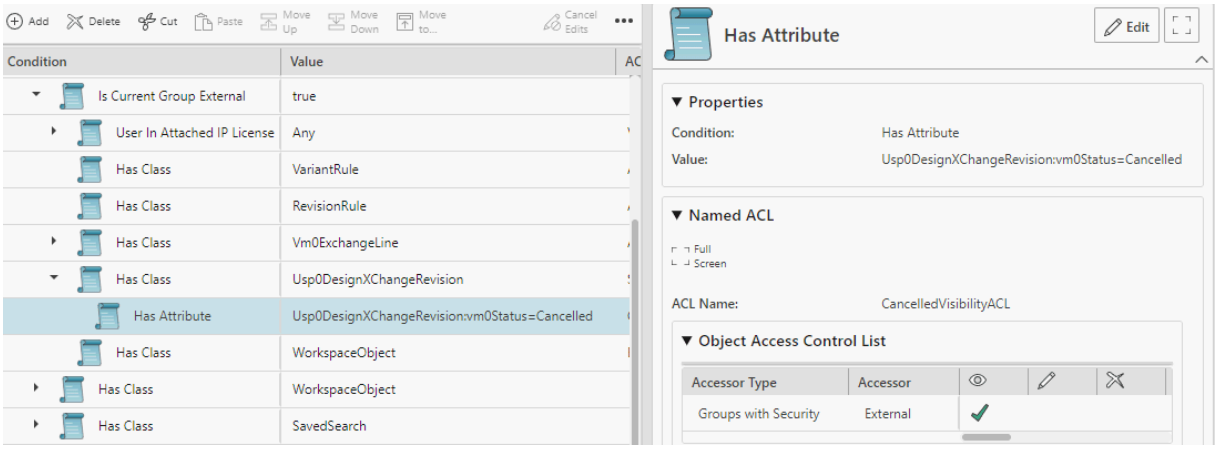
i. Select the **Has Class (POM Object)** > **Is Current Group External** > **Has Class (Usp0DesignXChangeRevision)** node from the AM rule tree, and create the **SUPPORTAL_ACL** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privilege
Has Class	**Usp0DesignXChangeRevision**	**User**	Administrator user specified as the IDSM administrator in the *run_tc_idsm.bat* script file	Grant these privileges: • **Write** • **Change** • **Remote Check-Out** • **Check-In/ Check-Out**



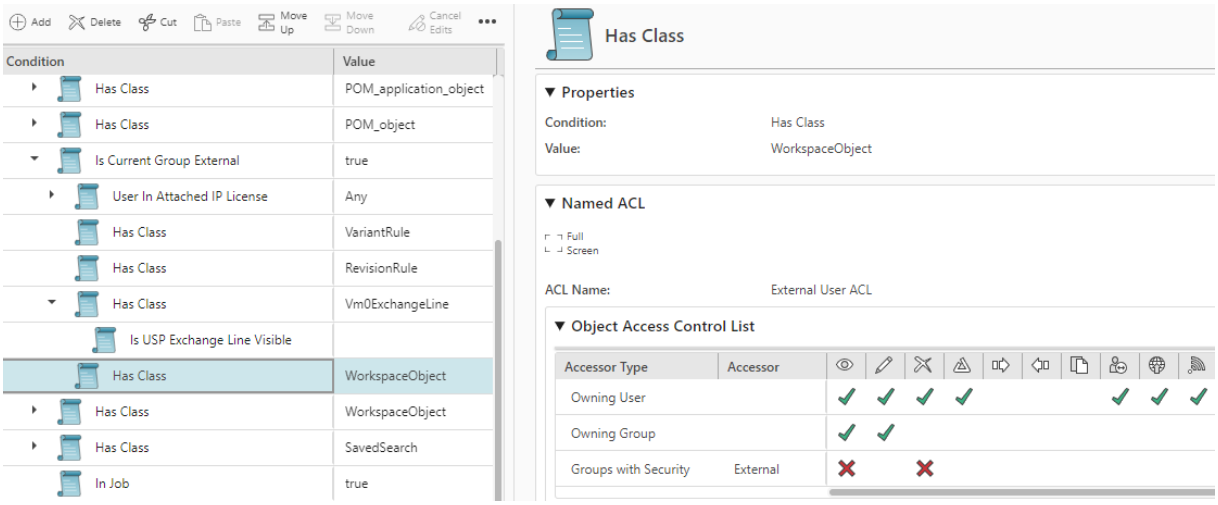
j. Select the **Has Class (POM Object)** > **Is Current Group External** > **Has Class (Usp0DesignXChangeRevision)** node from the AM rule tree, and create the **CancelledVisibilityACL** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privilege
Has Attribute	**Usp0DesignXChangeRevision:vm0Status=Cancelled**	**Groups with Security**	**External**	Grant the **Read** privilege.



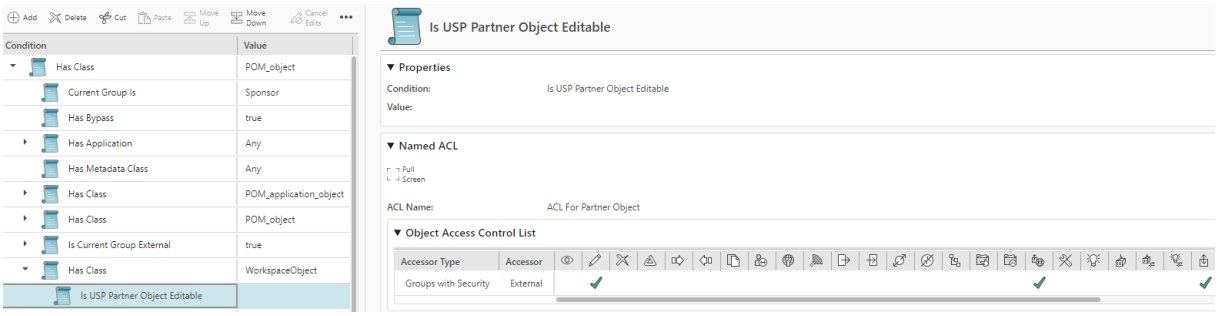
k. Select the **Has Class (POM Object)** > **Is Current Group External** node from the AM rule tree, and create the **External User ACL** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privileges
Has Class	**WorkspaceObject**	**Owning User**		Grant these privileges: • **Read** • **Write** • **Delete** • **Change** • **Change Ownership** • **Publish** • **Subscribe**
		Owning Group		Grant these privileges: • **Read** • **Write**
		Groups with Security	**External**	Deny these privileges: • **Read** • **Delete**



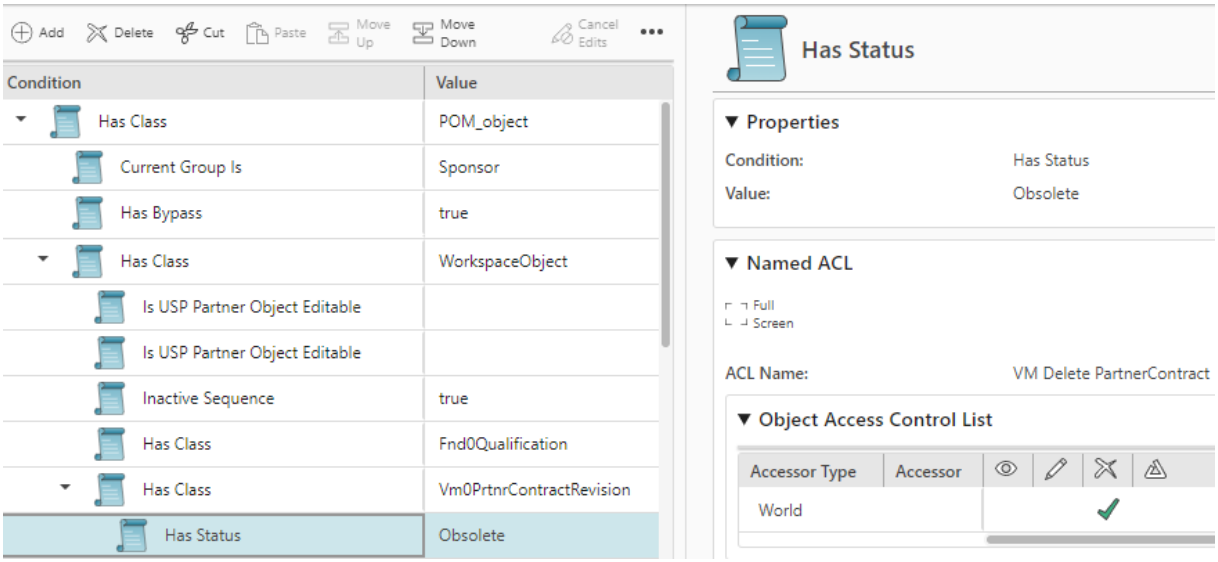
l. Select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** node from the AM rule tree, and create the **ACL For Partner Object** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privilege
Is USP Partner Object Editable		**Groups with Security**	**External**	Grant these privileges: • **Write** • **Remote Check-Out** • **Check-In/Check-Out**



m. Select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** > **Vm0PrtnrContractRevision** node from the AM rule tree, and create the **VM Delete Partner Contract** ACL with the following details:

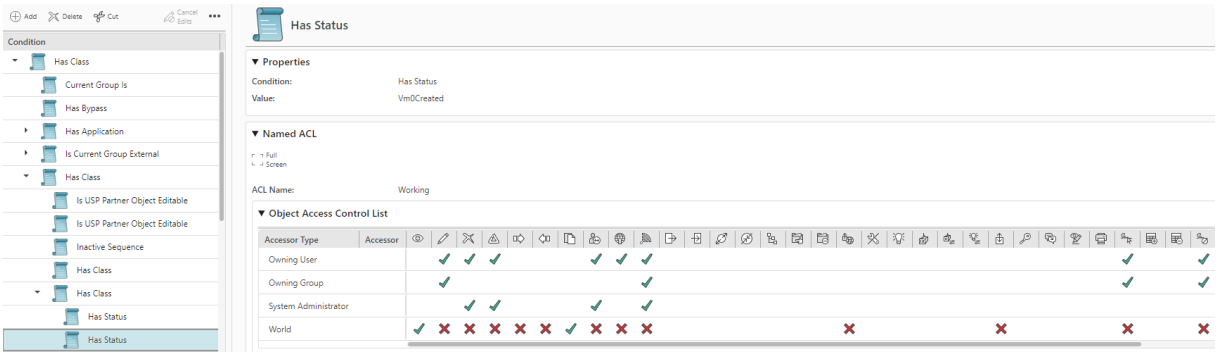
Condition	Value	Accessor Type	Privilege
Has Status	**Obsolete**	**World**	Grant the **Delete** privilege.



n. Create the **Working** ACL with the following details:

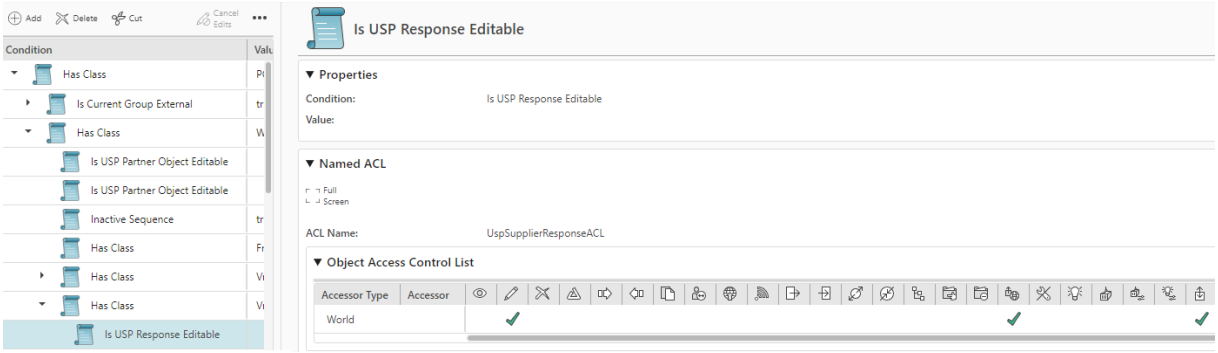
Condition	Value	Accessor Type	Privileges
Has Status	**Vm0Created**	**Owning User**	Grant these privileges: • **Write** • **Delete** • **Change** • **Change Ownership** • **Publish** • **Subscribe** • **Digitally Sign** • **Void Digital Signature**
		Owning Group	Grant these privileges: • **Write** • **Subscribe** • **Digitally Sign** • **Void Digital Signature**

Condition	Value	Accessor Type	Privileges
		System Administrator	Grant these privileges: • **Delete** • **Change** • **Change Ownership** • **Subscribe**
		World	Grant these privileges: • **Read** • **Copy** Deny these privileges: • **Write** • **Delete** • **Change** • **Promote** • **Demote** • **Change Ownership** • **Publish** • **Subscribe** • **Remote Check-Out** • **Check-In/Check-Out** • **Digitally Sign** • **Void Digital Signature**



o. Select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** > **Vm0SupplierResponseObject** node from the AM rule tree, and create the **UspSupplierResponseACL** ACL with the following details:

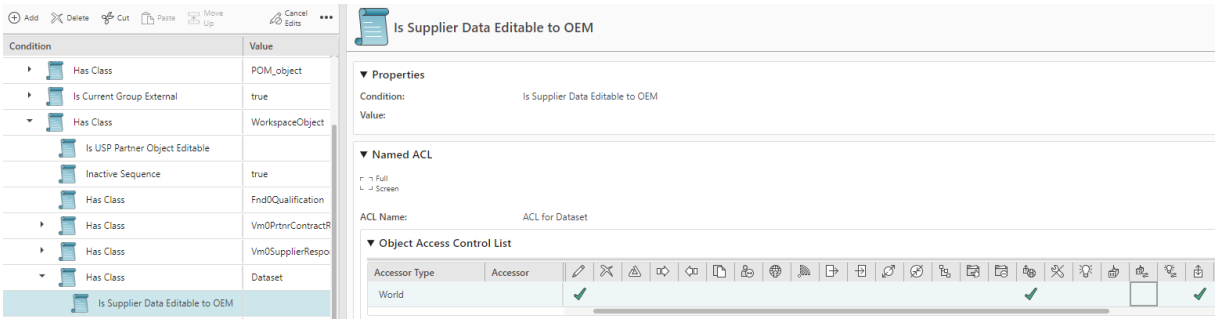
Condition	Accessor Type	Privileges
Is USP Response Editable	**World**	Grant these privileges: • **Write** • **Remote Check-Out** • **Check-In/Check-Out**



p. Select the **Has Class (POM Object)** > **Has Class (WorkspaceObject)** > **Has Class (Dataset)** node from the AM rule tree, and create the **ACL for Dataset** ACL with the following details:

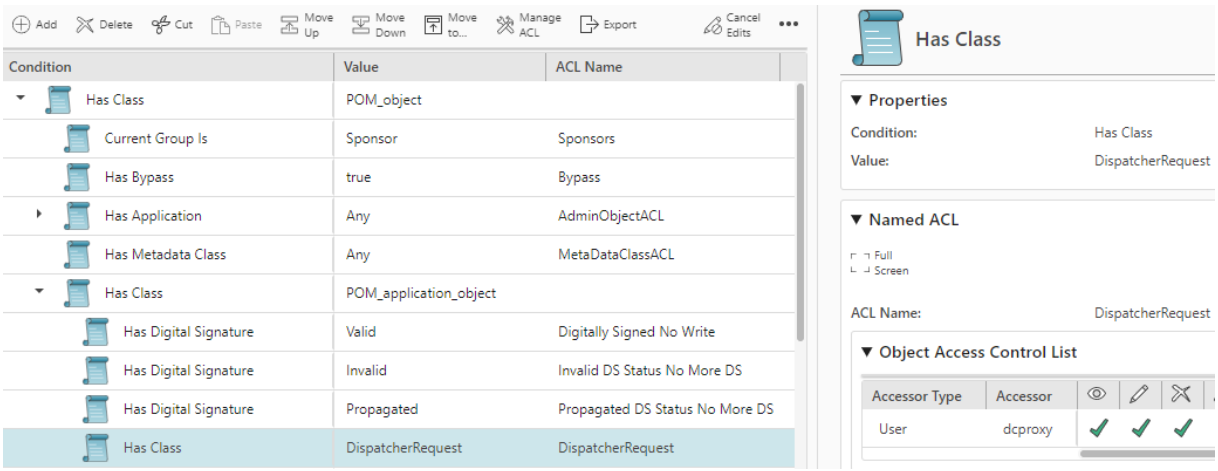
Condition	Accessor Type	Privileges
Is Supplier Data Editable to OEM	**World**	Grant these privileges: • **Write** • **Remote Check-Out**

Condition	Accessor Type	Privileges
		• **Check-In/Check-Out**



q. Select the **Has Class (POM Object)** > **Has Class (POM Application Object)** node from the AM rule tree, and create the **DispatcherRequest** ACL with the following details:

Condition	Value	Accessor Type	Accessor	Privileges
Has Class	**DispatcherRequest**	**User**	**dcproxy**	Grant these privileges: • **Read** • **Write** • **Delete**



12. Configure a supplier's access to only their workflow jobs, workflow tasks, and emails. For more information, see *Partner Connect — Deployment and Administration* in the Teamcenter documentation.

13. Assign a default sponsor for the Self Service packages requested by suppliers as follows:

a. Log on as a user with Teamcenter administration privileges.

b. On the home page, click the **PREFERENCES** tile.

c. In the **Search** box, type **SUPPORTAL_SelfServiceSponsor**.

d. Specify the User ID of the default sponsor for the Self Service packages.

e. Click **Save** to save your changes.

14. To ensure that suppliers have access only to the objects assigned to their specific project, do the following:

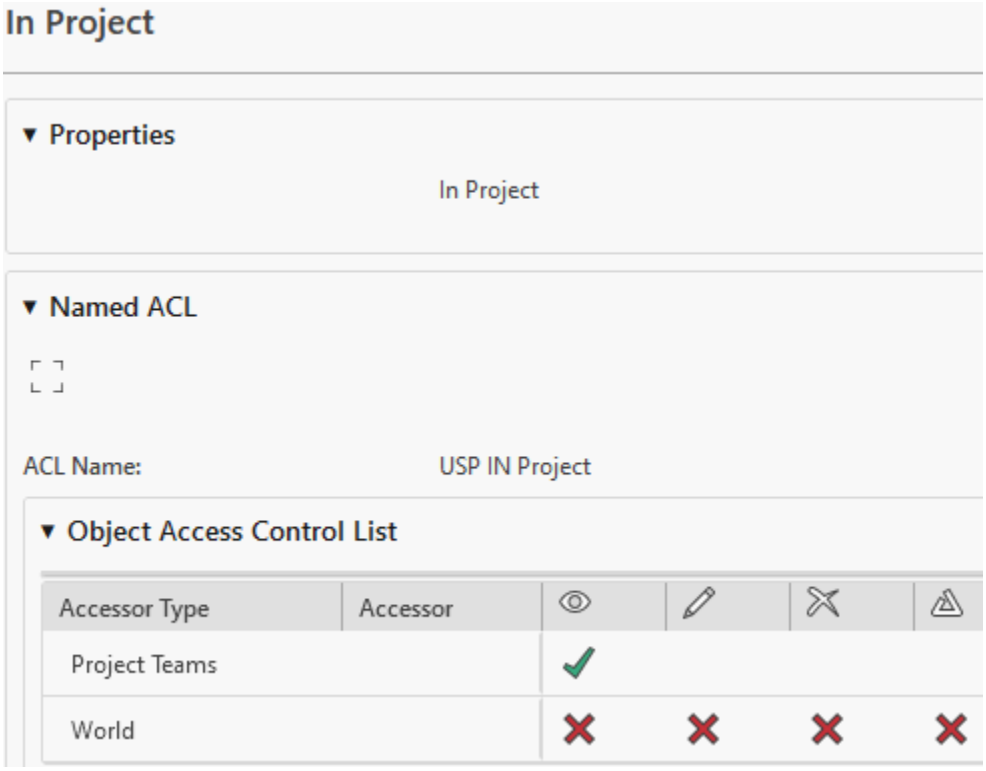
    a. Create the following ACL:

        A. Log on to the web client as a user with Teamcenter administration privileges.

        B. On the home page, click the **ACCESS MANAGER** tile.

        C. Select the **Has Class (POM Object)** > **Is Current Group External** > **User In Attached IP License** > **VM External Group Security** node from the AM rule tree, and create the **USP IN Project** ACL with the following details:

Condition	Accessor Type	Privileges
In Project	**Project Teams**	Grant the **Read** privilege.
In Project	**World**	Deny these privileges: • **Read** • **Write** • **Delete** • **Change**



b. Import the projects by using the **admin_data_import** utility. For more information about using the **admin_data_import** utility, see *Teamcenter Utilities* in the Teamcenter documentation.

> Note:
>
> You must run this utility whenever you create a new project to keep the data synchronized.

15. By default, inaccessible assembly components are displayed with **<<UNREADABLE>>**. To prevent the display of **<<UNREADABLE>>** in an assembly, set the **BOM_hide_unreadable_lines** preference to **All** in the OEM Supplier Site.

16. To use subtypes of Supplier Connect objects, you must configure the following preferences with the names of the subtype objects:

    - **SUPPORTAL_Usp0OEMDeXChange_type_name**
    - **SUPPORTAL_Usp0SupDeXChange_type_name**

17. If you are working with multiple OEM Sponsor Sites, do the following additional configurations:

    a. Specify the multiple OEM Sponsor Site names in the **SUPPORTAL_share_site_names** preference.

b. Ensure that the encryption keys are the same on all the sites.

8. Set up the vendors and their suppliers

After you complete installing and configuring Supplier Connect, you must create the vendors and assign their suppliers (company contacts) in the OEM Sponsor Site. Vendors are any companies that are external to the OEM company. They can be another vendor, a supplier, or a joint venture partner. Suppliers are employees of the companies, and are represented by **Company Contacts** in Teamcenter.

You also assign a Teamcenter user account to each of the vendor's suppliers. After you do this, share the OEM design engineer user accounts and the Teamcenter user accounts assigned to suppliers with the OEM Supplier Site. You can share these accounts at one time in a batch or share them individually when you create them. This allows the suppliers to log on to their OEM Supplier Site with the assigned Teamcenter user accounts. Additionally, when an OEM design engineer shares a data exchange package to the OEM Supplier Site, the package owner is correctly indicated in the OEM Supplier Site.

Prerequisites

Supplier Connect must be installed and configured on the OEM Sponsor Site and the OEM Supplier Site.

Procedure

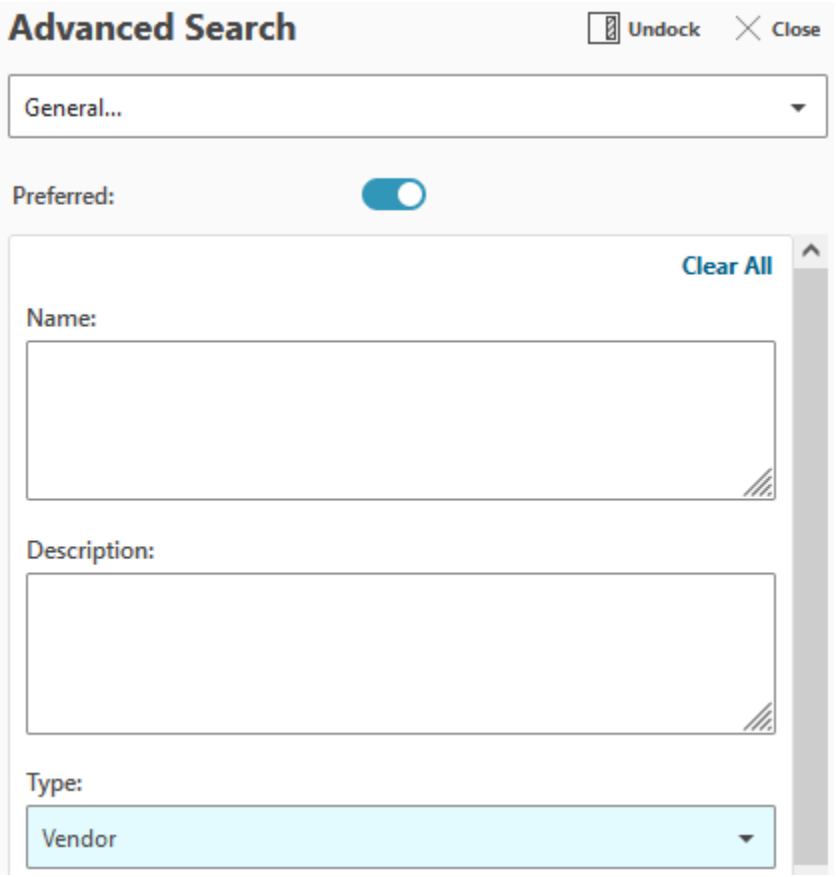
1. In the OEM Sponsor Site, create the vendors and their suppliers as follows:

    a. Create a vendor.

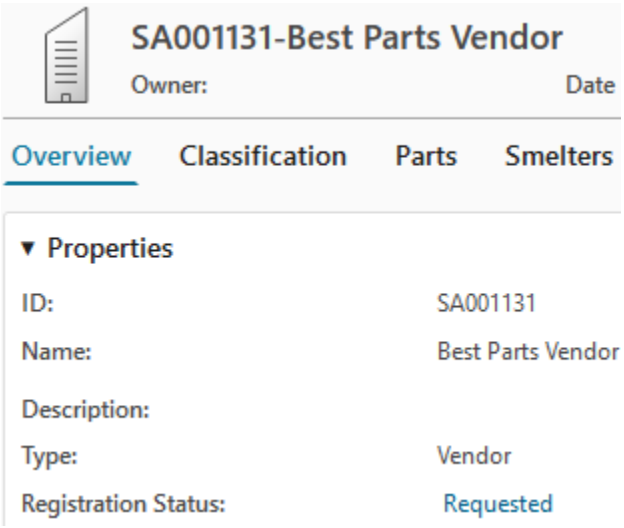
    For more information, see *Vendor Management on Active Workspace — Usage* in the Teamcenter documentation.

    b. For each vendor, ensure that the **Registration Status** of the vendor is **Approved**. Do the following:

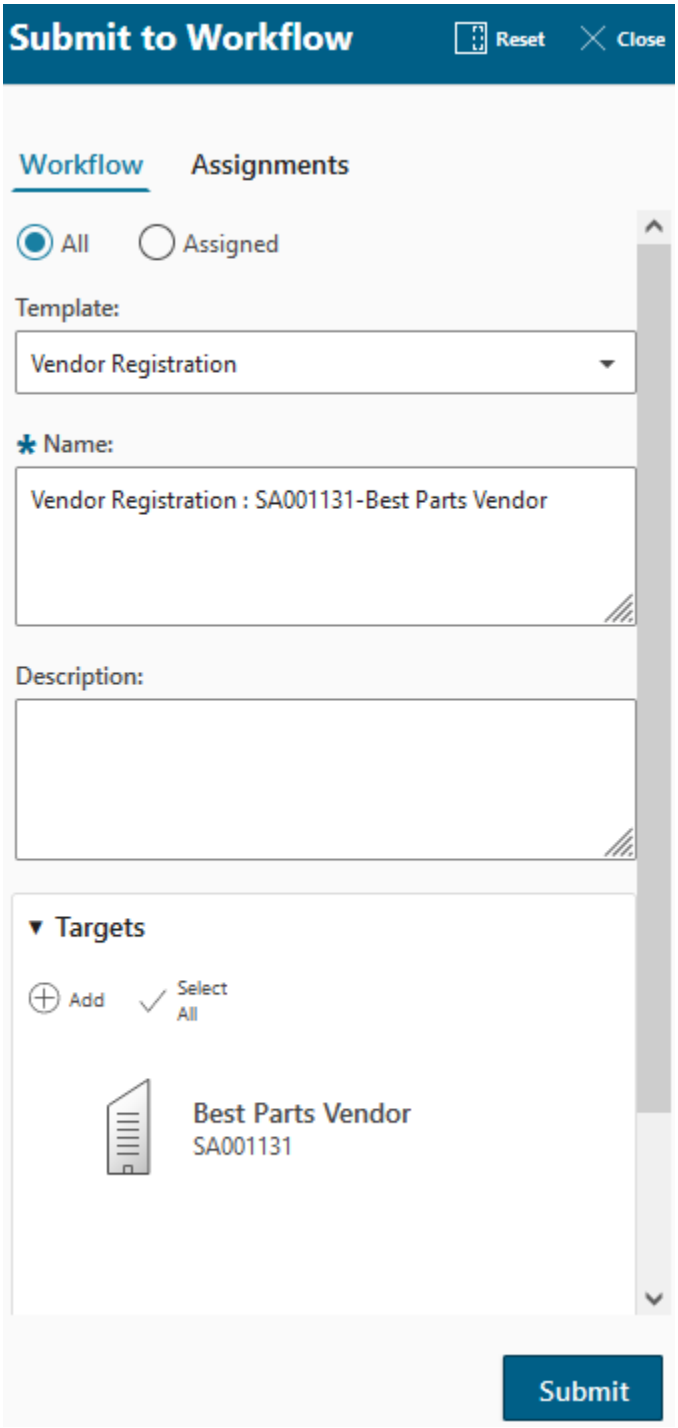
        A. In **Advanced Search**, select **General**, select **Vendor** as the type of search, and click **Search**.



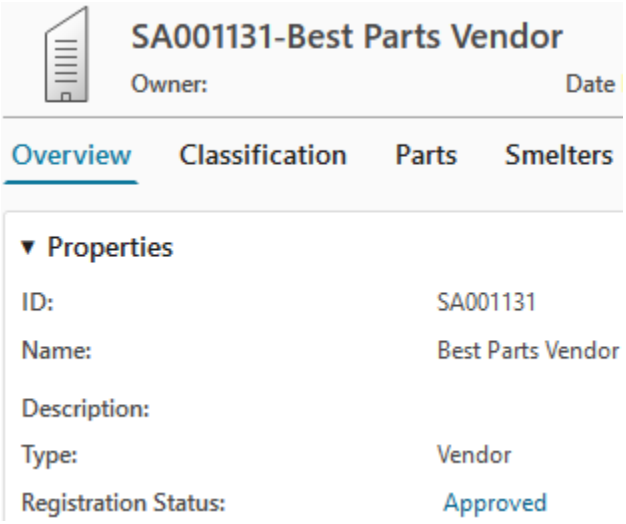
B. In the search results, select a vendor whose **Registration Status** is **Requested**, and choose **More commands** ••• > **Manage** > **Submit to Workflow**.



C. From the **Template** list, ensure that **Vendor Registration** is selected, and click **Submit**.



The vendor's **Registration Status** is updated to **Approved**.



c. For each vendor, assign a supplier, represented by **Company Contacts** in Teamcenter.

For more information, see *Vendor Management on Active Workspace — Usage* in the Teamcenter documentation.

Note:

- When you create the suppliers for a vendor, you must share the Teamcenter URL and logon credentials with the suppliers for them to access their Teamcenter site and work on their assigned tasks.
- For **Teamcenter Briefcase** data exchange packages, to search for relevant suppliers, ensure the following:
  - Suppliers must have a managed site associated with their **Vendor**.
  - The partner user assigned to the supplier is active.
- For **Briefcase** data exchange packages, to search for relevant suppliers, ensure the following:
  - Suppliers must have an unmanaged site associated with them.
  - The partner user assigned to the supplier is active.
  - The **Briefcase Browser Participant Level** property set to one of the following values:

- **NX** to assign a Briefcase Browser license and a Briefcase Browser plugin for NX license to the supplier.

  Suppliers require this license to download any Briefcase associated with the data exchange package, review the contents of the Briefcase, modify part designs in Briefcase Browser by using NX, and upload a new Briefcase with updated designs.

- **CATIA** to assign a Briefcase Browser license and a Briefcase Browser plugin for CATIA license to the supplier.

  Suppliers require this license to download any Briefcase associated with the data exchange package, review the contents of the Briefcase, modify part designs in Briefcase Browser by using CATIA, and upload a new Briefcase with updated designs.

d. Assign a Teamcenter user account to a supplier as follows:

   A. In the **Company Contacts** section, select the supplier to provide access.

   B. Choose **More commands** ••• > **Manage** > **Add Partner User**.

   C. In the **Add Partner User** panel, search for and select the required Teamcenter user account.

   > Caution:
   >
   > You can assign a Teamcenter user account to only one supplier at a time.

   D. Click **Add**.

> Note:
>
> If you cannot see the supplier before assigning a Teamcenter user account, you must activate the supplier.
>
> For more information, see *Partner Connect — Usage* in the Teamcenter documentation.

2. To share OEM design engineer user accounts and Teamcenter user accounts assigned to suppliers, do the following:

   a. In the OEM Sponsor Site, share the OEM design engineer user accounts and the Teamcenter user accounts assigned to suppliers with the OEM Supplier Site by using the **admin_data_export** utility. For more information about using the **admin_data_export** utility, see *Teamcenter Utilities* in the Teamcenter documentation.

   You must copy the generated ZIP file to the OEM Supplier Site. The location of this file is the path you specified in the **-outputPackage** argument.

> Note:
>
> You must run this utility whenever you create a new design engineer user account or Teamcenter user account assigned to a supplier.

b. In the OEM Supplier Site, import the OEM design engineer user accounts and the Teamcenter user accounts assigned to suppliers by using the **admin_data_import** utility. For more information about using the **admin_data_import** utility, see *Teamcenter Utilities* in the Teamcenter documentation.

> Note:
>
> You must run this utility whenever you create a new design engineer user account or Teamcenter user account assigned to a supplier.

3. To share additional individual OEM design engineer user accounts and Teamcenter user accounts assigned to suppliers, do the following:

a. In the OEM Sponsor Site and the OEM Supplier Site, configure the following preferences to exchange system administration data and organization data:

- Add the OEM Sponsor Site and the OEM Supplier Site to the **IDSM_dsa_sites_permitted_to_push_admin_data** preference to define the remote sites that are permitted to distribute system administration data to a local site.

  If you are working with multiple OEM Sponsor Sites, specify the multiple OEM Sponsor Site names as a comma-separated list in this preference, and update the preference on all the OEM Sponsor Sites.

- Add the OEM Sponsor Site and the OEM Supplier Site to the **IDSM_global_dsa_sites_permitted_to_push_admin_data** preference to define the remote sites that are permitted to use Multi-Site export to push organization data to a local site.

  If you are working with multiple OEM Sponsor Sites, specify the multiple OEM Sponsor Site names as a comma-separated list in this preference, and update the preference on all the OEM Sponsor Sites.

b. In the OEM Sponsor Site, log on to the rich client as a user with Teamcenter administration privileges.

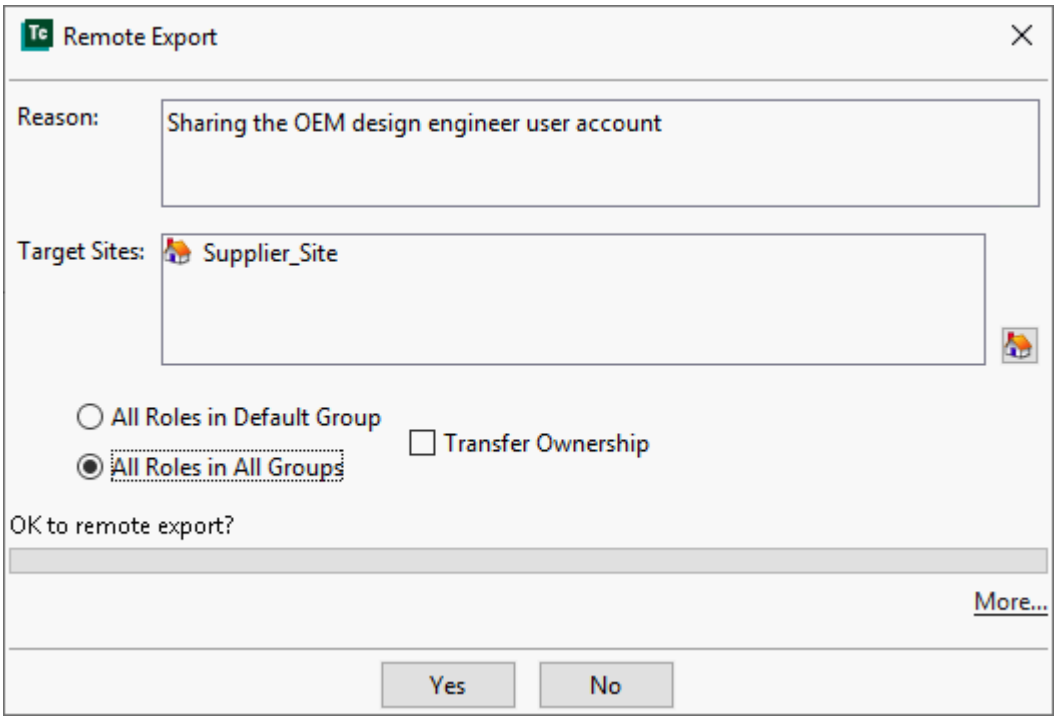
c. In the Organization application of Teamcenter, create the OEM design engineer user account or Teamcenter user account assigned to a supplier.

When you create the OEM design engineer user account, add the account to the **Engineering** group, and assign the **Designer** role to the account. When you create the Teamcenter user account for a supplier, you must add it to a group with its security set to **External**.

d. In the **Organization List** tree present in the lower-left pane, select the user account, and choose **Tools→Export→Remote Export**.

e. Click next to the **Target Sites** box, and select the target OEM Supplier Site.

f. Select **All Roles in All Groups** to export all group member roles associated with the user, and click **Yes**.



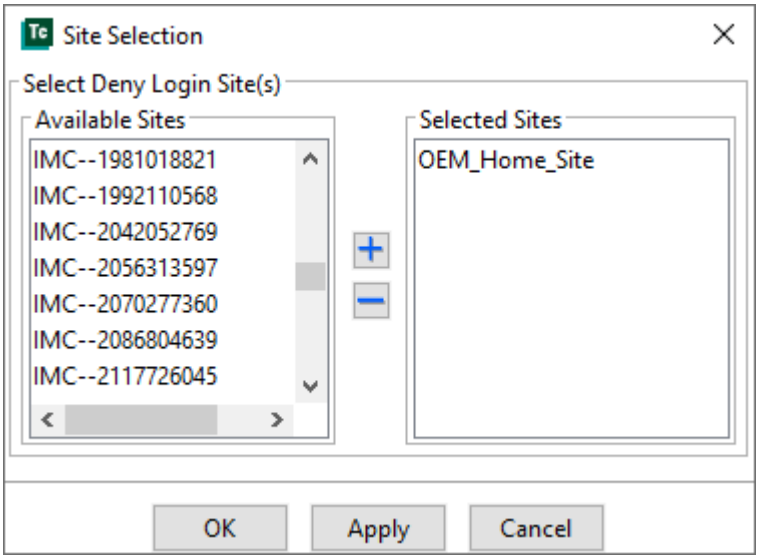
4. After you share the Teamcenter user account assigned to a supplier, the account is replicated at the OEM Supplier Site. Now, you must prevent this account from accessing the OEM Sponsor Site as follows:

a. In the OEM Sponsor Site, log on to the rich client as a user with Teamcenter administration privileges.

b. In the lower-left pane of the Organization application, select the Teamcenter user account assigned to a supplier.

c. Click **Select Sites** next to the **Deny Login At Sites** box.

d. In the **Site Selection** dialog box, add the OEM Sponsor Site to the **Selected Sites** column.



e. In the confirmation message, click **Yes**, and click **OK** to close the **Site Selection** dialog box.

5. Ensure that you assign Author and Consumer licenses to the suppliers as required.

   The following table describes the licenses required for certain tasks:

Consumer	Author
Submit a response.	Modify the properties of an item or item revision, such as its name or description.
Add an attachment and submit a response.	Add a child item to an assembly.
	Create a Self Service request for access to OEM data.
	Replace an attachment in a data exchange package.

6. If you are working with multiple OEM Sponsor Sites, do the following additional configurations:

   a. In the OEM Supplier Site and the multiple OEM Sponsor Sites, configure the following preferences to exchange system administration data and organization data:

      - Specify the OEM Supplier Site and the multiple OEM Sponsor Site names as a comma-separated list in the **IDSM_dsa_sites_permitted_to_push_admin_data** preference, and update the preference on all the OEM Sponsor Sites.

        This defines the remote sites that are permitted to distribute system administration data to a local site.

- Specify the OEM Supplier Site and the multiple OEM Sponsor Site names as a comma-separated list in the **IDSM_global_dsa_sites_permitted_to_push_admin_data** preference, and update the preference on all the OEM Sponsor Sites.

  This defines the remote sites that are permitted to use Multi-Site export to push organization data to a local site.

b. To ensure that the design engineers on all OEM Sponsor Sites exchange data with the same group of suppliers, do the following:

   A. In all OEM Sponsor Sites, create the Teamcenter user accounts to be assigned to suppliers.

      These Teamcenter user accounts must be same as the Teamcenter user accounts you imported into the OEM Supplier Site by using the **admin_data_import** utility.

   B. In all OEM Sponsor Sites, create the managed sites to be assigned to the vendors if their suppliers are working in their own Teamcenter environments.

      After you import the vendors in the OEM Supplier Site, you must assign these managed sites to the respective vendors.

   C. For each of the OEM Sponsor Sites, ensure that the suppliers **install an instance of Briefcase Browser** and update *CustomMappings.xml* with the values of **oem_name** and **site_id** for the respective OEMs.

      When a supplier receives a Briefcase from an OEM Sponsor Site, the supplier must open the Briefcase and work on it in the Briefcase Browser instance for the same OEM Sponsor Site.

   D. In any of the OEM Sponsor Sites, create the vendors and their suppliers.

      For more information, see *Vendor Management on Active Workspace — Usage* in the Teamcenter documentation.

   E. In the same OEM Sponsor Site, export the vendors and their suppliers to a Briefcase.

   F. Transfer the exported Briefcase file to the next OEM Sponsor Site.

   G. In the next OEM Sponsor Site, import the vendors and their suppliers from the Briefcase file.

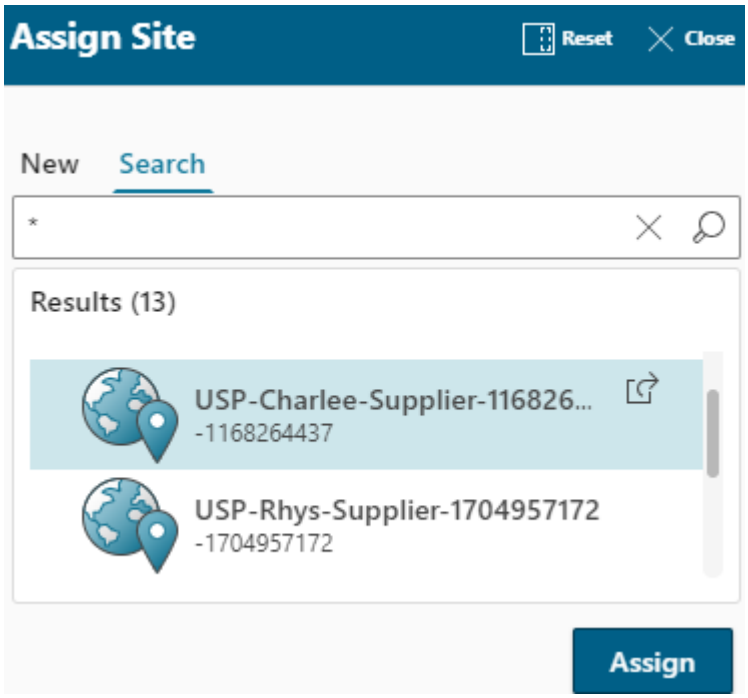
   H. To assign managed sites to the respective vendors in the next OEM Sponsor Site, do the following:

      i. Navigate to and open the folder where you have created the vendor, for example, your **Newstuff** folder.

ii. Select and open the vendor.

iii. Choose **More commands** ••• > **Manage** > **Assign Site** ⊕.

iv. Click the **Search** tab, specify the filter criteria, and select the required managed site.



v. Click **Assign**.

9. Migrate Supplier Collaboration Foundation users and data to Supplier Connect

If you have existing Supplier Collaboration Foundation users that you want to migrate to Supplier Connect, you must first extract the existing user accounts and then create these for the OEM Supplier Site. After migrating the users, you can migrate the associated Design Data Exchange packages to Supplier Connect. To do this, you must first convert the data to the Supplier Connect data model and then share the data with the OEM Supplier Site.

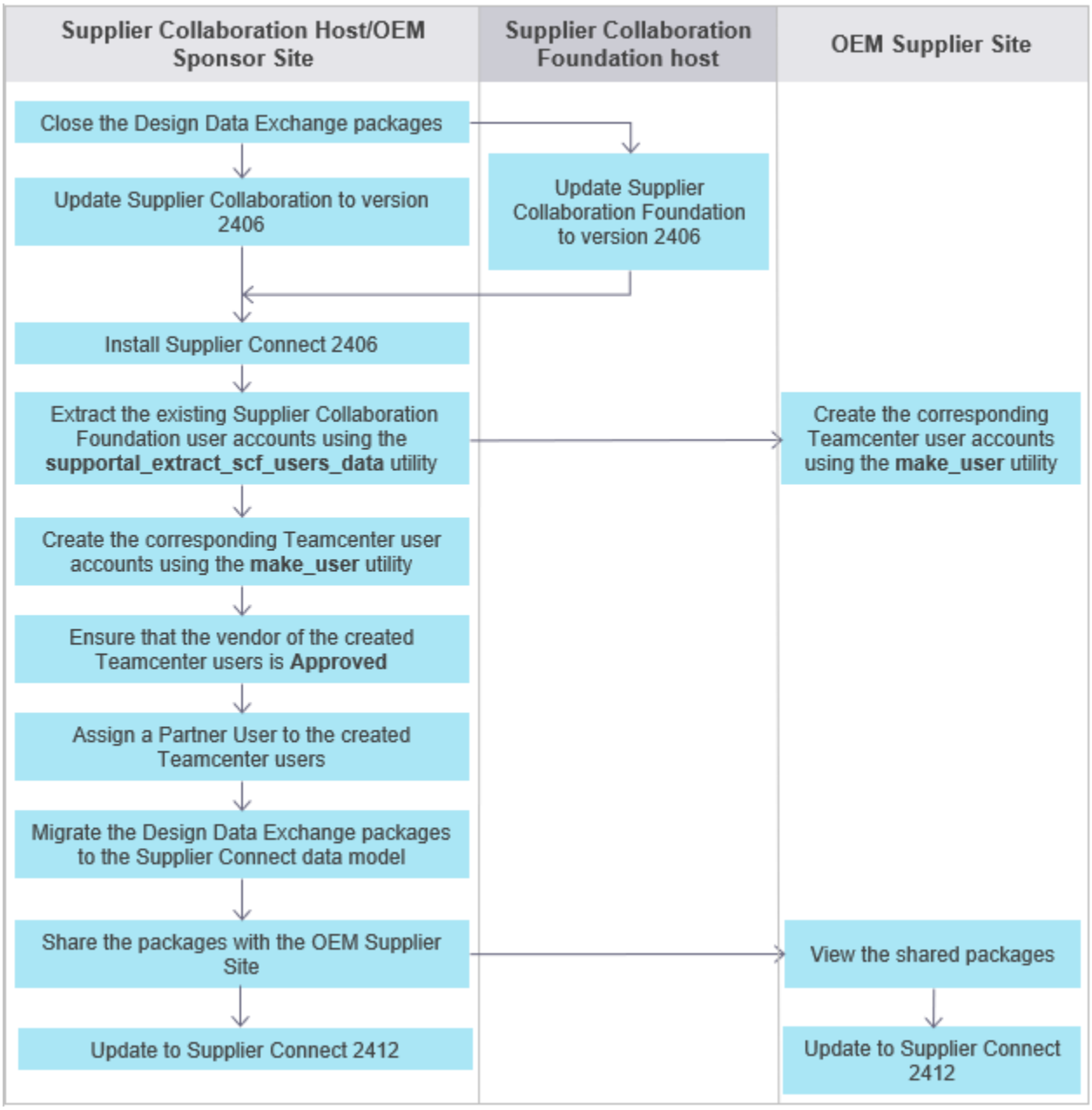
Caution:

- After you migrate Supplier Collaboration Foundation users to Supplier Connect, Siemens Digital Industries Software recommends that you no longer use Supplier Collaboration Foundation to work with suppliers because further migration of data will not be supported.
- You can migrate only those Design Data Exchange packages that are in the **Closed** state.

Note:

For migrated events, you can define the number of years after which an event is automatically closed. To do this, specify **0** or less than **0** in the **SUPPORTAL_migrated_close_date_offset_years** preference to immediately close the migrated events. The default value is **8** years.

The following graphic shows the sequence of tasks required to migrate Supplier Collaboration Foundation users and data to Supplier Connect:



Prerequisites

- Close the Supplier Collaboration Design Data Exchange packages, and ensure that the packages are in the **Closed** state.
- Update Supplier Collaboration and Supplier Collaboration Foundation to version 2406.
- **Install Supplier Connect 2406 on the Teamcenter environment where you have installed Supplier Collaboration**. This environment becomes the OEM Sponsor Site.
- **Install Supplier Connect 2406 on the OEM Supplier Site**.

- Configure **the OEM Sponsor Site** and **the OEM Supplier Site** to connect with each other. When you complete the required configurations, the OEM and suppliers can exchange data successfully.

- Ensure that you can establish a connection with the Supplier Collaboration Foundation database before you run the **supportal_extract_scf_users_data** utility.

  For an **Oracle** database, you can test the connection by running the following command in the command prompt:

  ```
  sqlplus "<database user name>/<database
  user password>@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
  (HOST=<database host name>)(PORT=<database port number>)))
  (CONNECT_DATA=(SERVICE_NAME=<System Identifier of the Supplier Collaboration
  Foundation database>)))"
  ```

  For a **PostgreSQL** database, you can test the connection by running the following command in the command prompt:

  ```
  psql -h <database host name> -p <database port number> -u <database user name>
  -d <Supplier Collaboration Foundation database name>
  ```

Procedure

1. To migrate Supplier Collaboration Foundation users to Supplier Connect, do the following:

   a. In the OEM Sponsor Site, to extract the existing Supplier Collaboration Foundation users, from *<TC_ROOT>\ bin\usp0supportal*, run the **supportal_extract_scf_users_data** utility with the following arguments:

      supportal_extract_scf_users_data [**-u=***user-id of the Supplier Collaboration Foundation database user*] [**-p=***password of the Supplier Collaboration Foundation database user*] [**-host=***name of the computer where the Supplier Collaboration Foundation database is installed*] [**-port=***port number of the Supplier Collaboration Foundation database server*] [**-sid=***System Identifier name assigned when the Supplier Collaboration Foundation database was created*][**-db=***type of the Supplier Collaboration Foundation database ('O' for Oracle database and 'P' for PostgreSQL database)*]

      -u

      Specifies the user ID of the Supplier Collaboration Foundation database user.

      -p

      Specifies the password of the Supplier Collaboration Foundation database user.

      -host

      Specifies the name of the computer where the Supplier Collaboration Foundation database is installed.

-port

Specifies the port number of the Supplier Collaboration Foundation database server.

-sid

Specifies the **System Identifier** name assigned when the Supplier Collaboration Foundation database was created.

-db

Specifies the type of the Supplier Collaboration Foundation database (*O* for the Oracle database and *P* for the PostgreSQL database).

-h

Displays the help for this utility.

This utility generates these two files in the *usp0supportal* folder of the Teamcenter data directory (*TC_DATA*):

- *scfUsers.csv*: This file contains the details of the Supplier Collaboration Foundation users, such as the name and user ID.
- *scfusersvscontacts.csv*: This file contains the details of the Supplier Collaboration Foundation user's relation with the Teamcenter vendor and its assigned Teamcenter user account.

b. In the OEM Sponsor Site and OEM Supplier Site, to create the corresponding Teamcenter users for the extracted Supplier Collaboration Foundation users, run the **make_user** utility with the following arguments:

make_user [**-u=***user-id*] [**-p=***password*] [**-file=***scfUsers.csv file that contains the details of the extracted Supplier Collaboration Foundation users*]

-u

Specifies the user ID.

This is generally a user with administration privileges.

-p

Specifies the password.

-file

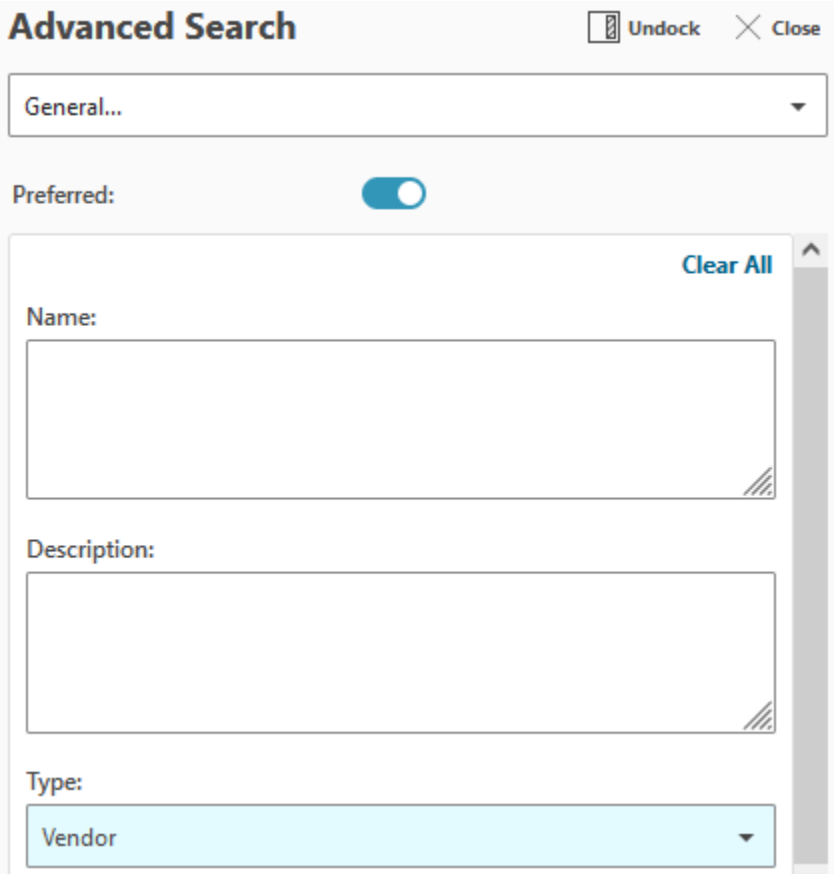
Specifies the *scfUsers.csv* file that contains the details of the extracted Supplier Collaboration Foundation users.

-h

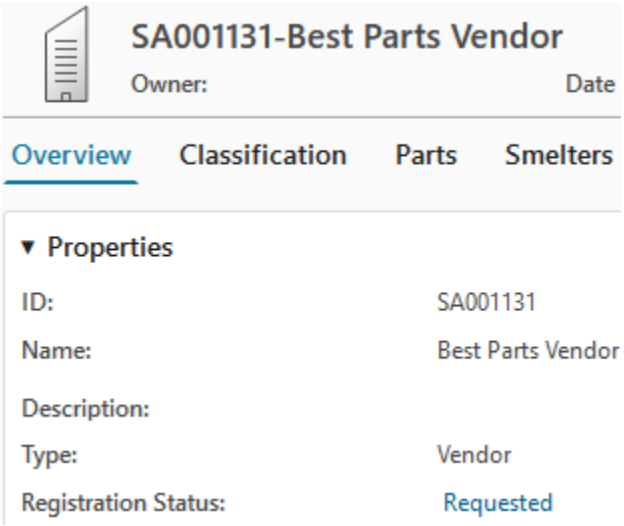
Displays the help for this utility.

c. For each vendor of the Teamcenter user accounts assigned to suppliers, search for the vendor, and ensure that the **Registration Status** of the vendor is **Approved**. Do the following:

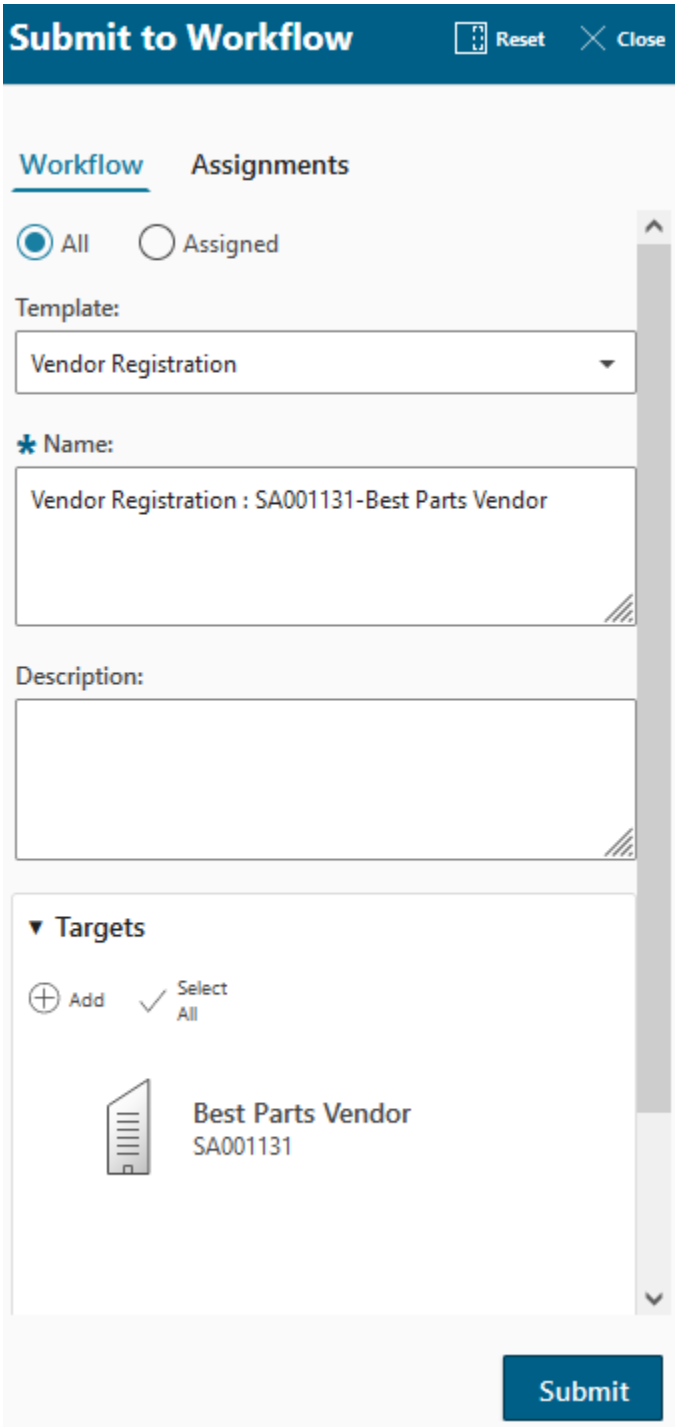
A. In **Advanced Search**, select **General**, select **Vendor** as the type of search, and click **Search**.



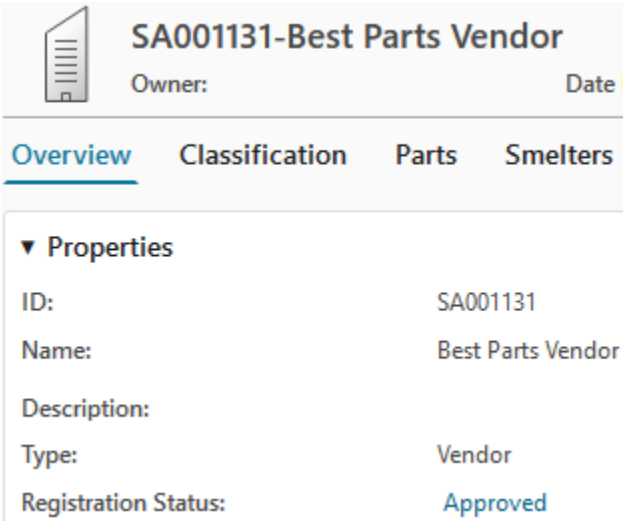
B. In the search results, select a vendor whose **Registration Status** is **Requested**, and choose **More commands** ••• > **Manage** > **Submit to Workflow**.



C. From the **Template** list, ensure that **Vendor Registration** is selected, and click **Submit**.

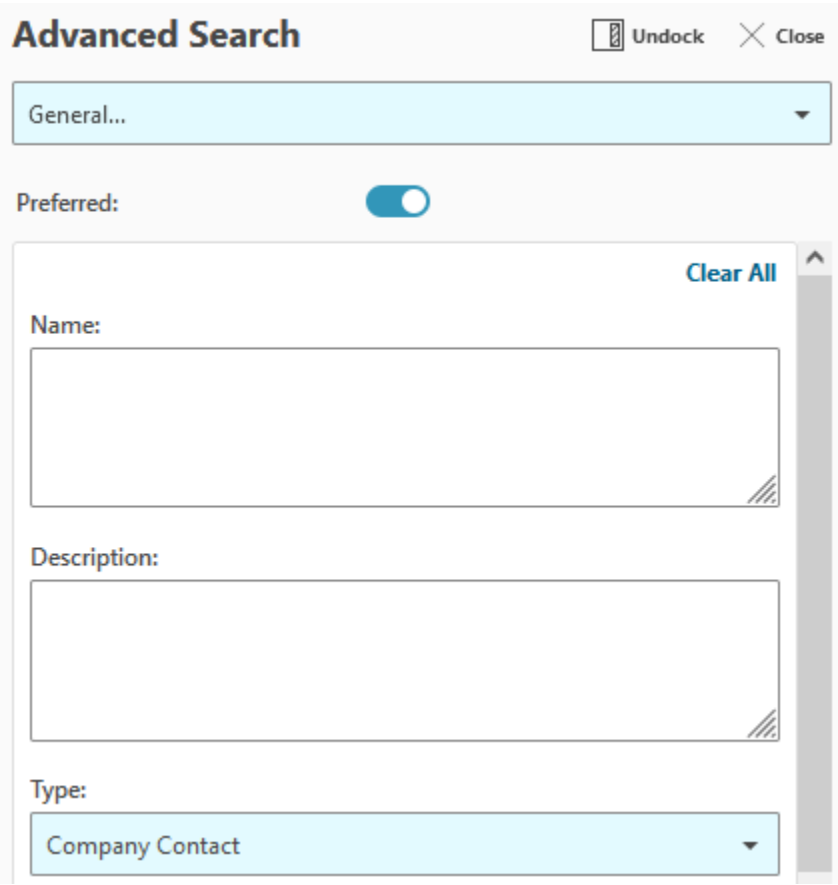


The vendor's **Registration Status** is updated to **Approved**.



d. For each Teamcenter user account assigned to a supplier, search for the corresponding **Company Contact**, and assign a Partner User as follows:

   A. In **Advanced Search**, select **General**, select **Company Contact** as the type of search, and click **Search**.



B. In the search results, select a Teamcenter user account assigned to a supplier, and choose **More commands** ••• > **Manage** > **Add Partner User**.

C. In the **Add Partner User** panel, search for and select the required Teamcenter user account.

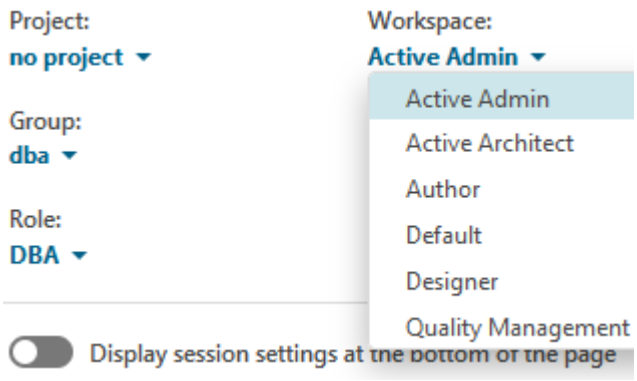
> Caution:
>
> You can assign a Teamcenter user account to only one partner representative at a time. You must be logged on as a user with Teamcenter administration privileges to assign partner users.

D. Click **Add Partner User**.

2. To migrate and share Design Data Exchange packages with Supplier Connect, do the following:

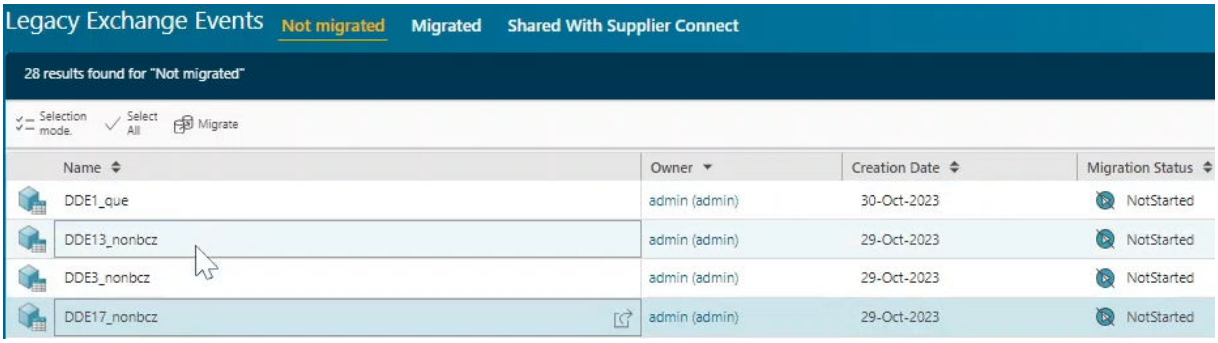
a. Go to the OEM Sponsor Site, and log on to the web client as a user with Teamcenter administration privileges.

Ensure that you are working in the **Active Admin** workspace.



b. Click the **MIGRATE LEGACY EXCHANGE EVENTS** tile.

c. In the **Not Migrated** tab, select the Design Data Exchange packages to be migrated to Supplier Connect, and click **Migrate**.

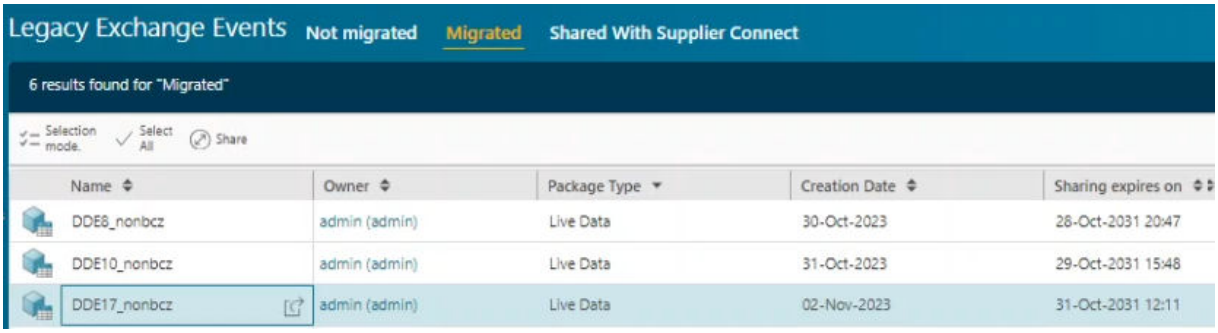


This migrates the Design Data Exchange packages to the Supplier Connect data model, and their status is updated to **MigratedNotShared**. The Design Data Exchange packages are moved from the **Not Migrated** tab to the **Migrated** tab. In this tab, you can view all packages that have been migrated to the Supplier Connect data model in the OEM Sponsor Site.

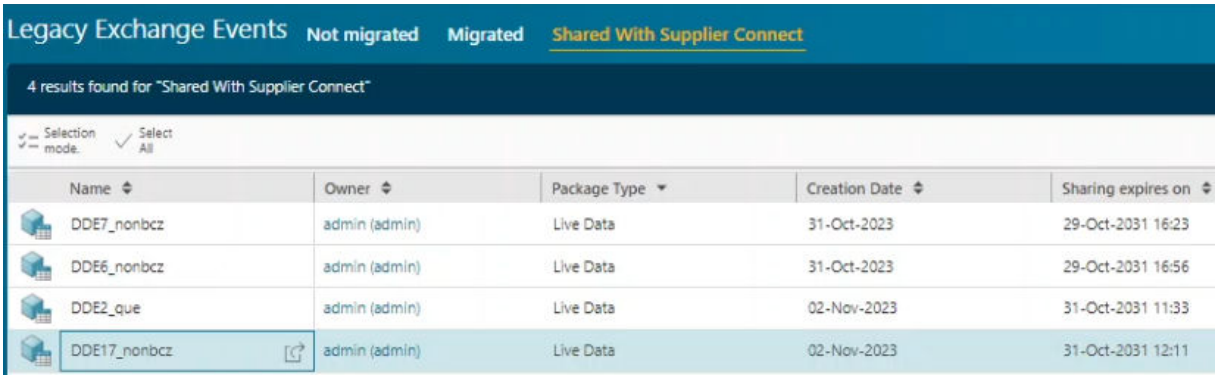
If you open the package from the **Migrated** tab, you can view the package details, such as:

- Item or assembly shared with suppliers
- Assigned suppliers
- Item or assembly updates made in Supplier Collaboration Foundation by the assigned suppliers
- Sponsor attachments and attachments added in Supplier Collaboration Foundation by the assigned suppliers
- Tracking report

d. To share the Design Data Exchange packages with the OEM Supplier Site, click the **Migrated** tab, select the required packages, and click **Share**.



The packages are shared with the OEM Supplier Site, and their status is updated to **MigratedShared**. The packages move from the **Migrated** tab to the **Shared with Supplier Connect** tab. In this tab, you can view all packages that have been shared with the OEM Supplier Site.



e. For a supplier to view the package in the OEM Supplier Site, do the following:

   A. The supplier must log on to the OEM Supplier Site.

   B. In **Advanced Search**, select **Data Exchange**, select **Migrated** from the **Exchange Status** list, and click **Search**.

   C. In the search results, select and open a package to view the package details, such as item or assembly shared with the logged-on supplier, item or assembly updates made in Supplier Collaboration Foundation by the logged-on supplier, and **Questionnaire** from Supplier Collaboration Foundation.

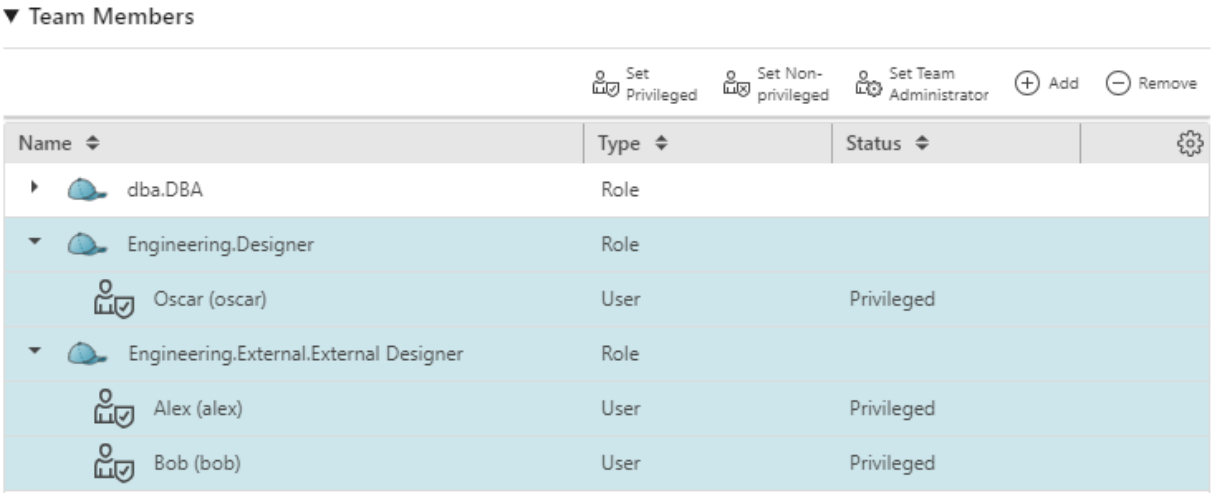
3. Update to Supplier Connect 2412 on **the OEM Sponsor Site** and **the OEM Supplier Site**.

10. Configure Supplier Connect to make an assembly available to all suppliers in the project

Implementing project security in your Teamcenter environment ensures that only project members can access the assemblies associated with the project. Design engineers can publish the assembly and make it available to all suppliers in the project simultaneously using **Publish to Suppliers** in the OEM Sponsor Site. To configure Supplier Connect for this, set up the necessary projects and assign design engineers, Teamcenter user accounts for the suppliers, and the suppliers to the same project. When design engineers publish the assembly, each supplier in the project can search for and work on it in their OEM Supplier Site.

Procedure

1. Log on to the web client as a user with Teamcenter administration privileges.
2. On the home page, click the **PROJECTS** tile.
3. Create a project.
4. To assign Teamcenter user accounts for the suppliers and design engineers to the project, do the following:
    a. In the **Team Members** section of the project, click **Add** ⊕.
    b. Search and filter to find the groups, roles, or users you want to add to the project.
    c. In **Results**, select the groups, roles, and users you want to add to the project.
    d. Click **Add**.
    e. Select the groups, roles, and users that you added to the project and click **Set Privileged**.



This allows users to view objects and add or remove objects.

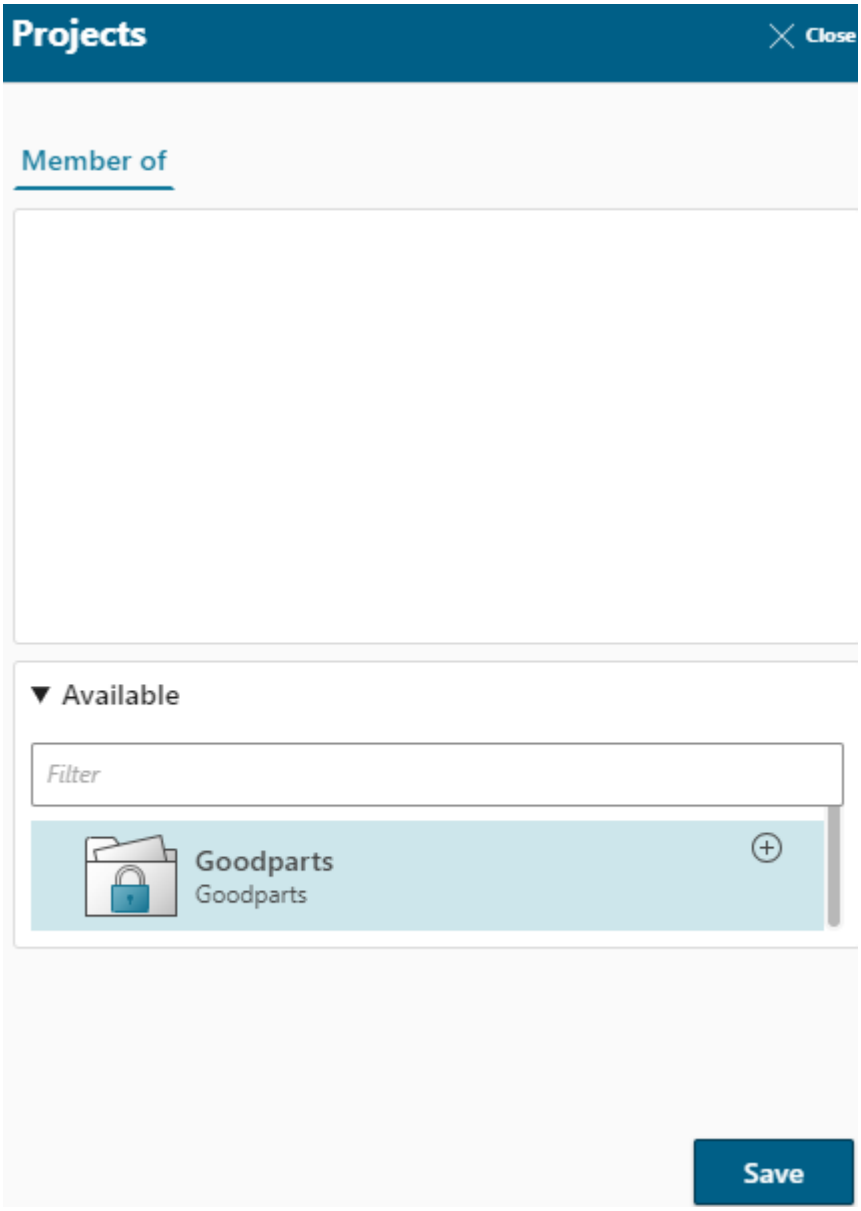
5. To assign suppliers to the project, do the following:

   a. On the home page, click **Advanced Search** from the **Search** box or from the **ADVANCED SEARCH** tile.

   b. In **Advanced Search**, select **General**, select **Company Contact** as the type of search, and click **Search**.

   c. In the search results, select the required suppliers, and choose **More commands** ••• > **Manage** > **Projects**.

   d. Select a project from the **Available** list and click **Add Project** ⊕ to move the project to the **Member of** project list.



e. Click **Save**.

6. Export the project to the OEM Supplier Site by using the **admin_data_export** utility. For more information about using the **admin_data_export** utility, see *Teamcenter Utilities* in the Teamcenter documentation.

   Copy the generated ZIP file to the OEM Supplier Site. The location of this file is specified in the **-outputPackage** argument.

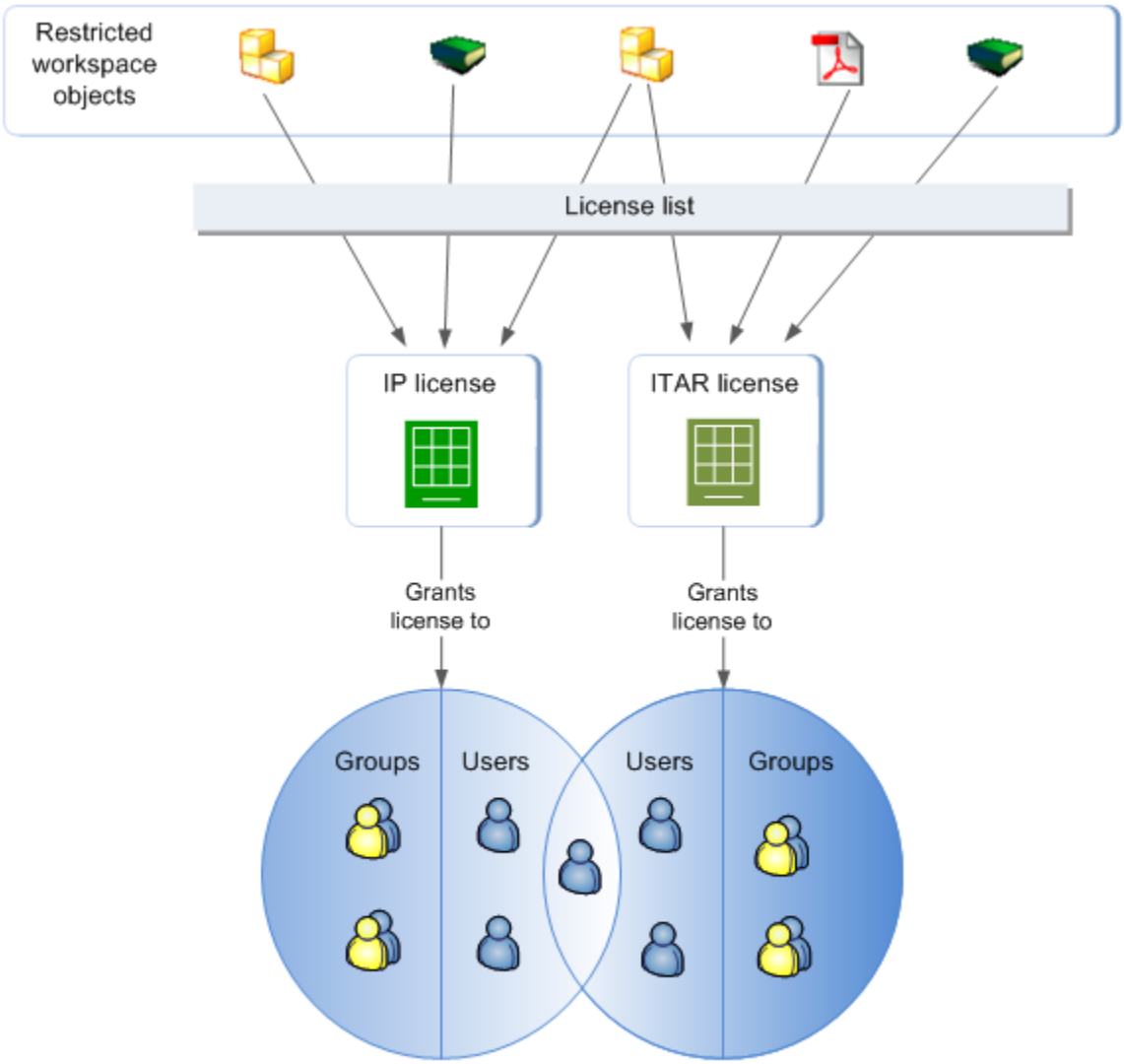
   > Note:
   >
   > You must run this utility whenever you create a new project to keep the data synchronized.

7. In the OEM Supplier Site, import the project by using the **admin_data_import** utility. For more information about using the **admin_data_import** utility, see *Teamcenter Utilities* in the Teamcenter documentation.

11. Configuring Supplier Connect to implement the access controls defined by ADA licenses

What is ADA License?

ADA License provides support to enforce the International Traffic in Arms Regulations (ITAR) and intellectual property (IP) policies using authorized data access (ADA) licenses. ADA licenses provide discretionary (time-limited) grants or denials of access to users who do not have access to classified data based on their clearance level. ITAR licenses are the authorizing documents in Teamcenter that represent an effective Technical Assistance Agreement (TAA). The third license type, exclude license, is a mechanism for denying users access to data for a specific period of time.



ADA functionality provides the ability to:

- Classify data per ITAR or IP policies.
- Specify IP or government clearance levels for users.
- Attach or detach ADA licenses to and from workspace objects.
- Control access to classified data through Access Manager conditions and rules.
- Create and maintain audit records for actions performed on ITAR or IP licenses.

ADA licenses can be managed by non-database administrators. In addition, you can define users whose role is only to classify workspace objects.

Types of Authorized Data Access (ADA) licenses

ADA License has three types of licenses that provide limited access or exclusion:

- **IP_License** 

  Grants discretionary access to specific users or groups to workspace objects that have intellectual property (IP) classification. It grants the access for a specified period of time.

- **ITAR_License** 

  Grants discretionary access to specific users or groups to workspace objects with International Traffic in Arms Regulations (ITAR) classifications for a specified period of time. Typically it is used to grant access for a specific time period to citizens of other countries, United States (U.S.) citizens physically located outside the U.S., or organizations that are named in an effective Technical Assistance Agreement (TAA) through an ITAR license.

  ITAR licenses are used to control access to data that is deemed military in nature. For example, technical information may be subject to ITAR policies and, if so, must be protected so that only citizens of the U.S. have open access to the data. Viewing this classified data outside the U.S. is considered equivalent to performing an ADA export of it, which requires that rights are granted by license. Information marked as non-technical is, for the purposes of ITAR, available to all users.

  The provisions for granting limited access to foreign nationals involve a Technical Assistance Agreement (TAA). These agreements are written for a specific entity or country, cover different types of information, and expire on different dates. Teamcenter-controlled information that is not technical is made available to all authorized U.S. citizens and users from foreign countries.

- **Exclude_License**

  Denies specific users or groups access to the attached workspace objects for a period of time.

Workspace objects that are under license control cannot be viewed by users who do not have specific user or group attribute values, such as:

- Nationality
- Geography
- Training
- IP or government clearance

Access based on these attributes is controlled through Access Manager (AM) rules, access control lists (ACLs), and accessors. Licenses can also be locked and you can set dates on which they will expire.

Overview of implementing the access controls defined by ADA licenses

ADA License is a Teamcenter security application for authorized data access (ADA) that complements other Teamcenter security features, such as Access Manager rules and access control lists (ACLs). This application controls sensitive data by data classification, user clearance, and authorizing documents. When users or groups attempt to access classified data in Teamcenter, their clearance level is evaluated against the classification of the object based on Access Manager rules. If the user or group clearance level is equal to or greater than the classification on the object, access is granted.

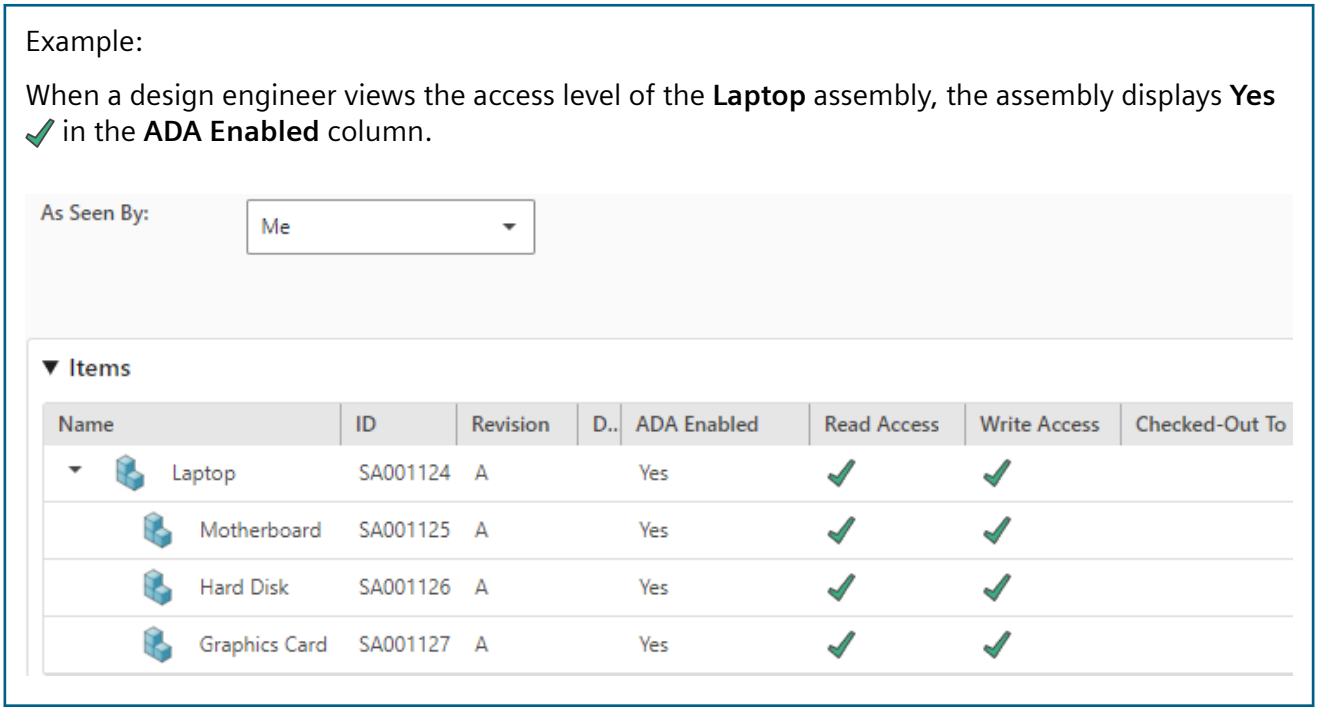
ADA License has three types of licenses that provide limited access or exclusion:

- **IP_License**
- **ITAR_License**
- **Exclude_License**

When a design engineer creates a data exchange package for an item or assembly with an ADA license, the **ADA Enabled** column displays **Yes** ✓ for the item or assembly in the **Structure** tab of the data exchange package.

Example:

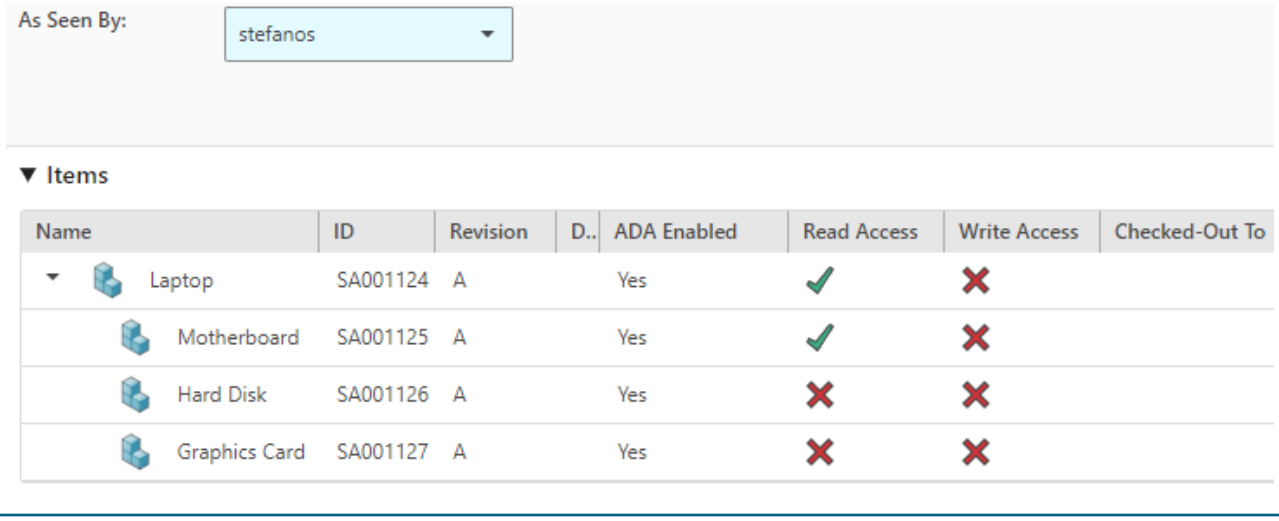
When a design engineer views the access level of the **Laptop** assembly, the assembly displays **Yes** ✓ in the **ADA Enabled** column.



When a design engineer wants to assign a supplier to this assembly, the design engineer can view the supplier's access to the assembly components in this column. The design engineer can then assign modification rights accordingly.

Example:

For the **Laptop** assembly, the supplier **stefanos** has access to only **Laptop** and **Motherboard**. Therefore, the assembly displays **Yes** ✓ in the **ADA Enabled** column for these components.



When the design engineer searches for a supplier, Supplier Connect evaluates the ADA licenses assigned to the assembly and the supplier. If a supplier matches the access level defined in the license, the supplier appears in the search results.

Note:

If the root of the assembly has a matching ADA license (**ADA Enabled** column displays **Yes**), then Supplier Connect displays only the suppliers with ADA licenses in the search results.

If a supplier does not have access to the selected item or assembly, ✗ appears next to the selected item or assembly. When a supplier views the data exchange package in their Teamcenter, the supplier can view only the accessible components of an assembly.

Configure Supplier Connect to implement the access controls defined by ADA licenses

To implement the access controls defined by authorized data access (ADA) licenses, you must create the ADA licenses in the ADA License Teamcenter security application, assign the required clearance level to design engineers and suppliers for the licenses, ensure that Supplier Connect allows access only to suppliers who have the required access level to items or assemblies, and create the required access control lists (ACLs) in Teamcenter Access Manager.

Note:

You must configure the ADA licenses and ACLs and set the required preferences for both the OEM Sponsor Site and the OEM Supplier Site.

Procedure

1. Create the ADA licenses and assign design engineers, IDSM administrators, and suppliers to them:

    a. Log on to the rich client as a user with an ADA administrator role (intellectual property (IP) Admin or International Traffic in Arms Regulations (ITAR) Admin).

    b. Start **ADA License** and select the **ADA Licenses** node (top node) in the left pane.

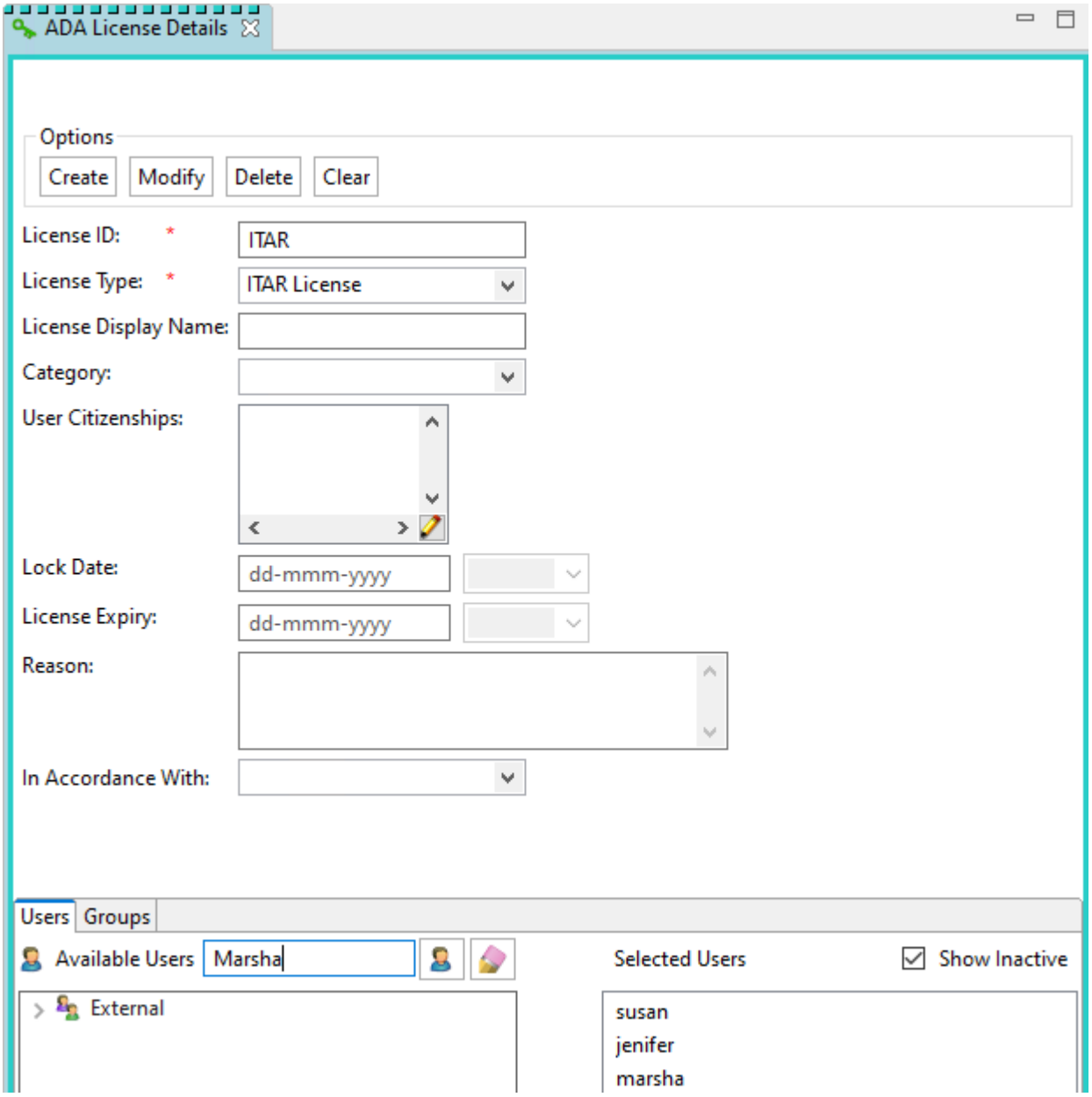
    c. Type a name for the license in the **License ID** box, for example, **ITAR**.

    d. Select the type of license from the **License Type** list, for example, **ITAR_License**.

    e. Select the design engineers and suppliers who are allowed to access objects with the license attached.

    - To allow access to specific users, click the **Users** tab, select the user name in the **Available Users** list, and click (>) to add the user to the **Selected Users** list.

    - To allow access to specific groups and the associated subgroups (if configured for subgroups), click the **Groups** tab, select the group name in the **Available Groups** list, and click (>) to add the user to the **Selected Groups** list.



f. Click **Create**.

For more information, see *Security Administration* in the Teamcenter documentation.

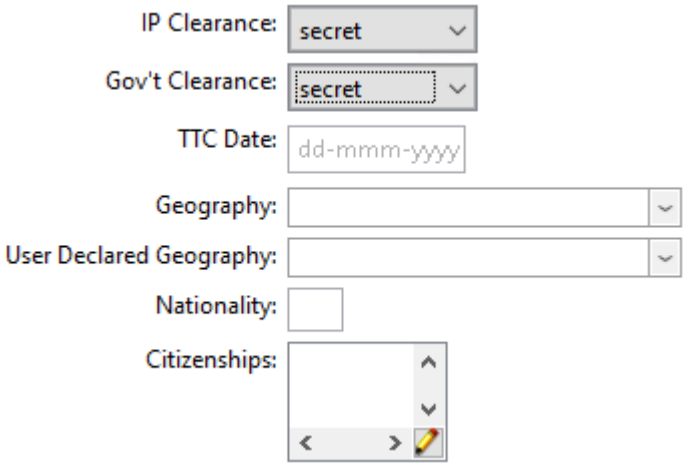
2. Assign the required clearance level to the design engineers, IDSM administrators, and suppliers:

a. Log on to the rich client as a user with Teamcenter administration privileges.

b. In the lower-left pane of the Organization application, select the required design engineer, IDSM administrator, or supplier account.

c. In **IP Clearance** of the **ADA/ITAR Attributes** section, select the clearance level that users must have to classified data with **IP** license.

d. In **Government Clearance** of the **ADA/ITAR Attributes** section, select the clearance level that users must have to classified data with **ITAR** license.



e. Click **Modify**.

3. When the design engineer searches for a supplier, to ensure that Supplier Connect evaluates the ADA licenses assigned to the assembly and the supplier and displays only the suppliers that match the access level in the search results, do the following:

a. Log on to the web client as a user with Teamcenter administration privileges.

b. On the home page, click the **PREFERENCES** tile.

c. Set the **SUPPORTAL_enable_ITAR** preference to **True** to view the **ADA Enabled** column for an item or assembly.

d. Set the **SUPPORTAL_share_ITAR_data** preference to **False** to share ADA-licensed data with only ADA-licensed suppliers.

If this preference is set to **True**, the search results display all suppliers, irrespective of their access level.

e. Ensure that the following values are set for the **ITAR_level_list_ordering** and **IP_level_list_ordering** preferences:

- **secret**
- **super-secret**
- **top-secret**

f. Click **Save** to save your changes.

4. For the **ITAR** license, create ACLs for the **Has Government Classification** and **User In Attached ITAR License** conditions in Teamcenter Access Manager:

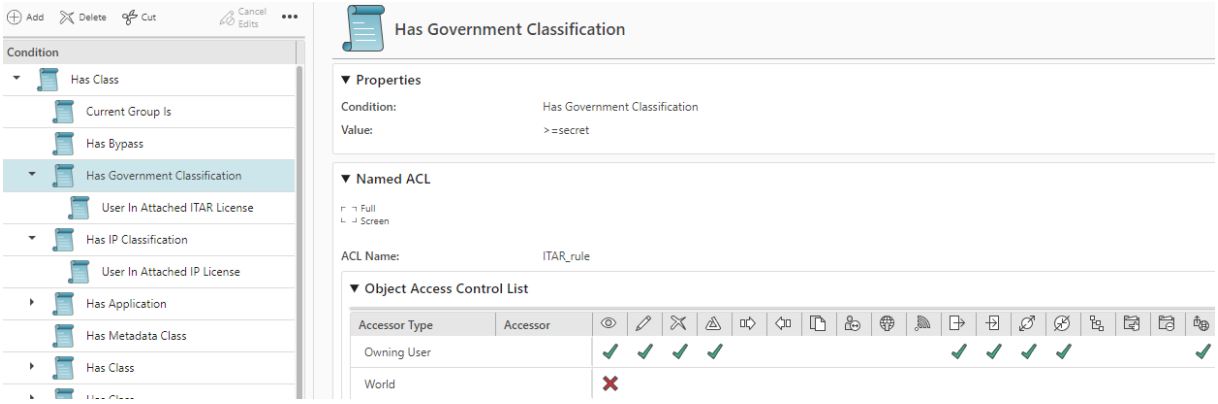
   a. Log on to the web client as a user with Teamcenter administration privileges.

   b. On the home page, click the **ACCESS MANAGER** tile.

   c. Select the **Has Class (POM Object)** node from the Access Manager (AM) rule tree.

   d. Create an ACL with the following details:

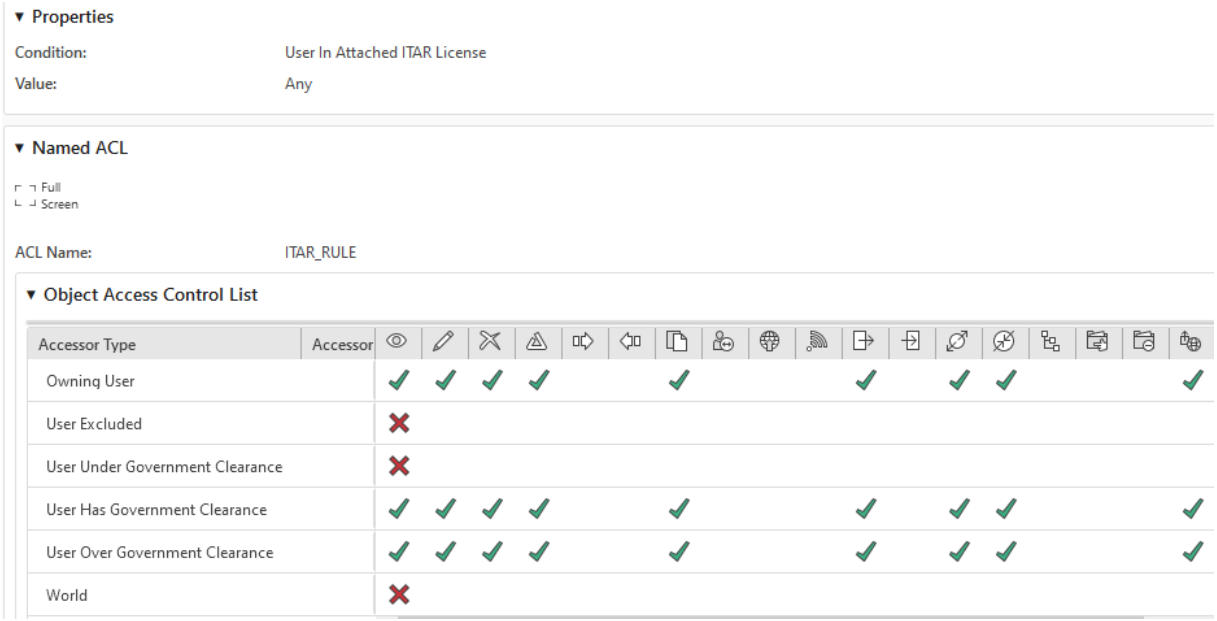
Condition	Value	Accessor Type	Privileges
Has Government Classification	**>=secret**	**Owning User**	Grant these privileges: • **Read** • **Write** • **Delete** • **Change** • **Export** • **Import** • **Transfer Out** • **Transfer In** • **Remote Check-Out**
		World	Deny the **Read** privilege.



e. Select the **Has Government Classification** condition and create an ACL for the **User In Attached ITAR License** condition with the following details:

Condition	Value	Accessor Type	Privileges
User In Attached ITAR License	**Any**	**Owning User**	Grant these privileges: • **Read** • **Write** • **Delete** • **Change** • **Copy** • **Export** • **Transfer Out** • **Transfer In** • **Remote Check-Out**
		User Over Government Clearance	Grant these privileges: • **Read** • **Write** • **Delete** • **Change**

Condition	Value	Accessor Type	Privileges
			• **Copy** • **Export** • **Transfer Out** • **Transfer In** • **Remote Check-Out**
		User Has Government Clearance	Grant these privileges: • **Read** • **Write** • **Delete** • **Change** • **Copy** • **Export** • **Transfer Out** • **Transfer In** • **Remote Check-Out**
		User Excluded	Deny the **Read** privilege.
		User Under Government Clearance	Deny the **Read** privilege.
		World	Deny the **Read** privilege.



5. For the **IP** license, to create ACLs for the **Has IP Classification** and **User In Attached IP License** conditions in Teamcenter Access Manager, do the following:

   a. Log on to the web client as a user with Teamcenter administration privileges.

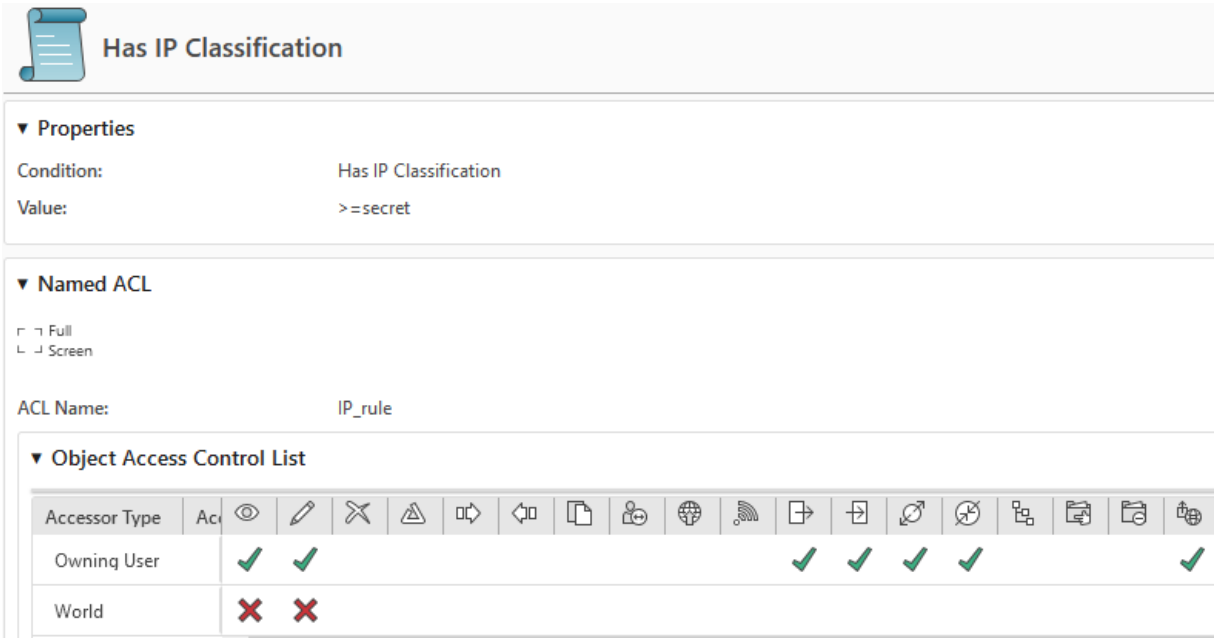
   b. On the home page, click the **ACCESS MANAGER** tile.

   c. Select the **Has Class (POM Object)** node from the AM rule tree.

   d. Create an ACL with the following details:

Condition	Value	Accessor Type	Privileges
Has IP Classification	**>=secret**	**Owning User**	Grant these privileges: • **Read** • **Write** • **Export** • **Import** • **Transfer Out** • **Transfer In**

Condition	Value	Accessor Type	Privileges
			• **Remote Check-Out**
		World	Deny these privileges: • **Read** • **Write**

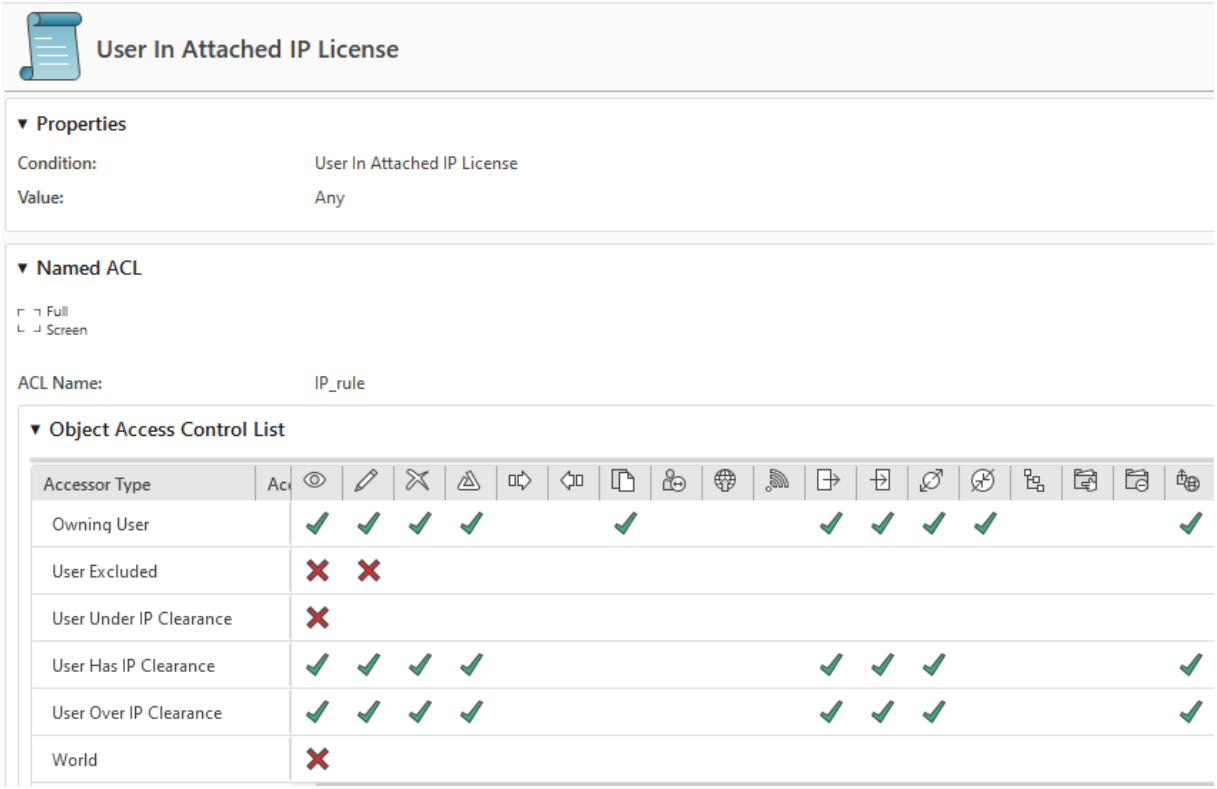


e. Select the **Has IP Classification** condition and create an ACL for the **User In Attached IP License** condition with the following details:

Condition	Value	Accessor Type	Privileges
User In Attached IP License	**Any**	**Owning User**	Grant these privileges: • **Read** • **Write** • **Delete** • **Change** • **Copy** • **Export**

Condition	Value	Accessor Type	Privileges
			• **Import** • **Transfer Out** • **Transfer In** • **Remote Check-Out**
		User Over IP Clearance	Grant these privileges: • **Read** • **Write** • **Delete** • **Change** • **Copy** • **Export** • **Import** • **Transfer Out** • **Transfer In** • **Remote Check-Out**
		User Has IP Clearance	Grant these privileges: • **Read** • **Write** • **Delete** • **Change** • **Copy** • **Export** • **Import**

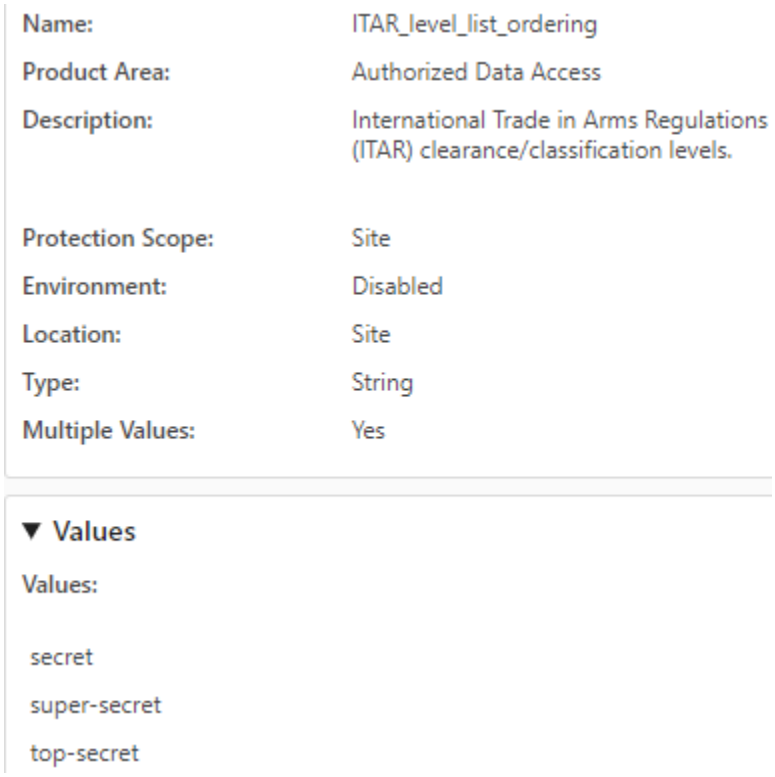
Condition	Value	Accessor Type	Privileges
			• **Transfer Out** • **Transfer In** • **Remote Check-Out**
		User Excluded	Deny these privileges: • **Read** • **Write**
		User Under IP Clearance	Deny the **Read** privilege.
		World	Deny the **Read** privilege.



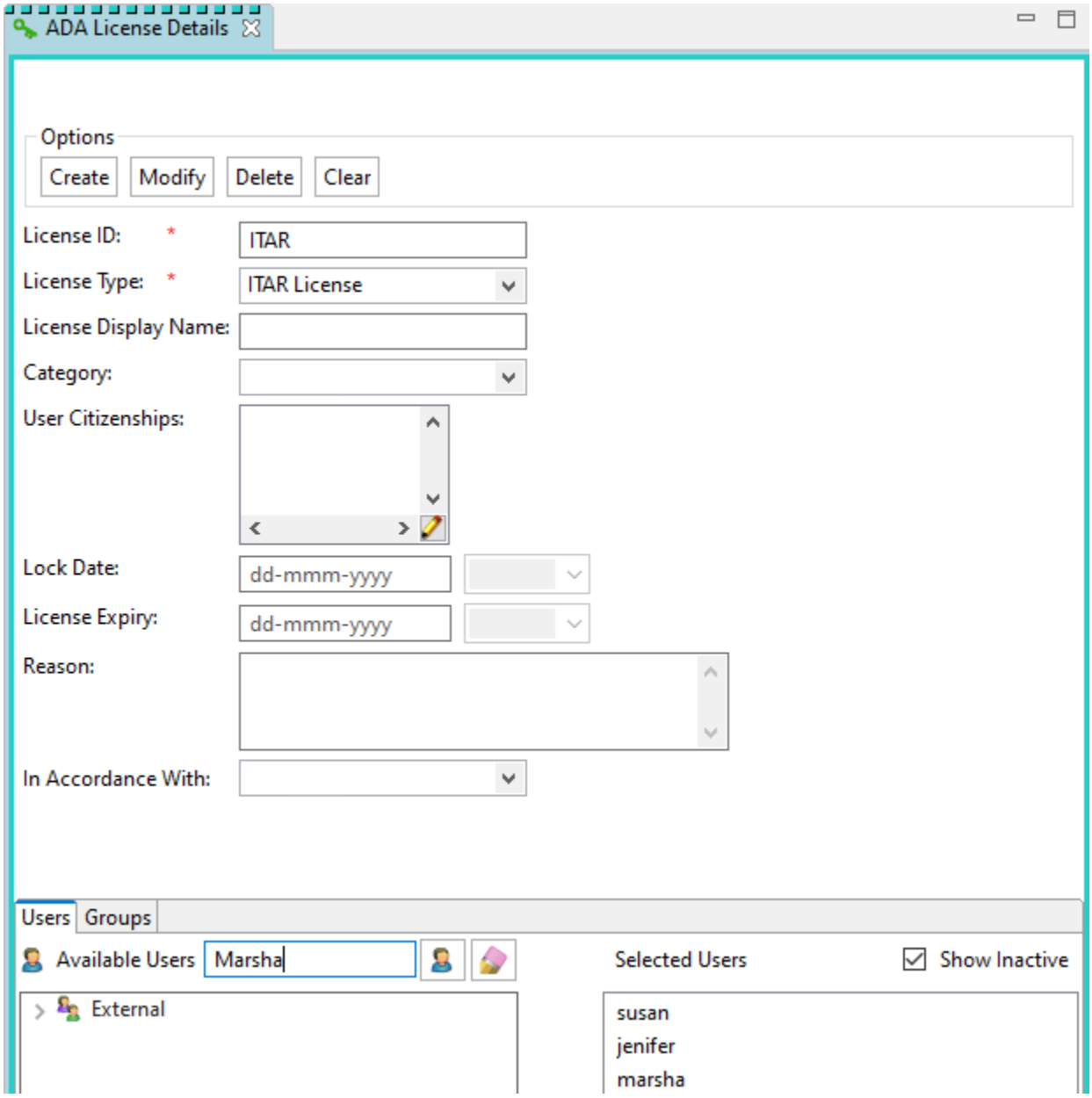
Example: Supplier Connect implements the access controls defined for an ITAR License

Consider a scenario where you have configured the following combination of ITAR license and access control lists (ACLs) in a Teamcenter environment:

- Configure the **ITAR_level_list_ordering** preference as follows:



- Assign an ITAR License to the required suppliers as follows:



For more information, see *Security Administration* in the Teamcenter documentation.

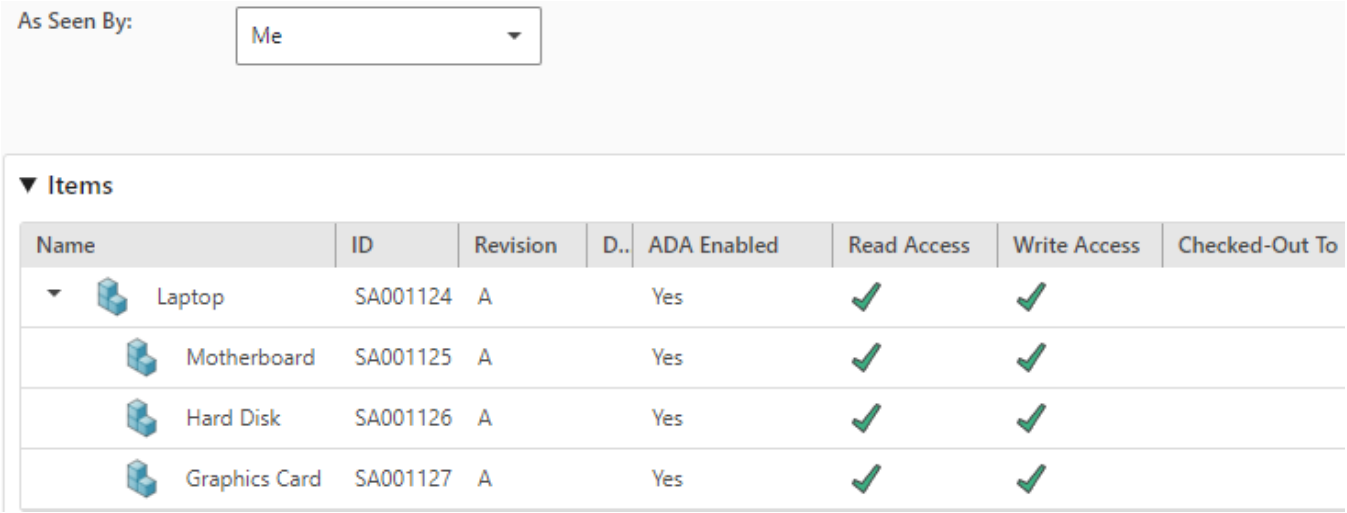
- Assign the required clearance level to the design engineers and suppliers as follows:

Supplier	ITAR Classification
Jenifer	This supplier has the **secret** ITAR Classification.
Marsha	This supplier has the **super-secret** ITAR Classification.
Susan	This supplier has the **top-secret** ITAR Classification.

- You must attach a license to the required assemblies. The access level of the supplier for the assembly is as follows:

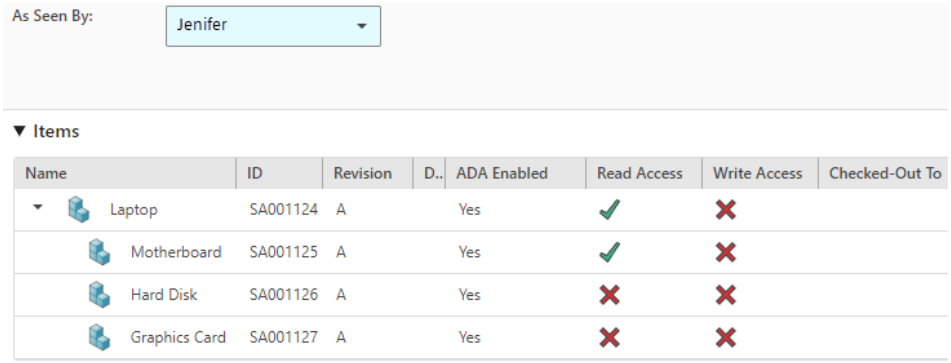
ITAR License attached to the assembly	ITAR classification of the supplier	Accessible to the supplier
Government Clearance: **secret**	**secret**	Yes
	super-secret	Yes
	top-secret	Yes
Government Clearance: **super-secret**	**secret**	No
	super-secret	Yes
	top-secret	Yes
Government Clearance: **top-secret**	**secret**	No
	super-secret	No
	top-secret	Yes

The design engineer creates a data exchange package for the following assembly, and assigns it to the suppliers Jenifer, Marsha, and Susan.

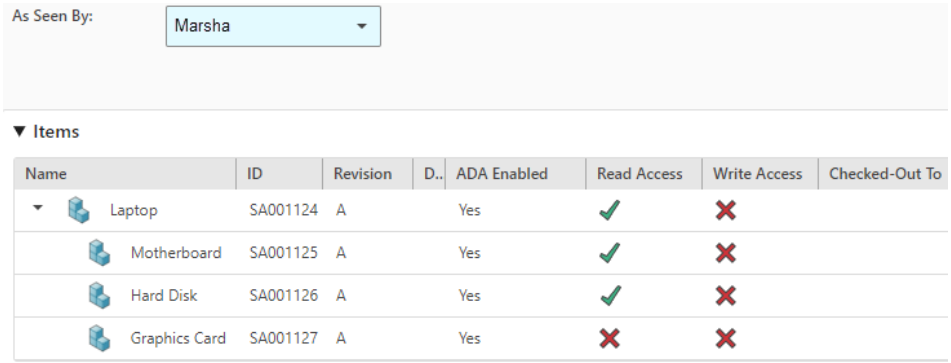


When these suppliers view their assigned data exchange package in the OEM Supplier Site, they view the only following assembly components because Supplier Connect applies the associated ACLs and license assignments and then creates the data exchange package with only the accessible assembly components:

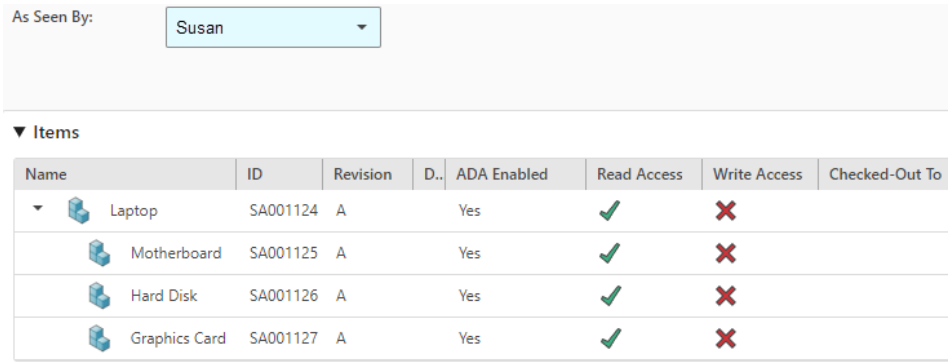
Jenifer with the **secret** access views these assembly components:



Marsha with the **super-secret** access views these assembly components:



Susan with the **top-secret** access views these assembly components:



12. Configure Supplier Connect to track the supplier actions and display updates in a response

After a design engineer sends a data exchange package to a supplier, the supplier works on the package in the OEM Supplier Site and submits a response. For the design engineer to track the supplier actions and view updates to an item or assembly in the OEM Sponsor Site, you must enable auditing in the OEM Supplier Site.

As the supplier works on the package in the OEM Supplier Site, the design engineer can open the package in the OEM Sponsor Site and track the supplier actions in the **Tracking** tab of the package.

After the supplier submits a response, the design engineer can open the response to view the type of updates made by the supplier. If the supplier has updated an assembly or its child component, a yellow bar appears next to it. This indicates that the supplier might have updated the assembly itself or a child component in the assembly. A green bar indicates an addition to the assembly, and a red bar indicates a deletion in the assembly.

Procedure

1. To track the supplier actions and display updates in a response, you must set the following preferences on the OEM Supplier Site:

   - Set the **AWC_show_audit_logs** preference to **True**.
   - Set the **TC_audit_manager** preference to **ON**.
   - Set the **TC_audit_manager_version** preference is set to **3** (default value).

   For more information, see *BMIDE for Data Model Design* in the Teamcenter documentation.

2. On the OEM Supplier Site, make the required audit definitions active as follows:

   a. In Business Modeler IDE, create a new Business Modeler IDE template project.

   b. To track the supplier actions, make the following audit definitions active:

      - **BOMView Revision:__Component_Add**
      - **BOMView Revision:__Component_Remove**
      - **Dataset:_Create**

- **Dataset:_Open**
- **PSBOMView:_Modify**
- **PSBOMViewRevision:_Modify**
- **Item:_Attach**
- **Item:_Detach**
- **Item:_Modify**
- **ItemRevision:_Attach**
- **ItemRevision:_Detach**
- **ItemRevision:_Modify**

c. To display the supplier updates in a response, make the following audit definitions active:

- **ImanFile:_Read_File**
- **ImanFile:_Write_File**

d. On the main toolbar, click **Save Data Model**.

e. Generate a software package for distribution and deploy the package using Deployment Center.

For more information about generating a software package for distribution, see *BMIDE for Data Model Design* in the Teamcenter documentation. For more information about deploying a package using Deployment Center, see *Deployment Center — Usage* in the Teamcenter documentation.

13. Share the Briefcase Browser installation file with suppliers

For suppliers to work on Briefcases sent by you, the OEM, you must set up a location from where the suppliers can download the Briefcase Browser installation file. One option is to set up a File Transfer Protocol (FTP) server, add the Briefcase Browser installation file to this server, and share the location with the suppliers.

1. Download version 2412 of **Briefcase Browser** from the download page on **Support Center**.

2. Decide on a secure method to share the Briefcase Browser installation file, such as:

   - Email with a secure attachment.
   - Secure FTP server.
   - Cloud storage service with restricted access.
   - Company's internal network or file-sharing system.

3. Write clear instructions on how to access and download the installation file.

   Include any necessary passwords or access codes, while ensuring they are shared securely.

4. Send an email or notification to your suppliers with the following information:

   - Brief explanation of what Briefcase Browser is and why they need to install it.
   - Access instructions or a direct link to download the installation file.
   - Installation and configuration instructions or a link to a guide on how to install and configure Briefcase Browser.

     > Note:
     >
     > You can share the information provided in the *Configuration tasks to be performed by suppliers to work with Briefcases* section.

   - Contact information for support in case they encounter issues.
   - **Site Name** and **Site ID** of the OEM Sponsor Site. This information is available in the **Sites** node of the **Organization** application of Teamcenter.

- ID of the **Unmanaged Site** for each supplier. This information is available when you open the associated vendor of the supplier, select and open the **Company Contact**, and copy the ID from the **Unmanaged Site** box.

After sharing the installation file, ensure that you are available to assist with any installation issues and that all suppliers have successfully installed and configured Briefcase Browser.

14. Configuration tasks to be performed by suppliers to work with Briefcases

Requirements for using Briefcase Browser

Prerequisites

There are no prerequisites for installing and running Briefcase Browser. However, to perform specific actions in Briefcase Browser, there are some requirements:

- Briefcase Browser requires a 64-bit Window operating system.
- You must have Java Runtime Environment (JRE) 1.8 or later installed.

  For NX, the JRE version must be the same as that required by the version of NX you are using.
- To create new NX assemblies or modify existing NX assemblies or components, you must have Siemens Digital Industries Software NX 9.0 or later installed.
- To customize Briefcase Browser, you must have Eclipse software with version 3.8 of the Eclipse RCP installed.

See the Hardware and Software Certifications knowledge base article on Support Center for the latest information about supported software versions.

Enable Briefcase Browser

If you receive an unmanaged site Briefcase configuration file from your Teamcenter manufacturer (OEM) or supplier, you must load it to set the proper site attributes before you use Briefcase Browser.

Configure Briefcase Browser

You can change your Briefcase configuration, when required, from within the Briefcase Browser interface.

To customize your Briefcase Browser, copy *CustomDatasetMappings* to the current configuration.

Start Briefcase Browser

Start the application as you do any application on your system. No password or user ID is required.

Install and configure Briefcase Browser on the supplier's computer

Suppliers must install and configure Briefcase Browser on their computers to work on Briefcases sent by the OEM. The OEM provides a location from where the suppliers can download the Briefcase Browser installation file.

1. Browse to the folder where the suppliers have downloaded the Briefcase Browser installation file, and extract the contents of the Briefcase Browser kit to a local folder on their computer.

2. If you are using the plugin for NX, perform the following steps:

   a. Ensure the value of the **UGII_ROOT_DIR** environment variable is set to the location of the root directory for the NX installation that you use with Briefcase Browser.

   b. Add the **UGII_ROOT_DIR** and **UGII_BASE_DIR** environment variables to the start of the **PATH** environment variable value.

   c. Open a command window and run the following batch file:

      bb_install_path\BB*BB_version*\ConfigureNXplugins.bat

   The NX instance and Java virtual machine used by Briefcase Browser must be 64 bit.

   If you have multiple versions of NX installed on your host, the version that Briefcase Browser uses is determined by the NX version instance that is in the Windows registry.

3. Place the Briefcase Browser archive file (**bb_wntx64.zip**) in the directory in which you want to install it. Unzip the file.

4. If you are using a non-NX CAD program plugin (such as the plugin for CATIA), remove the following file from your system.

   bb_install_path\BB*BB_version*\plugins\com.teamcenter.bce.cad.nx.*version_and_date*.jar

   Refer to the instructions provided with the **BBpC** plug-in in Support Center for information about differences in the installation process.

5. If you are using the Briefcase Browser JT plugin, open a command window and run the following batch file:

   bb_install_path\BB*BB_version*\ConfigureBBJTplugins.bat

6. After Briefcase Browser is installed, use the following steps to configure Briefcase Browser to exchange data with a particular Teamcenter (OEM) site. After following these steps, the configuration will appear in the **Configuration Name** list on the **Preferences** dialog box.

a. Start Briefcase Browser and choose **Window→Preferences**.

b. Under **Configuration Name**, click **New**.

c. Enter a name identifying the site configuration, the site ID provided by the Teamcenter site, and click **OK**.

A new directory is created to hold the site's configuration files.

> Example:
>
> *bb_install_path*\BB*BB_version*\bbworkspace\configurations*new_site*

d. Close Briefcase Browser.

e. Navigate to the following directory.

bb_install_path\BB*BB_version*\example\bbworkspace\configurations\example

f. Copy the *example* directory's contents to the directory you created at the start of this procedure.

g. In the *site-id.properties* file, update the value of **site-id** to the ID of the **Unmanaged Site** for the supplier who is configuring Briefcase Browser.

The OEM provides the ID of the **Unmanaged Site** for each supplier.

h. Open the following file in a text editor.

bb_install_path\BB*BB_version*\bbworkspace\configurations*new_site*\CustomMappings.xml

i. In *CustomMappings.xml*, update the values of **oem_name** and **site_id** to the values assigned to the Teamcenter (OEM) site from which you are receiving data.

> Note:
>
> The OEM provides the **Site Name** and **Site ID** details to the supplier.

> Example:
>
> `<oem name="OEM Name" site_id="2468" ...`

> Note:
>
> If the suppliers are working with multiple OEMs, they must install an instance of Briefcase Browser for each OEM and update *CustomMappings.xml* with the values of **oem_name** and **site_id** for the respective OEMs.

j. Save the file. The configuration appears in the **Configuration Name** list on the **Preferences** dialog box the next time you start Briefcase Browser.

7. To configure a new supplier site, in the **Preference** dialog box, click **New**.

8. Type the **Site ID** for the supplier site.

   The OEM provides the ID of the **Unmanaged Site** for each supplier.

9. Click **OK** and close the **Preferences** dialog box.

10. Close Briefcase Browser.

11. After the suppliers install and configure Briefcase Browser, they can start it by double-clicking the Briefcase Browser program file:

    bb_install_path\BB*BB_version*\BriefcaseBrowser.exe

12. On the **Welcome** screen of Briefcase Browser, click **Edit Preferences**.

    Verify that the supplier site is configured.

13. Click **OK** and close the **Preferences** dialog box.

Briefcase Browser documentation

View Briefcase Browser documentation by choosing **Help Contents** from the **Help** menu. Briefcase Browser documentation is also available in PDF format:

bb_install_path\BB*BB_version*\docs\Teamcenter_Briefcase_Browser_Guide.pdf

Install the BBpC plug-in for CATIA

To open a Briefcase containing CATIA data and to update the CAD data in CATIA, you must install and configure the **BBpC** plug-in for CATIA. You can download this plug-in from the download page on **Support Center**. For more information about installing and configuring the **BBpC** plug-in, see the instructions provided with the plug-in.

Briefcase Browser site configuration files

Briefcase Browser reads the XML configuration files in the **bbworkspace\configurations** directory. Each configuration has a separate directory that contains the **site-id.properties** file as a minimum.

The **create_briefcase_browser_config_package** utility creates a compressed package file of the configuration files that you can provide to your suppliers. The utility takes the path to the Briefcase Browser installation ZIP file (**-bbDir** argument) and generates a managed (OEM) site ZIP file containing the OEM configuration package.

```
create_briefcase_browser_config_package -u=username -p=passwd -g=dba
-bbDir=C:\apps\bb
```

The package name is the OEM site name. It contains the **CustomMappings.xml** file with the OEM site ID set as the target site ID. It also contains the **TCXML.xsd** schema file, generated from the OEM and the OEM configuration file.

site-id.properties

Defines the unmanaged site ID. This value can be any numeric sequence not starting with a zero and is not required to meet Teamcenter site ID requirements. If this file is not present, Briefcase Browser does not allow you to create a Briefcase file. You can create or modify this file manually or use the **Preference** dialog box in Briefcase Browser.

It must also contain the following additional configuration files:

TCXML.xsd

Defines the schema that Briefcase Browser uses to load, display, and create Briefcase files. This file is typically supplied by the managed (OEM) site to the supplier (unmanaged) site. It is available in the *TC_DATA* directory of the Teamcenter installation.

If a **TCXML.xsd** file does not exist in the configuration directory for your site, Briefcase Browser uses the standard Teamcenter schema. **TCXML.xsd** is required in this directory for comparing and previewing Briefcase files.

> Note:
>
> The uniform resources identifiers (URIs) that appear in the headers of PLM XML and TC XML files serve as namespace names, are unique identifiers for an XML vocabulary. Although they are URIs, they are not used to identify and retrieve web addresses.

CustomMappings.xml

Defines the following information about the Teamcenter (OEM) site with which you exchange Briefcase files:

- The site name.

- The site ID.
- The Teamcenter version.
- If your site must use the **auto_baseline** (baseline) feature when exchanging updated Briefcase data.
- If the site allows precise or imprecise structures.
- If your site must create all replica objects as stubs (**include_all_objects=false**). When writing reference objects as stubs, Briefcase Browser does not package any corresponding CAD data in the Briefcase package. If this value is set to **true**, Briefcase Browser writes all objects as full objects in the Briefcase file reference replica parts.
- If your site must include full objects for all checked-out parts and locally owned parts (**include_modified_objects_only=false**). If this value is set to **true**, Briefcase Browser writes local parts as full objects. Parts checked out to your site as full objects are also written as full objects if they are modified since the file was last saved, including their parent and grandparent objects. If objects checked out to your site have not been modified, they are written as stub objects and the corresponding part files are not included in the Briefcase package.
- The separator character the site requires between the item ID and revision.
- Custom type mapping to OEM objects.
- Release status values the managed (OEM) site allows you to assign to parts or assemblies that you create in the **release_status_name** elements. Briefcase Browser displays the values that you supply in **release_status_name** elements in the **Release Status Name** list in the **Preferences** dialog box. The value you select in the **Preferences** dialog box is assigned as the release status of any new CAD parts or assemblies you create. The value must match one of the valid values for the Teamcenter release status at the OEM site.
- Custom forms related to item revisions to process when exchanging data, such as business object forms with mass-related properties. When **ir_to_form** is set to **true**, the listed forms are processed. If **ir_to_form** is set to **false**, the forms are ignored. See the **ir_to_form** section in the following sample for examples.

Sample content for this file:

```
<?xml version="1.0" encoding="UTF-8"?>
<custom_mappings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                 xsi:noNamespaceSchemaLocation="../bce-core/CustomMappings.xsd">
   <oem name="your_oem_name" site_id="87654321" tc_version="Target-TC-Version"
        auto_baseline="false" generate_validation_xml="false" is_precise="true"
        separator="/" object_name_separator="/" bomview_type_name="view"
        include_modified_objects_only="false" include_all_objects="false"
        extract_to_sub_directory="false" process_reference_briefcases="true">
     <release_status_name>Snapshot</release_status_name>
     <release_status_name>TCM Released</release_status_name>
```

```
   <release_status_name>R2InWork</release_status_name>
</oem>

<ir_to_form enabled="false">
  <form_type>custom_form_type</form_type>
  <relation>custom_relation</relation>
</ir_to_form>

<item_type_mapping custom_type="Item">
  <multi_field_key>
    <attribute>item_id</attribute>
  </multi_field_key>
  <helper_object_map custom_type="ItemRevision"
          ootb_type="ItemRevision"/>
  <helper_object_map custom_type="Item--Master"
          ootb_type="Item--Master"/>
  <helper_object_map custom_type="ItemRevision--Master"
          ootb_type="ItemRevision--Master"/>
</item_type_mapping>

<item_type_mapping custom_type="CAD">
  <multi_field_key>
    <attribute>item_id</attribute>
  </multi_field_key>
  <helper_object_map custom_type="CAD--Revision"
                     ootb_type="ItemRevision"/>
  <helper_object_map custom_type="CAD--Master"
                     ootb_type="Item--Master"/>
  <helper_object_map custom_type="CAD--Revision--Master"
                     ootb_type="ItemRevision--Master"/>
</item_type_mapping>

<item_type_mapping custom_type="B4Item">
<multi_field_key>
  <attribute>item_id</attribute>
</multi_field_key>
<helper_object_map custom_type="B4ItemRevision"
                   ootb_type="ItemRevision"/>
<helper_object_map custom_type="B4ItemMaster"
                   ootb_type="Item--Master"/>
<helper_object_map custom_type="B4ItemRevisionMaster"
                   ootb_type="ItemRevision--Master"/>
/item_type_mapping>

<item_type_mapping custom_type="CommercialPart">
  <multi_field_key>
    <attribute>item_id</attribute>
  </multi_field_key>
  <helper_object_map custom_type="CommercialPart--Revision"
                     ootb_type="ItemRevision"/>
  <helper_object_map custom_type="CommercialPart--Master"
                     ootb_type="Item--Master"/>
  <helper_object_map custom_type="CommercialPart--Revision--Master"
                     ootb_type="ItemRevision--Master"/>
</item_type_mapping>

<item_type_mapping custom_type="Design">
  <multi_field_key>
    <attribute>item_id</attribute>
  </multi_field_key>
```

```
    <helper_object_map custom_type="Design--Revision"
                       ootb_type="ItemRevision"/>
    <helper_object_map custom_type="Design--Master"
                       ootb_type="Item--Master"/>
    <helper_object_map custom_type="Design--Revision--Master"
                       ootb_type="ItemRevision--Master"/>
  </item_type_mapping>

  <item_type_mapping custom_type="Part">
    <multi_field_key>
      <attribute>item_id</attribute>
    </multi_field_key>
    <helper_object_map custom_type="Part--Revision"
                       ootb_type="ItemRevision"/>
    <helper_object_map custom_type="Part--Master"
                       ootb_type="Item--Master"/>
    <helper_object_map custom_type="Part--Revision--Master"
                       ootb_type="ItemRevision--Master"/>
  </item_type_mapping>
</custom_mappings>
```

The **auto_baseline** attribute indicates whether or not your Briefcase Browser provides autobaseline functionality. If this is set to **true**, the baseline feature is enabled. The template file has this value set to **true**. If it is set to **false**, Briefcase Browser does not automatically revision objects. If the attribute is not defined in this file, Briefcase Browser performs automatic revisions as if the attribute was set to **true**.

If the Briefcase file you are exchanging must contain precise assembly structures, set the **is_precise** attribute to **true**. Set this value to **false** when imprecise assembly structures are allowed.

If you intend to add objects to CAD parts in the CAD application, set the **include_all_objects** attribute to **true** to include them when you save the Briefcase file for exporting back to Teamcenter.

You can have any number of release status elements. These become the selection list for **Release Status** in your Briefcase Browser **Preferences** dialog box.

You map custom CAD parts types to OEM types by assigning a custom **Item** type to the items in the TC XML data created for your CAD part. You define the subtype of the **Item** type as a helper object, for example:

```
<helper_object_map custom_type="CADPart" ootb_type="Item"/>
```

This causes the TC XML data generated for custom **CADPart** supplier owned parts to be created as **Item** objects at the OEM site.

> Note:
>
> The custom item type must be defined in the schema (**TCXML.xsd**) file used by Briefcase Browser.

You can have multiple custom types defined in this file. Briefcase Browser locates the matching custom type in the file and maps the file to the defined OEM object. If a custom type part is not found in the **CustomMappings.xml** file, the first custom type defined is used. If there are no custom types defined, Briefcase Browser maps the part to the standard Teamcenter type.

CustomDatasetMappings.xml

This XML file contains valid dataset extensions and relation types supported for Non-CAD files. Each dataset extension specifies whether it is a primary (master), dataset name, **ref_names**, and relation to be used while generating TC XML. Each relation type specifies the display relation for the **Add Dataset** dialog box and the actual relation to be used for generating TC XML. If this file is not found, an OOTB file is used. You can add additional non-CAD types to this file.

Caution:

If your system has CAD dataset types other than the primary dataset, and the dataset type follows the model file naming convention, you must add an entry representing the dataset. Add the entry with the **is_master** attribute set to **False**, for example:

```
<cad_data_set_mapping is_master="False" dataset_type="UGPART"
ref_names="UGPART" relation=""/>
```

This prevents an error from occurring when you open or synchronize an updated CAD assembly in Briefcase Browser.

```
<?xml version="1.0" encoding="utf-8"?>

<!-- XML file containing valid dataset extensions and relation types supported for
Non-CAD files.
  Each dataset extension specifies if it is a master, dataset name, ref_names and
relation to be
  used while generating TCXML. Each relation type specifies the display relation for
the Add Dataset
  dialog and the actual relation to be used for generating
  TCXML. -->
<custom_data_set_mapping xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<data_set_mapping extension="prt">
<cad_data_set_mapping is_master="True" dataset_type="UGMASTER" ref_names="UGPART"
relation=""/>
<cad_data_set_mapping dataset_type="UGPART" ref_names="UGPART" relation=""/>

</data_set_mapping>
        <data_set_mapping extension="doc">
        <cad_data_set_mapping dataset_type="MSWord" ref_names="word"
        relation="IMAN_reference"/>
</data_set_mapping>
        <data_set_mapping extension="docx">
        <cad_data_set_mapping dataset_type="MSWord" ref_names="word"
        relation=""/>
</data_set_mapping>
        <data_set_mapping extension="xls">
        <cad_data_set_mapping dataset_type="MSExcel" ref_names="excel"
        relation=""/>
</data_set_mapping>
```

```
        <data_set_mapping extension="jpg">
        <cad_data_set_mapping dataset_type="JPEG" ref_names="JPEG_Reference"
        relation=""/>
</data_set_mapping>
        <data_set_mapping extension="jt">
        <cad_data_set_mapping dataset_type="DirectModel" ref_names="JTPART"
relation="IMAN_Rendering"/>
</data_set_mapping>
            <relation_type actual_relation="IMAN_specification"
display_relation="specification"/>
            <relation_type actual_relation="IMAN_Rendering"
display_relation="rendering"/>
            <relation_type actual_relation="IMAN_manifestation"
display_relation="manifestation"/>
            <relation_type actual_relation="IMAN_reference"
display_relation="reference"/>
</custom_data_set_mapping>
```

cad_to_tc_attribute_map.xml

Defines the mapping of user-defined NX attributes to qualified Teamcenter object attributes. The user-defined attributes must be part of the configured TC XML schema (**TCXML.xsd** file). This allows you to define attributes for qualified objects in addition to the required attributes.

> Caution:
>
> You can map only one CAD part attribute to one Teamcenter attribute (1-to-1 map). Mapping a CAD part attribute to multiple Teamcenter attributes or a single attribute to multiple item types can corrupt or lost data.

Example:

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- Only one CAD2TC_attribute_mappings that can contain more than one
     attribute map. These mappings will hold a list of CAD attributes
     that map to teamcenter attribute -->

<CAD2TC_attribute_mappings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:noNamespaceSchemaLocation="cad_to_tc_attribute_map.xsd">

  <!-- cad_part_attr should be unique for each attribute_mapping -->
  <attribute_mapping cad_part_attr="PART_MATERIAL" tc_attr="nisPartMaterial"
                     tc_type="CAD--Revision--Master"/>
  <attribute_mapping cad_part_attr="PART_THICKNESS" tc_attr="nisPartThickness"
                     tc_type="CAD--Revision--Master"/>
  <attribute_mapping cad_part_attr="CALC_WEIGHT" tc_attr="nisCalculationWeight"
                     tc_type="CAD--Revision--Master"/>
  <attribute_mapping cad_part_attr="CALCULATIVE_COEFFICIENT"
                     tc_attr="nisCalculativeCoefficient"
                     tc_type="CAD--Revision--Master"/>
  <attribute_mapping cad_part_attr="Z_CENTROID" tc_attr="nisGravityZ"
                     tc_type="ItemRevision--Master"/>
  <attribute_mapping cad_part_attr="Y_CENTROID" tc_attr="nisGravityY"
                     tc_type="CAD--Revision--Master"/>
  <attribute_mapping cad_part_attr="X_CENTROID" tc_attr="nisGravityX"
```

```
                        tc_type="CAD--Revision--Master"/>
    </CAD2TC_attribute_mappings>
```

visible-attributes.xml

Defines the attributes that are displayed in Briefcase Browser properties views. By default, Briefcase Browser displays all qualified attributes. If this file is present, Briefcase Browser limits the attributes in the properties views to the attributes defined in this file. The following is sample content for this file:

```
<visible_attributes>

    <group name="Item">
        <attribute ootb_type="Item" name="item_id"/>
        <attribute ootb_type="ItemRevision" name="object_name"/>
        <attribute ootb_type="ItemRevision"
name="object_description"/>
    </group>

    <group name="Admin">
        <attribute ootb_type="POM_imc" name="POM_imc"/>
        <attribute ootb_type="Group" name="Group"/>
        <attribute ootb_type="User" name="User"/>
    </group>

</visible_attributes>
```

attributes_text_locale.xml

Defines the localized values for the language indicated by the name of the directory containing the file. The directory name consists of a two-character locale and two-character country code such as **en_US**. The language directories must be in the **lang** directory in the site's configuration directory.

For example, the following shows the US English (**en_US**) and the Japanese localization (**ja_JP**) directories:

Briefcase Browser reads the TC XML file content and displays the object property names as defined in the file. The properties are database field names that may not be readable by your users. You can use this file to map the database field names to usable localized names.

Your **attributes_text_locale.xml** files must be UTF-8 encoded. They must also contain the following element as the root XML element in the file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

If the property names are not displayed in your locale language, use a different text editor for UTF-8 encoding.

Following is sample content for this file in the Japanese locale:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<textsrv filename="attributes_text_locale.xml">

<key id="inbox_type">志信トレイ</key>
<key id="inbox_name_1">実行タスク</key>
<key id="inbox_name_2">追跡タスク</key>
<key id="type_label">タイプ</key>
<key id="object_label">オブジェクト</key>
<key id="property_label">プロパティ</key>
<key id="msg_string">フォルダ倉も癈存在癇宓癌ん。</key>

<!--generic_shell.cxx-->
<key id="shell_string">ObjectListBox Shell</key>

<!--objectlistbox.cxx-->
<key id="ownerid_string">所有者ID</key>
<key id="date_string">作房日</key>
<key id="cannot_string">読込盈丿帳</key>
<key id="readOnlyMsg">読込盈専用</key>
<key id="app_encapsulation_label">アプリケーション覿約</key>
<!--tool.cxx-->

<!--distributionlist.cxx  envelope.cxx-->
<key id="mail_label">メール</key>

<!--form.cxx-->
<key id="form_def_label">フォーム定義ファイル忿</key>
<key id="structure_group_label">構房グループ</key>

<!--bomview.cxx-->
<key id="bomview_label">BOMビュー</key>
<key id="product_label">製弩</key>
<key id="PSM_label">PSM</key>
<key id="item_id_string">アイテムID</key>
<key id="dataset_id">データセットID</key>
<!--! <MSF> 04-Mar-1994 Workspace column headings - the xxx names are used-->
<!--! for backward compatibility with existing .tc_env files-->
<key id="private_object_string" scope="private">オブジエクト</key>
<key id="private_id_label" scope="private">ID</key>

<!-- Part Object -->
<key id="is_designrequired">デザイン癈必覿</key>
<key id="make_or_buy">製造/購買</key>
<key id="part_make">製造</key>
<key id="part_buy">購買</key>
  .
  .
  .
</textsrv>
```

Sample files are provided for each of these configuration files in the **example\bbworkspace\configurations\example** directory.