TEAMCENTER

Substance Compliance — 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

Substance Compliance utilities

1. Setting up Teamcenter Substance Compliance

Substance compliance is the process of checking if the parts used in your company products conform to environmental regulations. Teamcenter helps verify if the products are environmentally compliant by checking the material and substance information for in-house parts and supplier parts used in the products.

Teamcenter helps compliance officers request and import this material and substance information for parts, review the information for completeness, run a compliance check on parts and assemblies, and then apply exemptions where applicable.

As an administrator, you install the various **components** of Substance Compliance. You then integrate these components with Teamcenter using a middleware component, Teamcenter Integration Framework. Further, you configure Teamcenter to import the regulations required for checking the compliance of a part. You also set up various validations. This enables compliance officers to perform the different tasks for checking the compliance of a part or assembly.

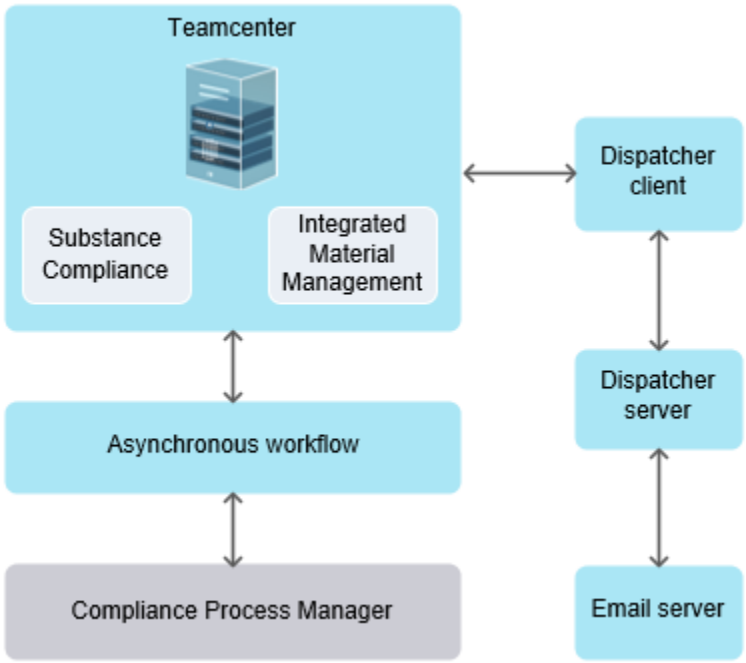
Where do I go from here?

Compliance officer	**Checking compliance in Active Workspace** — See *Substance Compliance on Active Workspace — Usage*

	Checking compliance in Rich Client — See *Substance Compliance on Rich Client — Usage*
Administrator	
How do I deploy Substance Compliance?	See the different high-level tasks specified in a recommended sequence to deploy **Substance Compliance**.
Install Dispatcher	Dispatcher provides the framework to extract and load data to Teamcenter. You need to install both Dispatcher Server and Dispatcher Client as a standalone instance, as described. These **steps outline how to do that**.
What is Compliance Process Manager (CPM) and does it need to be integrated with Teamcenter?	To be able to check the compliance of parts, you must integrate Teamcenter with CPM. See the **async workflow to integrate the two**.
Configure Teamcenter to work with Substance Compliance	See the tasks specified in the section on how to **configure Teamcenter for Substance Compliance**
Configure Substance Compliance for various tasks	You configure Substance Compliance to enable requesting, importing, validating, and reviewing supplier declarations. Follow the **tasks specified to configure Substance Compliance**.
Email polling in Teamcenter	Set up email polling to enable downloading supplier declarations in Teamcenter. Specifically, refer to the **workflow to set up email polling**.

2. Components of Teamcenter Substance Compliance

The Teamcenter Substance Compliance solution consists of the following components:



- **Teamcenter Substance Compliance**

  The Teamcenter Substance Compliance solution is used for verifying if your company product conforms to specific environmental regulations. If the product uses supplier parts, a request to obtain the material and substance information is sent to the suppliers, using this solution.

- **Integrated Material Management**

  Integrated Material Management (IMM) stores the approved material and substance information imported from a third-party database, for example, from Granta. These materials and substances are associated with the parts used in your company product.

- **Compliance Process Manager**

  Compliance Process Manager (CPM) is a third-party application that Teamcenter Substance Compliance uses for performing the substance compliance check.

- **Teamcenter Integration Framework**

> Caution:
>
> Substance Compliance no longer requires Teamcenter Integration Framework for connecting with CPM. New **async workflow** is provided for this connection. Teamcenter Integration Framework- CPM connect function from Substance Compliance is now deprecated and will be obsolete soon.

Teamcenter Integration Framework is a middleware component that integrates Teamcenter with CPM. With this integration, the substance compliance check initiated for a part in Teamcenter is sent to CPM. CPM assesses the part for restricted substances and sends the compliance status back to Teamcenter.

- **Dispatcher Server**

  Dispatcher Server enables Teamcenter users to manage job distribution and execution. This enables asynchronously distribution of jobs to different computers that have the resource capacity to execute the job. Distributing resource-intensive activities helps reduce the server load. You can also schedule high-CPU or high-memory jobs for off-hours processing.

  When working with Substance Compliance, you can schedule the supplier declarations to be imported automatically from the email server to a particular location at a specific time.

- **Dispatcher Client**

  This component provides the framework to extract and load data to Teamcenter. It provides the communication mechanism to use the other Dispatcher Server components.

  When used with Substance Compliance, Dispatcher Client sends the tasks received from Teamcenter for jobs related to processing the supplier declarations to the Scheduler which then forwards them to the Module. These tasks include, among others, requesting, importing, and validating supplier declarations. The server subsequently executes these tasks and records the logs at a specific location.

- **Email Server**

  Email server is a server on your network used for sending, receiving, and storing emails. In the case of Substance Compliance, the declaration-request emails are sent to the suppliers via the email server. Additionally, the emails received from the suppliers with the declarations as attachments are stored on the email server. Dispatcher Server polls the email server at regular intervals to download these emails at a specified location.

3. Planning your Substance Compliance deployment

Applications required for Substance Compliance

Application	Description
Teamcenter Foundation	Teamcenter Foundation has the complete Teamcenter application root directory, including the Teamcenter server process. It either creates a data directory for storing database specific files or configures the Teamcenter installation to connect to an existing data directory.
Teamcenter Vendor Management	Teamcenter Vendor Management stores the supplier information such as the supplier name, supplier location, contact number, and email address. This information is required when requesting declarations, such as material substance declaration or conflict mineral declaration from the supplier.
(Optional) Teamcenter BOMcheck Integration	Teamcenter BOMcheck Integration enables suppliers to provide material and substance declarations on the BOMcheck web portal. Teamcenter then imports the declarations from BOMcheck to review and perform a compliance check.
Integrated Material Management	Integrated Material Management (IMM) stores the approved material and substance information imported from a third-party database, for example, from Granta. These materials and substances are associated with the parts used in your company product.
Compliance Process Manager	Compliance Process Manager (CPM) is a third-party application that Teamcenter Substance Compliance uses for performing the substance compliance check.

Considerations for installing Teamcenter Integration Framework

> Caution:
>
> Substance Compliance no longer requires Teamcenter Integration Framework for connecting with CPM. New **async workflow** is provided for this connection. Teamcenter Integration Framework-CPM connect function from Substance Compliance is now deprecated and will be obsolete soon.

You can install Teamcenter Integration Framework as a standalone instance or install it in an existing Teamcenter environment. A standalone instance of Teamcenter Integration Framework has the advantage that it can be run on a separate host from the Teamcenter server.

If Teamcenter Integration Framework is already installed in your existing Teamcenter environment, you can use the same instance. However, you must modify the framework for installing the integration that is specific to Substance Compliance or if you **upgrade Teamcenter Integration Framework**.

Considerations for installing Dispatcher Server and Dispatcher Client

You can **install Dispatcher Server and Dispatcher Client as a standalone instance** or **install them in an existing Teamcenter environment**.

> Tip:
>
> A standalone instance of Dispatcher Server provides better load balancing.

If Dispatcher Server is already installed in your existing Teamcenter environment, you can use the same instance. However, you must modify it to include the translators that are specific to Substance Compliance.

System requirements for installing Integrated Material Management

See the IMM documentation available on Support Center for IMM system requirements. For details, download the *IMM_*_Documentation ZIP* file available at Support Center > Teamcenter > **Downloads** > **Additional Downloads**. Here, the asterisk (*) refers to the IMM version.

System requirements for installing Compliance Process Manager

See the CPM documentation available on Support Center for CPM system requirements. For details, see *CPM_ServerAdministrators_Guide* available in the *CPM_x.y.z.zip* file. Here, *x.y.z* specifies the major, minor, and patch versions for CPM.

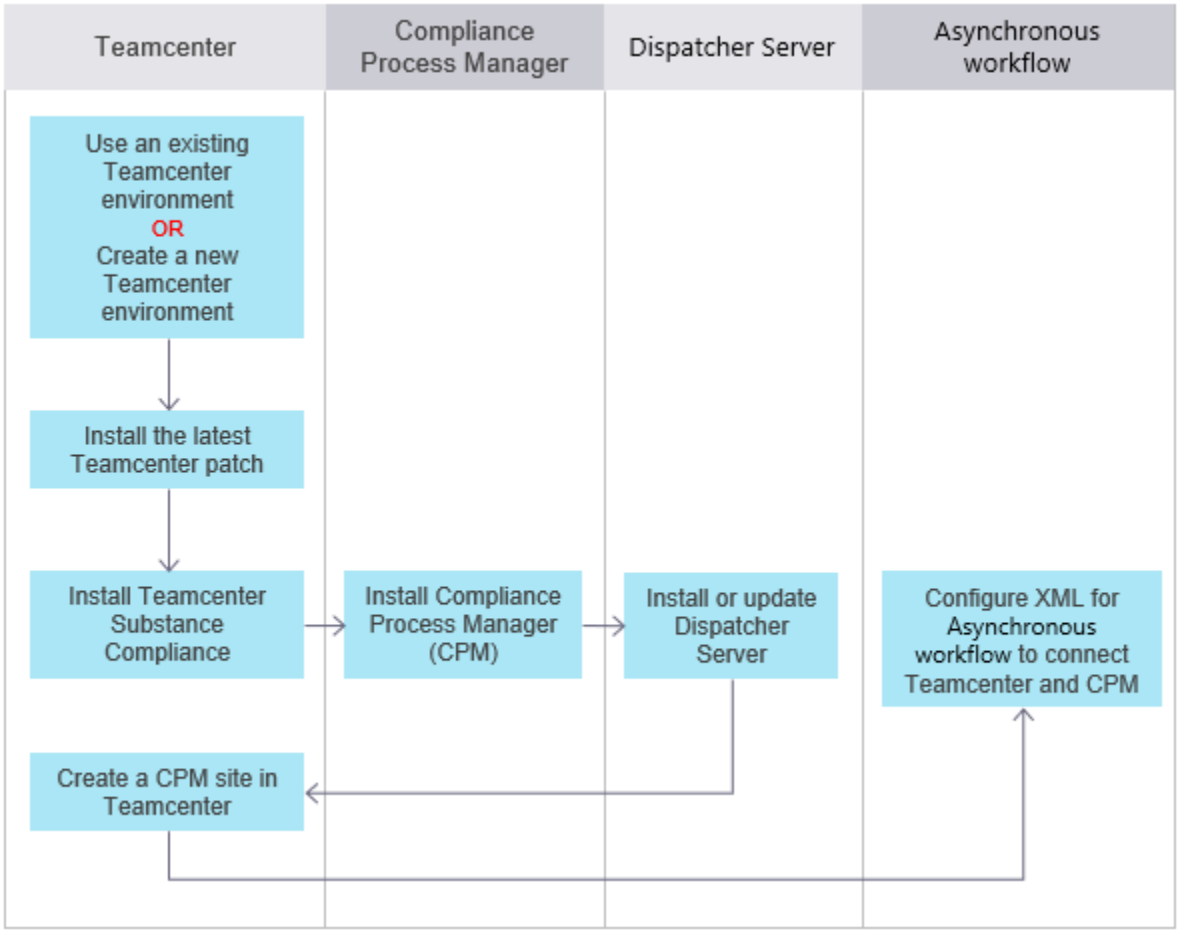
Configure async workflow for connection with CPM

See **async workflow** for configuration of communication parameters.

Checking for compatibility between Teamcenter and the different applications

Verify the compatible version of both IMM and CPM in the *TcSC_CPM_IMM_version_matrix.xlsx* file available at Support Center > **Teamcenter** > **Downloads** > **Substance Compliance CPM**.

4. Substance Compliance deployment workflow



5. Installing Teamcenter Substance Compliance

Install Substance Compliance using TEM

The following procedures assume that you are installing Substance Compliance on an existing Teamcenter set up and that you are familiar with Teamcenter Environment Manager (TEM).

Run TEM and select the following features in the **Features** panel:

- **Extensions→Enterprise Knowledge Foundation→Material Management**
- **Extensions→Supplier Relationship Management→Vendor Management**
- **Extensions→Supplier Relationship Management→Substance Compliance**
- **Extensions→Substances of Concern in Products**
- **Base Install→Active Workspace→Server Extensions→Material Management**
- **Base Install→Active Workspace→Server Extensions→Vendor Management**
- **Base Install→Active Workspace→Server Extensions→Substance Compliance**
- **Base Install→Active Workspace→Client→Material Management**
- **Base Install→Active Workspace→Client→Vendor Management**
- **Base Install→Active Workspace→Client→Substance Compliance**

For more information about installing Teamcenter, see *Teamcenter Installation on Windows Using TEM* or *Teamcenter Installation on Linux Using TEM*.

Install Substance Compliance using Deployment Center

The following procedures assume that you are installing Substance Compliance on an existing Teamcenter and that you are familiar with Deployment Center.

1. Log on to Deployment Center.
2. Select the following applications in the **Applications** task:

Substance Compliance no longer requires Teamcenter Integration Framework for connecting with CPM. New **async workflow** is provided for this connection. Teamcenter Integration Framework-CPM connect function from Substance Compliance is now deprecated and will be obsolete soon.

Application	Description
Material Management	Installs the material and substance database. These materials and substances are associated with the parts used in your company product.
Vendor Management	Provides support for creating and managing vendor information.
Dispatcher	Provides support for Dispatcher Server and Dispatcher Client.
Integration Framework Core	Installs the framework components required to integrate Teamcenter with Compliance Process Manager. Required only if you use TcIF for compliance check.
Integration Framework for Applications	Installs the framework components required to integrate Teamcenter with Compliance Process Manager. Required only if you use TcIF for compliance check.
TcIF Substance Compliance solution	Installs the framework components required to integrate Teamcenter with Compliance Process Manager. Required only if you use TcIF for compliance check.
Substances of Concern in Products	Provides support to identify products that contain hazardous substances above 0.1% weight of the product, which are required to be reported to the European Chemical Agency (ECHA) Substances of Concern in Products (SCIP) database for products.
Substance Compliance	Installs the Substance Compliance application to run a compliance check on parts and assemblies used in your company product. This installs the rich client component of the application.
Substance Compliance for Active Workspace	Installs enhancements to improve the default data model with additional attributes for Active Workspace.

Application	Description
	This installs the Active Workspace component of the application.

3. Go to **Components** and in **Selected Components**, click **Dispatcher Module**.

> Note:
>
> **Dispatcher Module** is visible only if you have selected **Dispatcher** under **Applications** in the earlier step.

4. In the right pane, under **Dispatcher Module**, select all translators available for Substance Compliance.

5. Generate deployment scripts.

For information about using Deployment Center, see *Deployment Center — Usage*.

For more information about installing Teamcenter using Deployment Center, see *Teamcenter Installation Using Deployment Center*.

6. Installing and updating Dispatcher Server and Dispatcher Client

Install Dispatcher Server and Dispatcher Client as a standalone instance

You can install Dispatcher Server and Dispatcher Client together as a standalone instance or **in an existing Teamcenter environment**.

To install a standalone instance of Dispatcher Server and Dispatcher Client:

1. Run Teamcenter Environment Manager (TEM) from the Teamcenter software distribution image. Do not start TEM from the **install** directory of an existing Teamcenter environment.

2. Select the language in the **Installer Language** dialog box.

3. Click **Install** in the **Install/Upgrade Options** panel.

4. Type a new identification and description in the **Configuration** panel, if you do not wish to use the defaults.

5. In the **Solutions** panel, select **Dispatcher (Dispatcher Server)** and click **Next**.

6. In the **Features** panel:

    a. Click **Base Install→Teamcenter Foundation**.

    b. Click **Extensions→Enterprise Knowledge Foundation** and select **Dispatcher Server** and **Dispatcher Client**.

7. Enter information as needed in the subsequent panels.

8. In the **Dispatcher Component** panel:

    a. In **Dispatcher Root Directory**, type or select the Dispatcher root directory. This directory is referred to as *DISP_ROOT*.

    For example, *C:/Program Files/Siemens/Dispatcher*.

    b. Select the **Install Scheduler** check box to install the scheduler.

    c. Select the **Install Module** check box to install the module. On selecting this check box, the **Staging Directory** box is activated.

d. In **Staging Directory**, you can choose the default staging directory or type a new one.

For example, *C:/Program Files/Siemens/Dispatcher/Stage*.

e. Select the **Install Admin Client** check box to install the Admin Client.

f. Click **Next**.

9. In the **Dispatcher Settings** panel:

a. Select the logging level in **Enter logging Level**, for example, **DEBUG**.

b. **Dispatcher Services Log Directory** is automatically populated with the location of the log directory.

c. Select the **Install Documentation** check box to install Javadocs for the Dispatcher components.

d. In **Documentation Install Directory**, type or browse to the location where you want the documentation installed.

For example, *C:/Program Files/Siemens/Dispatcher/Docs*.

e. If you want to start Dispatcher services after installation, select the **Start Dispatcher** check box.

- To start Dispatcher services as a Windows service, click **Windows Service**.
- To start Dispatcher services at the console, click **Console Application**.

f. Click **Next**.

10. In the **Select Translators** panel, select the following and click **Next**:

- **Controller Replication Translators**:
  - **Create AssemblyPLMXML**
  - **PLMXMLBasedSync**
  - **ReplicatePLMXML**
  - **ImportObjects**
- **Spatial Search Indexer→QSearchProcessQueue**

- **Asynchronous Service Translator→AsyncService**
- **Substance Compliance Services**:
  - **Compliance Results Validation**
  - **Supplier Declaration Validation**
  - **Supplier Declaration Import**
  - **Supplier Declaration Re-Request**
- **Email Polling→Email Polling**.

11. In the **Dispatcher Client** panel:

    a. Choose the **Dispatcher Server Connection Type** option. This option allows you to choose how Dispatcher Client communicates between Teamcenter and the Dispatcher components.

       - Select **RMI** for communicating using the RMI mode, which is faster than the web server mode.
       - Select **WebServer** if sending translation requests over a firewall.

    b. In **Dispatcher Server Hostname**, type the name of the server where the translation server will be hosted, for example, *localhost*.

    c. In **Dispatcher Server Port**, type the port to be used for Dispatcher Server. The default port number is **2001** if the Dispatcher connection type is **RMI** and **8080** if the Dispatcher connection type is **WebServer**.

       In the RMI mode, the scheduler port is used and in the web server mode, the web server port is used.

       Ensure that the port you choose is not used by any other process.

    d. In **Staging Directory**, type or browse to the location to be used as the staging directory for Dispatcher Client.

    e. In **Dispatcher Client Proxy User Name**, type the user name for the proxy user.

    f. In **Dispatcher Client Proxy Password**, type the password for the proxy user.

    g. In **Polling interval in seconds**, type the time duration (in seconds) for which Dispatcher Client should wait before querying for Dispatcher requests, for example, *60*.

h. In **Do you want to store JT files in Source Volume?**, select **Yes** if you want to store visualization files in the associated visualization dataset.

i. Click **Next**.

12. In the **Dispatcher Client** panel:

a. Select the logging level in the **Enter Logging Level** list.

b. The **Dispatcher Client Log Directory** is automatically populated with the location of the log directory.

c. In the **Advanced Settings** section:

A. In the **Do you want to Update Existing Visualization Data?** box, select **Yes** to update the existing visualization data to the latest version.

B. In the **Deletion of successful translation in minutes** box, specify the time duration (in minutes) that the Dispatcher Client should wait before querying and deleting successful translation request objects. For example, *60* seconds.

If the interval is set to **0**, the translation request cleanup will not be carried out.

C. In **Threshold time in minutes for successful translation deletion**, specify the time duration, in minutes (for example, *480*) that must pass after a successful translation request object is last modified before it can be deleted.

D. In **Deletion of unsuccessful translation in minutes**, specify the time duration, in minutes (for example, *120*) for which Dispatcher Client should wait before querying and deleting the unsuccessful translation request objects.

E. In **Threshold time in minutes for unsuccessful translation deletion**, specify the time duration, in minutes (for example, *2880*) that must pass after an unsuccessful translation request object is last modified before it can be deleted.

d. Click **Next**.

13. In the **Database Template Summary** panel, click **Next**.

14. In the **Confirmation** panel, click **Start**.

Install Dispatcher Server and Dispatcher Client in an existing Teamcenter environment

You can install Dispatcher Server and Dispatcher Client together as a **standalone instance** or in an existing Teamcenter environment.

To install a Dispatcher Server and Dispatcher Client in an existing Teamcenter environment:

1. Run Teamcenter Environment Manager (TEM) from your *TC_ROOT***install** directory.
   The *TC_ROOT* directory is the folder where you have installed Teamcenter, for example: *c:\Program Files\Siemens\Teamcenter2412\install*

2. In the **Maintenance** panel, select **Configuration Manager** and click **Next**.

3. In the **Configuration Maintenance** panel, select **Perform maintenance on an existing configuration** and click **Next**.

4. In the **Old Configuration** panel, select an existing configuration on which you want to install Substance Compliance and click **Next**.

5. In the **Feature Maintenance** panel, select **Add/Remove Features** and click **Next**.

6. In the **Features** panel, expand **Extensions→Enterprise Knowledge Foundation** and select **Dispatcher Server** and **Dispatcher Client**.

7. Enter the relevant information in the subsequent panels.

8. In the **Dispatcher Component** panel:

   a. In **Dispatcher Root Directory**, type or select the Dispatcher root directory. This directory is referred to as *DISP_ROOT*.

      For example, *C:/Program Files/Siemens/Dispatcher*.

   b. Select the **Install Scheduler** check box to install the scheduler.

   c. Select the **Install Module** check box to install the module. On selecting this check box, the **Staging Directory** box is activated.

   d. In **Staging Directory**, you can choose the default staging directory or type a new one.

      For example, *C:/Program Files/Siemens/Dispatcher/Stage*.

   e. Select the **Install Admin Client** check box to install the Admin Client.

   f. Click **Next**.

9. In the **Dispatcher Settings** panel:

   a. Select the logging level in **Enter logging Level**, for example, **DEBUG**.

   b. In **Dispatcher Services Log Directory**, provide the path for Dispatcher log files.

c. Select the **Install Documentation** check box to install Javadocs for the Dispatcher components.

d. In **Documentation Install Directory**, type or browse to the location where you want the documentation installed.

For example, *C:/Program Files/Siemens/Dispatcher/Docs*.

e. If you want to start Dispatcher services after installation, select the **Start Dispatcher** check box.

- To start Dispatcher services as a Windows service, click **Windows Service**.
- To start Dispatcher services from the console, click **Console Application**.

f. Click **Next**.

10. In the **Select Translators** panel, select the following and click **Next**:

- **Controller Replication Translators→Create AssemblyPLMXML**, **PLMXMLBasedSync**, **ReplicatePLMXML**, and **ImportObjects**.
- **Spatial Search Indexer→QSearchProcessQueue**
- **Asynchronous Service Translator→AsyncService**
- **Substance Compliance Services→Compliance Results Validation**, **Supplier Declaration Validation**, **Supplier Declaration Import**, and **Supplier Declaration Re-Request**.
- **Email Polling→Email Polling**.

11. In the **Dispatcher Client** panel:

a. Choose the **Dispatcher Server Connection Type** option, This option allows you to choose how Dispatcher Client communicates between Teamcenter and the Dispatcher components.

- Select **RMI** for communicating using the RMI mode, which is faster than the web server mode.
- Select **WebServer** if sending translation requests over a firewall.

b. In **Dispatcher Server Hostname**, type the name of the server where the translation server will be hosted.

c. In **Dispatcher Server Port**, type the port to be used for Dispatcher Server. The default port number is **2001** if the Dispatcher connection type is **RMI** and it is **8080** if the Dispatcher connection type is **WebServer**.

   In the RMI mode, the scheduler port is used and in the web server mode, the web server port is used.

   Ensure that the port you choose is not used by any other process.

d. In **Staging Directory**, type or browse to the location to be used as the staging directory for Dispatcher Client.

e. In **Dispatcher Client Proxy User Name**, type the user name for the proxy user.

f. In **Dispatcher Client Proxy Password**, type the password for the proxy user.

g. In **Polling interval in seconds**, type the time duration (in seconds) for which Dispatcher Client should wait before querying for Dispatcher requests.

h. In **Do you want to store JT files in Source Volume?**, select **Yes** if you want to store visualization files in the associated visualization dataset.

i. Click **Next**.

12. In the **Dispatcher Client** panel:

    a. Select the logging level from the **Enter Logging Level** list.

    b. The **Dispatcher Client Log Directory** is automatically populated with the location of the log directory.

    c. In the **Advanced Settings** section:

       A. In **Do you want to Update Existing Visualization Data?**, select **Yes** if you want to update the existing visualization data to the latest version.

       B. In **Deletion of successful translation in minutes**, specify the time duration (in minutes) for which Dispatcher Client should wait before querying and deleting successful translation request objects.
       If the interval is set to **0**, the translation request cleanup will not be done.

       C. In **Threshold time in minutes for successful translation deletion**, specify the time duration (in minutes) that must pass after a successful translation request object is last modified before it can be deleted.

D. In **Deletion of unsuccessful translation in minutes**, specify the time duration (in minutes) for which Dispatcher Client should wait before querying and deleting the unsuccessful translation request objects.

E. In **Threshold time in minutes for unsuccessful translation deletion**, specify the time duration (in minutes) that must pass after an unsuccessful translation request object is last modified before it can be deleted.

d. Click **Next**.

13. In the **Confirmation** panel, click **Start**.

Update the existing Dispatcher Server for Substance Compliance

If Dispatcher Server is already installed in your existing Teamcenter environment, you can use the same instance. However, you must modify it to include the translators that are specific to Substance Compliance.

To modify the existing Dispatcher Server:

1. Run Teamcenter Environment Manager (TEM) from your *TC_ROOT***install** directory.
The *TC_ROOT* directory is the folder where you have installed Teamcenter, for example, *c:\Program Files\Siemens\Teamcenter2412\install*.

2. In the **Maintenance** panel, select **Configuration Manager** and click **Next**.

3. In the **Configuration Maintenance** panel, select **Perform maintenance on an existing configuration** and click **Next**.

4. In the **Old Configuration** panel, select an existing configuration on which you want to install Substance Compliance and click **Next**.

5. In the **Feature Maintenance** panel, select **Dispatcher Server→Modify Dispatcher Settings** and click **Next**.

6. In the **Features** panel, expand **Extensions→Enterprise Knowledge Foundation** and select **Dispatcher Server**.

7. Enter information as needed in the subsequent panels.

8. In the **Dispatcher Component** panel:

a. In **Dispatcher Root Directory**, type or select the Dispatcher root directory, for example, *C:\Program Files\Siemens\Dispatcher*.

Keep this directory close to the Teamcenter root directory. This directory is referred to as *DISP_ROOT*.

b. Select the **Install Scheduler** check box to install the scheduler.

c. Select the **Install Module** check box to install the module. On selecting this check box, the **Staging Directory** box is activated.

d. In **Staging Directory**, you can choose the default staging directory or type a new one, for example, *C:\Program Files\Siemens\Dispatcher*.

e. Select the **Install Admin Client** check box to install the Admin Client.

f. Click **Next**.

9. In the **Dispatcher Settings** panel:

a. Select the logging level in **Enter logging Level**, for example, **DEBUG**.

b. The **Dispatcher Services Log Directory** is automatically populated with the location of the log directory.

c. Select the **Install Documentation** check box to install Javadocs for the Dispatcher components.

d. In **Documentation Install Directory**, type or browse to the location where you want the documentation installed for example, *C:\Program Files\Siemens\Dispatcher\Docs*.

e. If you want to start Dispatcher services after installation, select the **Start Dispatcher** check box.

- To start Dispatcher services as a Windows service, click **Windows Service**.
- To start Dispatcher services at the console, click **Console Application**.

f. Click **Next**.

10. In the **Select Translators** panel, select the following and click **Next**:

- **Controller Replication Translators→Create AssemblyPLMXML**, **PLMXMLBasedSync**, **ReplicatePLMXML**, and **ImportObjects**.
- **Spatial Search Indexer→QSearchProcessQueue**
- **Asynchronous Service Translator→AsyncService**

- **Substance Compliance Services→Compliance Results Validation**, **Supplier Declaration Validation**, **Supplier Declaration Import**, and **Supplier Declaration Re-Request**.

- **Email Polling→Email Polling**.

11. In the **Dispatcher Client** panel:

    a. Choose the **Dispatcher Server Connection Type** option. This option allows you to choose how Dispatcher Client communicates between Teamcenter and the Dispatcher components.

       - Select **RMI** for communicating using the RMI mode, which is faster than the web server mode.

       - Select **WebServer** if sending translation requests over a firewall.

    b. In **Dispatcher Server Hostname**, type the name of the server where the translation server will be hosted.

    c. In **Dispatcher Server Port**, type the port to be used for Dispatcher Server. The default port number is **2001** if the Dispatcher connection type is **RMI**, and it is **8080** if the Dispatcher connection type is **WebServer**.

       In the RMI mode, the scheduler port is used and in the web server mode, the web server port is used.

       Ensure that the port you choose is not used by any other process.

    d. In **Staging Directory**, type or browse to the location to be used as the staging directory for Dispatcher Client.

    e. In **Dispatcher Client Proxy User Name**, type the user name for the proxy user.

    f. In **Dispatcher Client Proxy Password**, type the password for the proxy user.

    g. In **Polling interval in seconds**, type the time duration (in seconds) for which Dispatcher Client should wait before querying for Dispatcher requests.

    h. In **Do you want to store JT files in Source Volume?**, select **Yes** if to store visualization files in the associated visualization dataset.

    i. Click **Next**.

12. In the **Dispatcher Client** panel:

    a. Select the logging level from the **Enter Logging Level** list.

b. The **Dispatcher Client Log Directory** is automatically populated with the location of the log directory.

c. In the **Advanced Settings** section:

   A. In **Do you want to Update Existing Visualization Data?**, select **Yes** if you want to update the existing visualization data to the latest version.

   B. In **Deletion of successful translation in minutes**, specify the time duration (in minutes) for which Dispatcher Client should wait before querying and deleting successful translation request objects.
   If the interval is set to **0**, the translation request cleanup will not be done.

   C. In **Threshold time in minutes for successful translation deletion**, specify the time duration (in minutes) that must pass after a successful translation request object is last modified before it can be deleted.

   D. In **Deletion of unsuccessful translation in minutes**, specify the time duration (in minutes) for which Dispatcher Client should wait before querying and deleting the unsuccessful translation request objects.

   E. In **Threshold time in minutes for unsuccessful translation deletion**, specify the time duration (in minutes) that must pass after an unsuccessful translation request object is last modified before it can be deleted.

d. Click **Next**.

13. In the **Confirmation** panel, click **Start**.

7. Install Compliance Process Manager

To install Compliance Process Manager (CPM), refer to the *CPM Administrators guide*. To access this guide:

1. Search for **CPM** on Support Center.

2. Download the zip file of the CPM version compatible with your Teamcenter version.

3. Navigate to the folder where you downloaded the CPM ZIP file and open the **doc** folder to access the *CPM Administrators guide*.

8. Configure parameters for asynchronous workflow to communicate with CPM

To establish communication with CPM, an asynchronous workflow must be configured using an *XML* file. After you update the configuration parameters in this file, the next time you perform a compliance check, the changes take effect and a connection is established with CPM.

Procedure

1. Modify and save *%TC_DATA%\subscmpl_data\config\subscmplComplianceConfiguration.xml* file with values according to your environment.

   Caution:

   Ensure the following points:

   You must modify this original file and not create a new copy and edit it.

   During a Teamcenter upgrade, you must back up this file to avoid rework.

9. Install or upgrade Teamcenter Integration Framework

Caution:

Substance Compliance no longer requires Teamcenter Integration Framework for connecting with CPM. New **async workflow** is provided for this connection. Teamcenter Integration Framework-CPM connect function from Substance Compliance is now deprecated and will be obsolete soon.

You can install Teamcenter Integration Framework as a standalone instance or in an existing Teamcenter environment. The standalone instance has an advantage in that it can be run on a host separate from the Teamcenter server. See *Installing and upgrading Teamcenter Integration Framework* in the Teamcenter Integration Framework documentation for installation details.

To upgrade, see *Upgrading and patching Teamcenter Integration Framework* in the Teamcenter Integration Framework documentation.

Tasks to perform for Substance Compliance when you upgrade to a new version of Teamcenter Integration Framework

When you upgrade to a new version of Teamcenter Integration Framework, you must manually restore some files specific to Substance Compliance and Compliance Process Manager that are saved in the Teamcenter Integration Framework datastore. An upgrade saves (or backs up) these solution-specific files in the *TCIF_ROOT/container/migrate* directory during the upgrade process.

The following are some of the files backed up in the *TCIF_ROOT/container/migrate/run/<unique_id>* directory:

- *LocalOldDS.zip*: A full backup of the previous Teamcenter Integration Framework datastore
- *LocalNewDS_initial.zip*: A snapshot of the new Teamcenter Integration Framework datastore with initial files

See *Resolve Teamcenter Integration Framework datastore migration conflicts* in the Teamcenter Integration Framework documentation for the complete list of files that are backed up.

To restore the Substance Compliance solution files:

1. Extract the files from *LocalOldDS.zip* and *LocalNewDS_initial.zip* in their respective directories.

   In case of a Teamcenter Integration Framework cluster upgrade, extract the files from the *ClusterOldDS.zip* and *ClusterNewDS_initial.zip* files.

2. Both directories contain a *config* and a *bos* directory with the following files.

config	*bos*
TCCPM_solutionConfig.jaxb	TeamcenterSoaCommercialPart.jaxb
cpm_graded_to_tcxml.xsl	
TCCPM_mapping.xsl	

Make sure *cpm_graded_to_tcxml.xsl* and *TCCPM_mapping.xsl* are picked from the location *TC_DATA/subcmpl_data/subsCmplDataStore/config* before upload.

Merge these files from the *LocalOldDS\config* and *LocalOldDS\bos* directories with the files from the *LocalNewDS_initial\config* and *LocalNewDS_initial\bos* directories and save the files in a directory.

3. Upload the merged files to the Teamcenter Integration Framework datastore:

   a. Start the Teamcenter Integration Framework web client.

   b. Click **Configure→Data Store** to open the **Configuration objects** web page.

   c. Click **Browse** and choose the merged files from the **Select a Location** list and click **Upload.**

10. Integrating Teamcenter and Compliance Process Manager

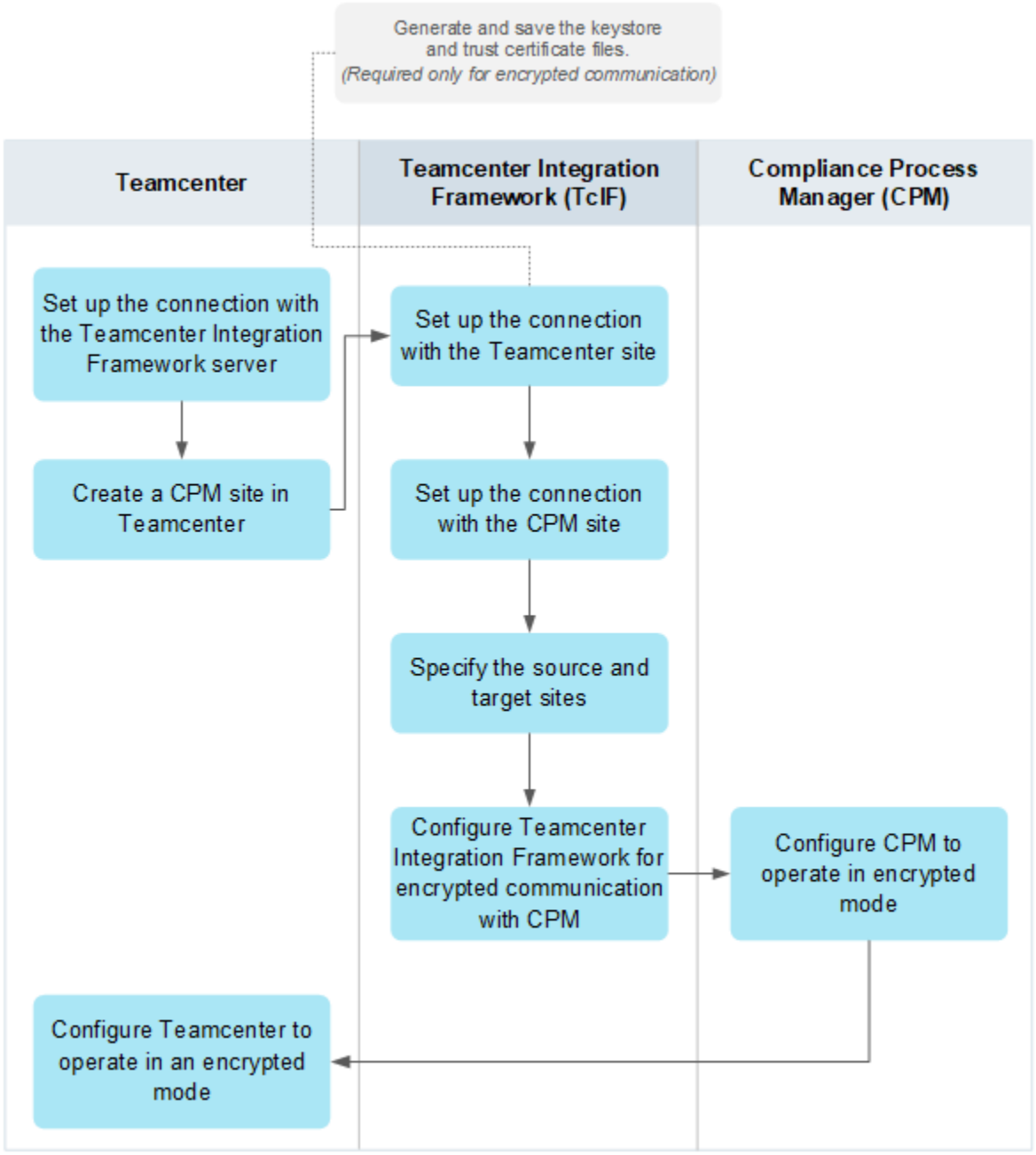
Workflow to integrate Teamcenter and Compliance Process Manager

> Caution:
>
> Substance Compliance no longer requires Teamcenter Integration Framework for connecting with CPM. New **async workflow** is provided for this connection. Teamcenter Integration Framework-CPM connect function from Substance Compliance is now deprecated and will be obsolete soon.

Teamcenter must communicate with Compliance Process Manager (CPM) to verify if a part conforms to certain environmental regulations. For this communication, you must integrate Teamcenter with CPM, using Teamcenter Integration Framework. You can establish this communication using either the HTTP or the HTTPS protocol.

For integrating the two applications, you require the values of certain Teamcenter, CPM, and Teamcenter Integration Framework attributes.

> Tip:
>
> For ease of access later, record these values in a **worksheet**.



Record values required to integrate Teamcenter and CPM

Attribute	Where to find	Sample value	Your value
Teamcenter host name	The computer on which Teamcenter is installed.	*Tc_host*	
Teamcenter site ID	*TC_ROOT/fsc/fmsmaster_FSC_xxxx.xml* where *TC_ROOT* is the folder where	*-1449123733*	

Attribute	Where to find	Sample value	Your value
	Teamcenter is installed, for example, *C:/Program Files/Siemens/Teamcenter2412*. Note the value of the **id** attribute of the **fmsenterprise** element.		
FMS ID	*TC_ROOT/fsc/fmsmaster_FSC_xxxx.xml* Note the value of the **id** attribute of the **fsc** element.	*FSC_Tc_host_yytcadm*	
FMS URL	*TC_ROOT/fsc/fmsmaster_FSC_xxxx.xml* Note the value of the **address** attribute of the **fsc** element.	*http://Tc_host:FSC_port*	
CPM host name	The computer on which CPM is installed.	*CPM_host*	
CPM site ID	The CPM site created in the Teamcenter Organization application. Note the value of **Site ID**.	*-90000*	
CPM port number	*CPM_ROOT/conf/server.xml*, where *CPM_ROOT* is the folder where CPM is installed, for example, *D:/CPM*. Note the value of the **HTTP/1.1** protocol.	*8080*	
Teamcenter Integration Framework host name	The computer on which Teamcenter Integration Framework is installed.	*TcIF_host*	
Teamcenter Integration Framework web UI port number	*TC_ROOT/tcif/container/etc/system.properties* or *TCIF_ROOT/tcif/container/etc/system.properties* The standalone instance is installed in the *TCIF_ROOT* folder, for example, D:/TCIF. If installed in an existing Teamcenter environment, it is located in the *TC_ROOT/tcif* folder. Note the value of **webui.port**.	*8040*	

Attribute	Where to find	Sample value	Your value
Teamcenter Integration Framework REST services port number	*TC_ROOT/tcif/container/etc/system.properties* or *TCIF_ROOT/tcif/container/etc/system.properties* Note the value of **restservices.port**.	*8090*	
Teamcenter Integration Framework web services port number	*TC_ROOT/tcif/container/etc/system.properties* or *TCIF_ROOT/tcif/container/etc/system.properties* Note the value of **webservices.port**.	*8080*	
Teamcenter Integration Framework URL	http://TcIF_host:TcIF_web_UI_port/tcif/controller/webclient	*http://Tc_host:8040/tcif/controller/webclient*	
Teamcenter Integration Framework SSL certificate path	The value of the **SUBSCMPL_ssl_cert_full_file_path** preference in Teamcenter.	*%TC_DATA%\subscmpl_data\config\vc6s004.cer*	

Set up the connection with the Teamcenter Integration Framework server in Teamcenter

When a substance compliance check is initiated from Teamcenter, the compliance check request is sent to Teamcenter Integration Framework using either the HTTP or the HTTPS protocol. Based on the preference of your organization, the communication mechanism between Teamcenter and Teamcenter Integration Framework is either a socket based (non-SSL) protocol or a curl-based (SSL) protocol.

To send the compliance check request, you must specify where the Teamcenter Integration Framework server resides and its REST services port number. To specify these values, you must update the Teamcenter site properties and the **SUBSCMPL_compliance_check_url** preference.

Update the Teamcenter site properties

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

2. Select the home Teamcenter site that must connect to Teamcenter Integration Framework, for example, **-1449123733**.

3. In the **Sites** pane, in **Site Node/URL**, type the name of the computer on which the Teamcenter site is hosted, for example, **Tc_host**.

4. In **SOA URL**, type the Service Oriented Architecture (SOA) URL, for example, **http://Tc_host:7001/tc**, where *tc* is the WAR file name.

5. Click **Modify**.

Update the compliance check URL

1. In My Teamcenter, click **Edit→Options**.
2. In the **Options** dialog box, click **Filters**.
3. Verify the values of the following preferences and update if required.
   a. Type the name of the preference in **Filters→Search by preference name**.
   b. Select the preference and click **Edit**.

Preference	Value
GS_USER_NAME	IFAdmin
GS_USER_PASSWORD	admin
SUBSCMPL_compliance_-check_url	Caution: • To avoid any compliance check issues, the value of the **SUBSCMPL_compliance_check_url** preference must be set to the one provided here based on whether your organization uses non-SSL or SSL communication. • Ensure that no characters in the URL are converted to a different value when updating the preference value. For example, ensure that the ampersand (&) is not converted to *&amp* when you update the value of the preference. • Additionally, ensure that the password you provide in the compliance check URL follows URL encoding standards. For example, characters such as percentage (%), ampersand (&), and a question mark (?) must not be used in the password. If such characters are used, Teamcenter Integration Framework does not interpret the value of the password in the compliance check URL correctly. For non-SSL or socket-based communication, use: GET http://TcIF_host:TcIF_host_port/tcif/publish?-publisher=test&type=complianceCheck&-j_username=IFAdmin&j_password=TCIF_USER_PASSWORD&source_attr_names=-sourceSid%5E%5EUID%5E%5EItemId%-

Preference	Value
	5E%5ERevision%5E%5EType%5E%5Eregulations%- 5E%5EOwner%5E%5EOptionset%5E%- 5ETransfermode%5E%5Erevrule%5E%- 5EsvruleUID%5E%5EprocessUnconfiguredByOccEff%- 5E%5EprocessSuppressedOcc%5E%- 5EprocessUnconfiguredVariants%5E%- 5EprocessUnconfiguredChanges%5E%- 5ESSOUserID%5E%5ESSOSessionKey%- 5E%5ENotifiers&source_attr_values=- SOURCESID%5E%5EITEMUID%5E%- 5EITEMID%5E%5EITEMREVISION%5E%- 5EITEMREVTYPE%5E%5EREGULATION%- 5E%5EOWNER%5E%5EOPTIONSET%5E%- 5ETRANSFERMODE%5E%5EREVRULE%5E%5ESVRULEUID%5E%- 5EPROCESSUNCONFIGUREDBYOCCEFF%- 5E%5EPROCESSSUPPRESSEDOCC%- 5E%5EPROCESSUNCONFIGUREDVARIANTS%- 5E%5EPROCESSUNCONFIGUREDCHANGES%- 5E%5ESSOUSERID%5E%5ESSOSESSIONKEY%- 5E%5ENOTIFIERSLIST&output=xml HTTP/1.1\nConnection: keep-Alive\nHost: TcIF_host\nContent-Type: text/xml\nCache- Control: no-cache\n\n Here, *TcIF_host* is replaced with the name of the computer that hosts Teamcenter Integration Framework, and *TcIF_host_port* is replaced with the REST services port number. For SSL or curl-based communication, use: https://TcIF_host:TcIF_host_port/tcif/publish?- publisher=test&type=complianceCheck&j_username =IFAdmin&j_password=TCIF_USER_PASSWORD&- source_attr_names=sourceSid%5E%5EUID%- 5E%5EItemId%5E%5ERevision%5E%5EType%- 5E%5Eregulations%5E%5EOwner%5E%- 5EOptionset%5E%5ETransfermode%5E%- 5Erevrule%5E%5EsvruleUID%5E%- 5EprocessUnconfiguredByOccEff%5E%- 5EprocessSuppressedOcc%5E%- 5EprocessUnconfiguredVariants%5E%- 5EprocessUnconfiguredChanges%5E%- 5ESSOUserID%5E%5ESSOSessionKey%- 5E%5ENotifiers&source_attr_values=- SOURCESID%5E%5EITEMUID%5E%- 5EITEMID%5E%5EITEMREVISION%- 5E%5EITEMREVTYPE%5E%5EREGULATION%- 5E%5EOWNER%5E%5EOPTIONSET%- 5E%5ETRANSFERMODE%5E%5EREVRULE%- 5E%5ESVRULEUID%5E%-

Preference	Value
	5EPROCESSUNCONFIGUREDBYOCCEFF%- 5E%5EPROCESSSUPPRESSEDOCC%- 5E%5EPROCESSUNCONFIGUREDVARIANTS%- 5E%5EPROCESSUNCONFIGUREDCHANGES%- 5E%5ESSOUSERID%5E%5ESSOSESSIONKEY%- 5E%5ENOTIFIERSLIST&output=xml
SUBSCMPL_ssl_cert_full_file_path	Note: Use this preference only when you want to operate in the SSL communication mode. The full path (including the file name) of the trust certificate stored on the Teamcenter host *%TC_DATA%\subscmpl_data\config\vc6s004.cer*
SUBSCMPL_compliance_-server_host	The host name of the Teamcenter Integration Framework server *TcIF_host* Note: For SSL configuration, ensure that the host name specified in certification generation is exactly the same as the one used in the compliance check URL. The host name is case sensitive.
SUBSCMPL_compliance_-server_port	*restservices.port*
TC_SSO_GS_APP_ID	Note: Use this preference only for an SSO configuration. TcIF Note: Substance Compliance assumes that the **TC_SSO_SERVICE** environment variable contains a valid value. Only then does the system use the value of the **TC_SSO_GS_APP_ID** preference to generate an SSO token.

Preference	Value
SUBSCMPL_regulation_-creator_groups	dba
SUBSCMPL_regulation_-creator_roles	DBA
TC_gms_server	The Teamcenter Integration Framework server URL location for Global Multi-Site (GMS) http://*TcIF_host*:*TcIF_host_port*/tcif
TCIF_url	http://*TcIF_host*:*TcIF_host_port*/tcif

4. Click **Save** and then click **Close**.

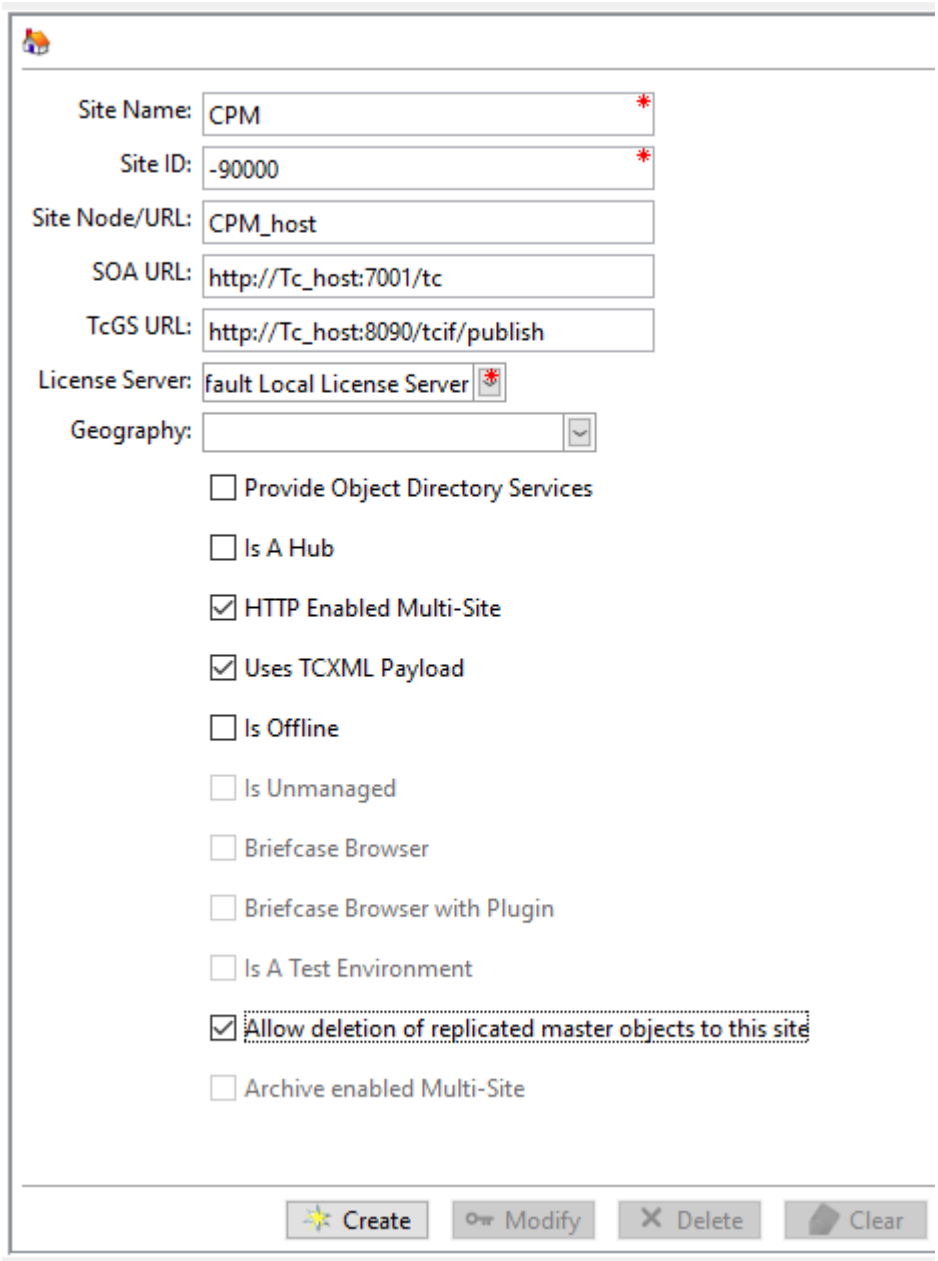
Create a Compliance Process Manager site in Teamcenter

For Teamcenter to interact with Compliance Process Manager (CPM), a site must be created for CPM using the Teamcenter Organization application. The site ID you enter while creating the CPM site is also required when you configure the CPM site later. Note down this site ID in the **installation worksheet**.

To create a site:

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

2. In the **Sites** pane, in **Site Name**, type a descriptive name for the site, for example, **CPM**.



3. In **Site ID**, type a unique identifier. The site ID must be an integer, for example, **-90000**.

4. In **Site Node/URL**, type the name of the computer on which the CPM site is hosted, for example, **CPM_host**.

5. In **SOA URL**, type the Service Oriented Architecture (SOA) URL, for example, **http://Tc_host:7001/tc**.

6. In **TcGS URL**, type the URL for your Teamcenter Integration Framework web server, for example, **http://Tc_host:8090/tcif/publish**. Here, *8090* is the REST services port number. To obtain this port

number, navigate to the *TC_ROOT/tcif/container/etc* folder and open the *system.properties* file. Note the value of **restservices.port**.

7. Select the **License Server**. By default, there is a local license server.

8. Select the **HTTP Enabled Multi-Site** check box to indicate that the site is enabled for Multi-Site Collaboration.

9. Select the **Uses TCXML Payload** check box to indicate that the site uses TC XML payload instead of an object manager.

10. Select the **Allow deletion of replicated master objects to this site** check box to allow replicated master objects to this site.

11. Click **Create**.

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

Set up the connection with the Teamcenter site in Teamcenter Integration Framework

You must provide information about the Teamcenter site from which Teamcenter Integration Framework must fetch the data to be exchanged with Compliance Process Manager (CPM). To do this, in Teamcenter Integration Framework, you must create the Teamcenter site.

1. Navigate to the *TC_ROOT/tcif/container/bin* and run the *trun.bat* file to start Teamcenter Integration Framework. Here, *TC_ROOT* is the directory where Teamcenter Integration Framework is installed. An example is *C:/Program Files/Siemens/Teamcenter2412*.

2. Open the Teamcenter Integration Framework web console by typing the following URL in a browser:

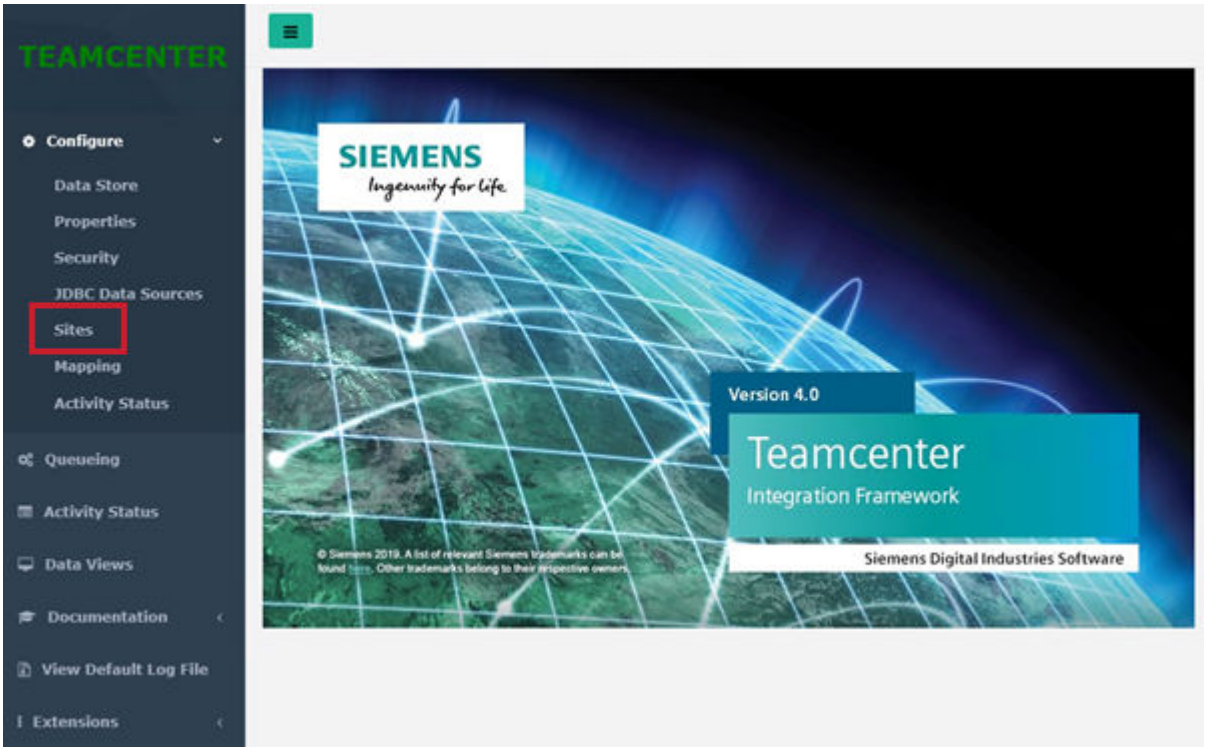
   `http://TcIF_host:TcIF_port/tcif/rest/login`

   Here, *TcIF_host* is the name of the computer that hosts Teamcenter Integration Framework. In addition, *TcIF_port* is the web UI port number of Teamcenter Integration Framework, for example, **http://Tc_host:8090/tcif/rest/login**.

   To obtain the web UI port number, navigate to the *TC_ROOT/tcif/container/etc* folder and open the *system.properties* file. Note the value of **restservices.port**.

   Enter the credentials to log on. By default, the **User ID** and **Password** are **IFAdmin** and **admin**, respectively.

3. Click **Configure** → **Sites**.

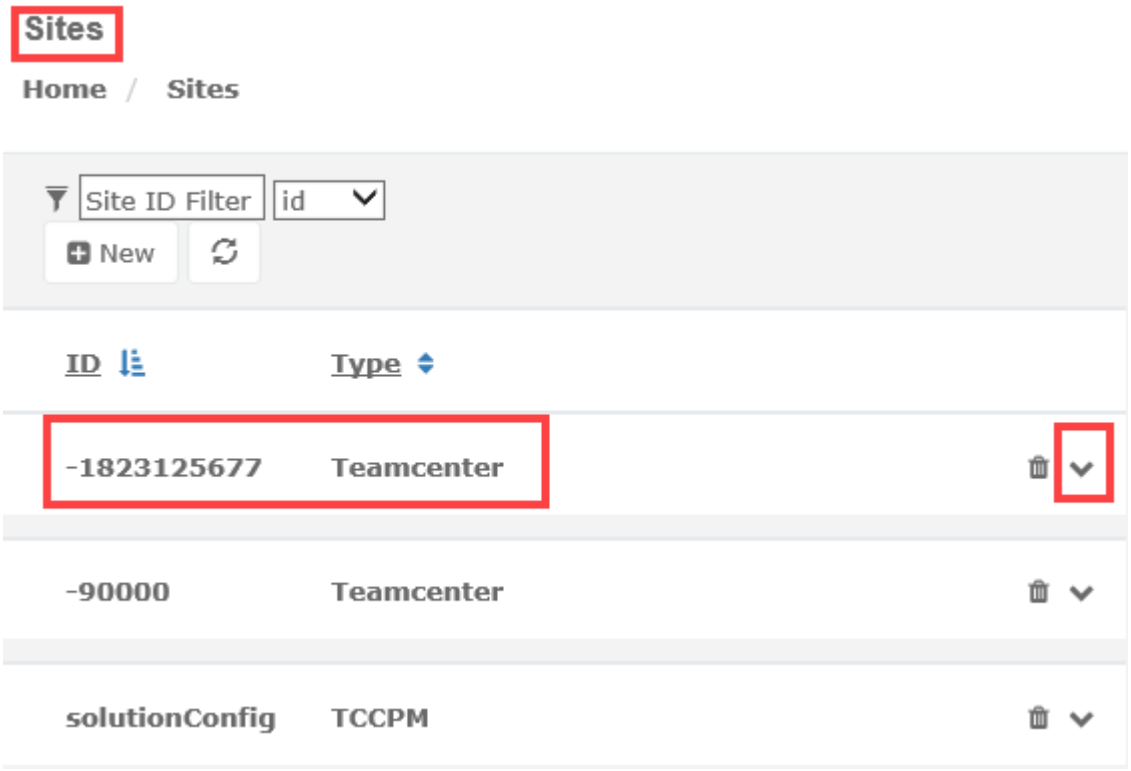


4. On the **Sites** page, click **New**.

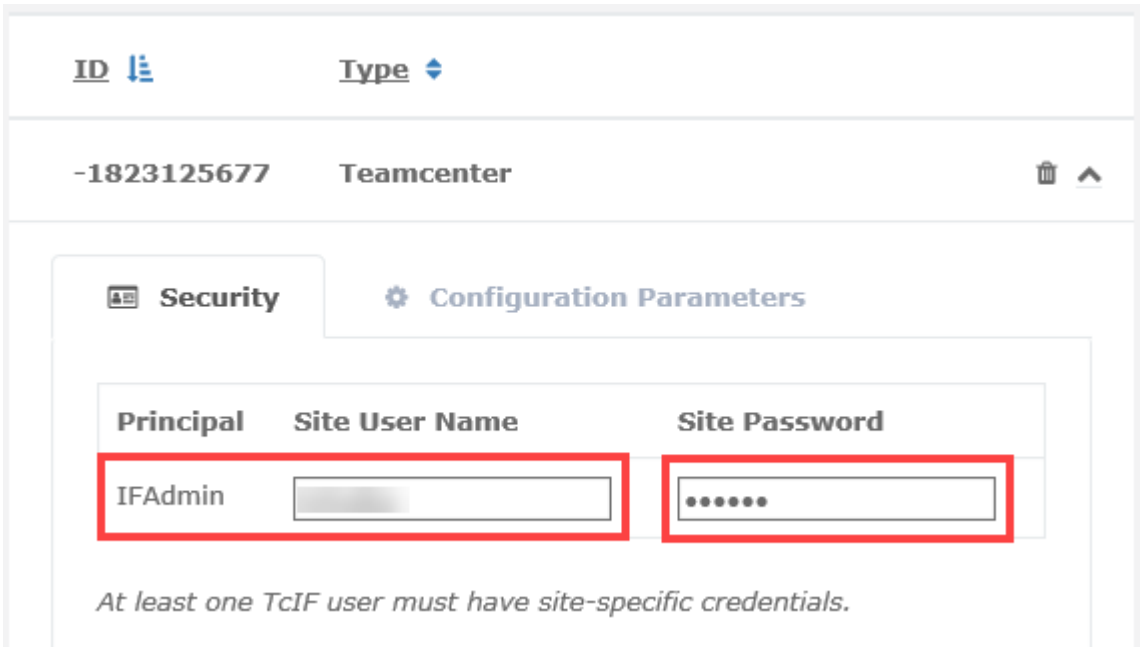
5. Enter the Teamcenter site ID in **ID** , and select **Teamcenter** in **Site Type**.

6. Click **Create**.

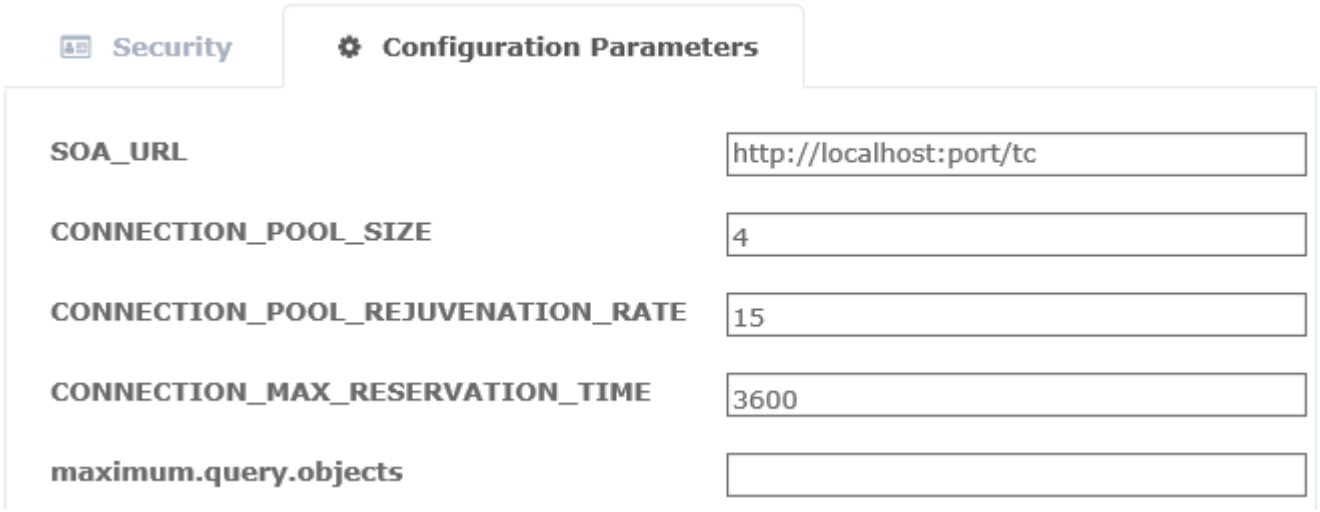
7. On the **Sites** page, expand the Teamcenter site ID section.



8. On the **Sites** page → **Security** tab, enter the Teamcenter administrative user credentials in **Site User Name** and **Site Password**.



9. In the **Configuration Parameters** tab, verify that the values appear correctly.



Ensure that *localhost:port* specify the correct Teamcenter host and port number.

10. Click **Save**.

11. (Optional) To configure Teamcenter Integration Framework for HTTPS (encrypted) communication with Teamcenter:

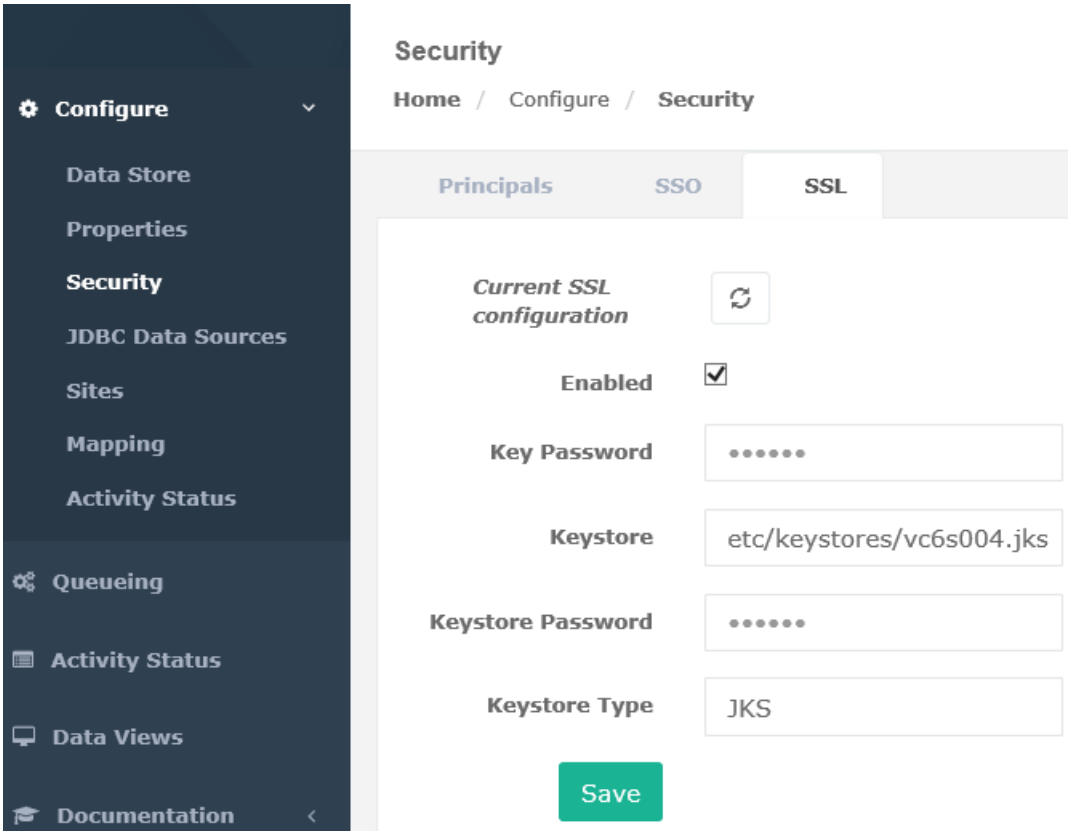
    a. Copy the keystore (*.jks*) file from your local machine to the Teamcenter Integration Framework server.

       For example, copy the *vc6s004.jks* keystore file to the *C:\apps\tc\tc2412\TR\tcif\container\etc\keystores* folder.

    b. Click **Configure** → **Security**.

    c. On the **Security** page, click the **SSL** tab.

    d. Select the **Enabled** check box to specify that Teamcenter Integration Framework must use an HTTPS communication.



e. Provide the values for **Key Password** and **Keystore Password**.

For details about the values to provide here, see the *SSL* documentation in the Teamcenter Integration Framework help.

f. In **Keystore**, specify the location of the repository for the security certificates used for SSL encryption and the name of the certificate.

This is the file that you copied in **step a**, for example, *C:\apps\tc\tc2412\TR\tcif\container\etc\keystores\vc6s004.jks*.

g. Set the **Keystore Type**. As Teamcenter Integration Framework is Java-based, the default is JKS. Another commonly used keystore type is PKCS#12, which is not Java-specific.

h. Click **Save**.

i. Restart Teamcenter Integration Framework to ensure that the configuration is saved.

Set up the connection with the CPM site in Teamcenter Integration Framework

You must provide information about the Compliance Process Manager (CPM) site to which Teamcenter Integration Framework must send the data fetched from Teamcenter. For this, you create a CPM site in Teamcenter Integration Framework:

1. Navigate to the *TC_ROOT/tcif/container/bin* folder and run the *trun.bat* file to start Teamcenter Integration Framework. Here, *TC_ROOT* is the directory where Teamcenter Integration Framework is installed. An example is *C:/Program Files/Siemens/Teamcenter2412*.

2. Open the Teamcenter Integration Framework web console by typing the following URL in a browser:

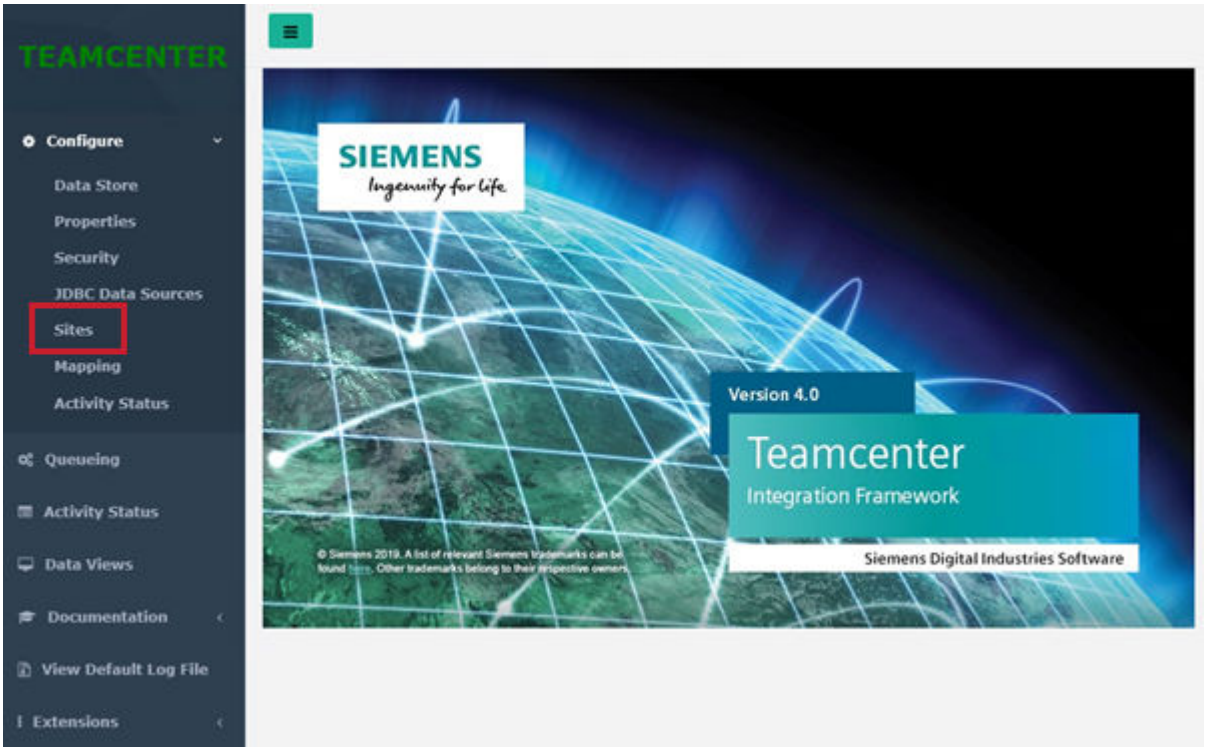
   `http://TcIF_host:TcIF_port/tcif/rest/login`

   Here, *TcIF_host* is the name of the computer that hosts Teamcenter Integration Framework, and *TcIF_port* is the web UI port number of Teamcenter Integration Framework. An example is **http://TcIF_host:8090/tcif/rest/login**.

   To obtain the *TcIF_port* port number, navigate to the *TC_ROOT/tcif/container/etc* folder and open the *system.properties* file. Note the value of **restservices.port**.

   Enter the credentials to log on. By default, the **User ID** and **Password** are **IFAdmin** and **admin**, respectively.

3. Click **Configure→Sites**.

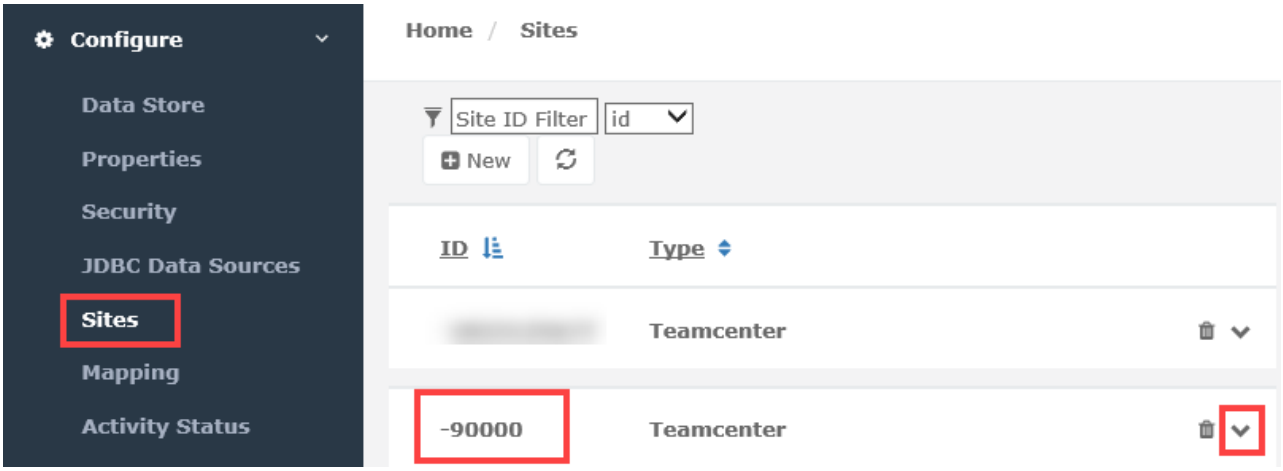


4. On the **Sites** page, click **New**.

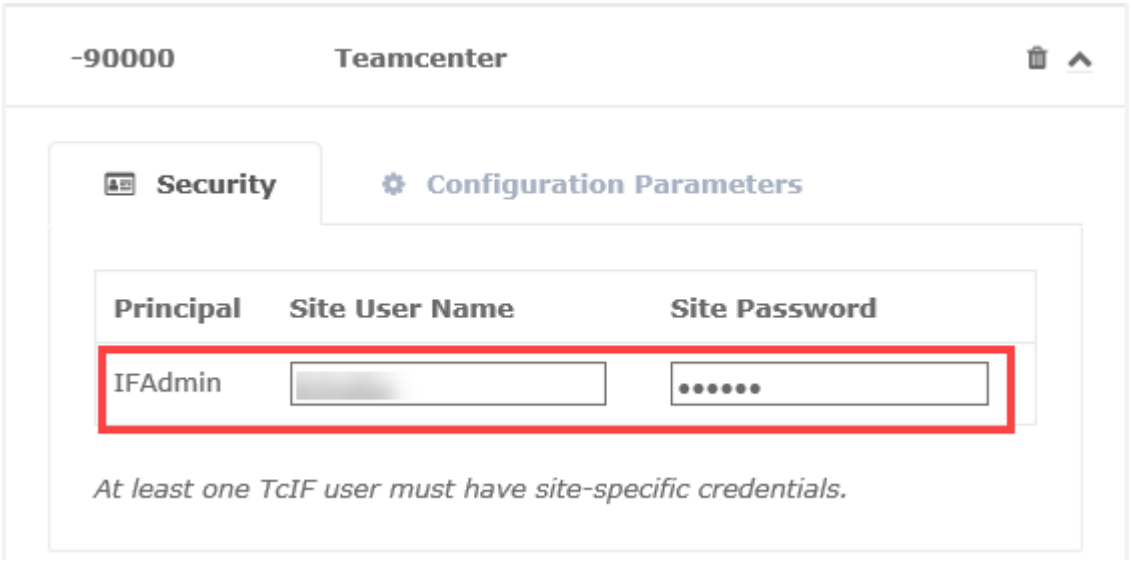
5. Enter the CPM site ID in **Site ID**, and select **Teamcenter** in **Site Type**.

6. Click **Create**.

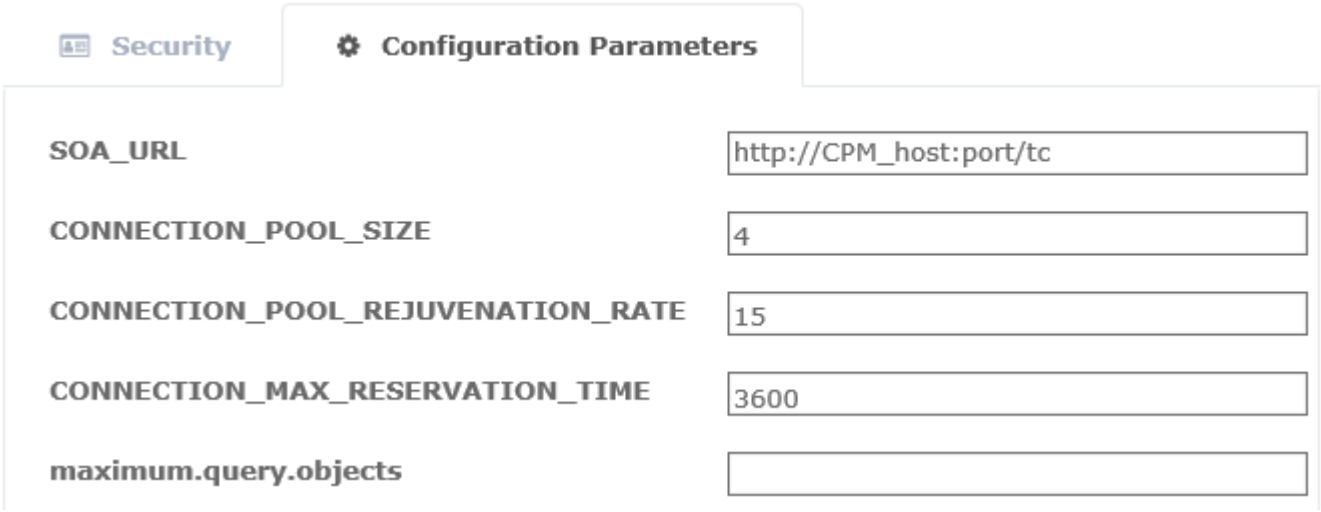
7. In the **Sites** tab, expand the section containing the CPM ID you created.



8. Enter the Teamcenter administrative user name in **Site User Name** and the password in **Site User Password**.



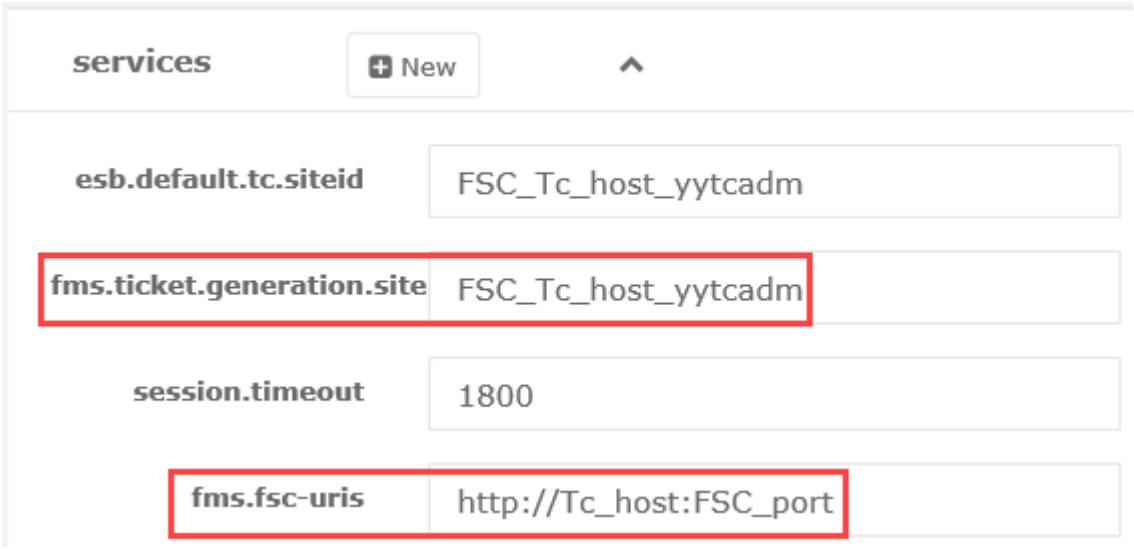
9. In the **Configuration Parameters** tab, verify that the values appear correctly.



Ensure that *CPM_host:port* specifies the correct CPM host and port number.

10. Click **Save**.

11. In the **Properties** tab, expand the **services** section and add the following values.



Property	Value
fms.ticket.generation.site	The value of the **id** attribute of the **fsc** element in the *TC_ROOT /fsc/ fmsmaster_FSC_xxxx.xml* file.
fms.fsc-uris	The value of the **address** attribute of the **fsc** element in the *TC_ROOT /fsc/ fmsmaster_FSC_xxxx.xml* file.

12. Click **Save changes**.

13. Restart Teamcenter Integration Framework to ensure that the configuration is saved.

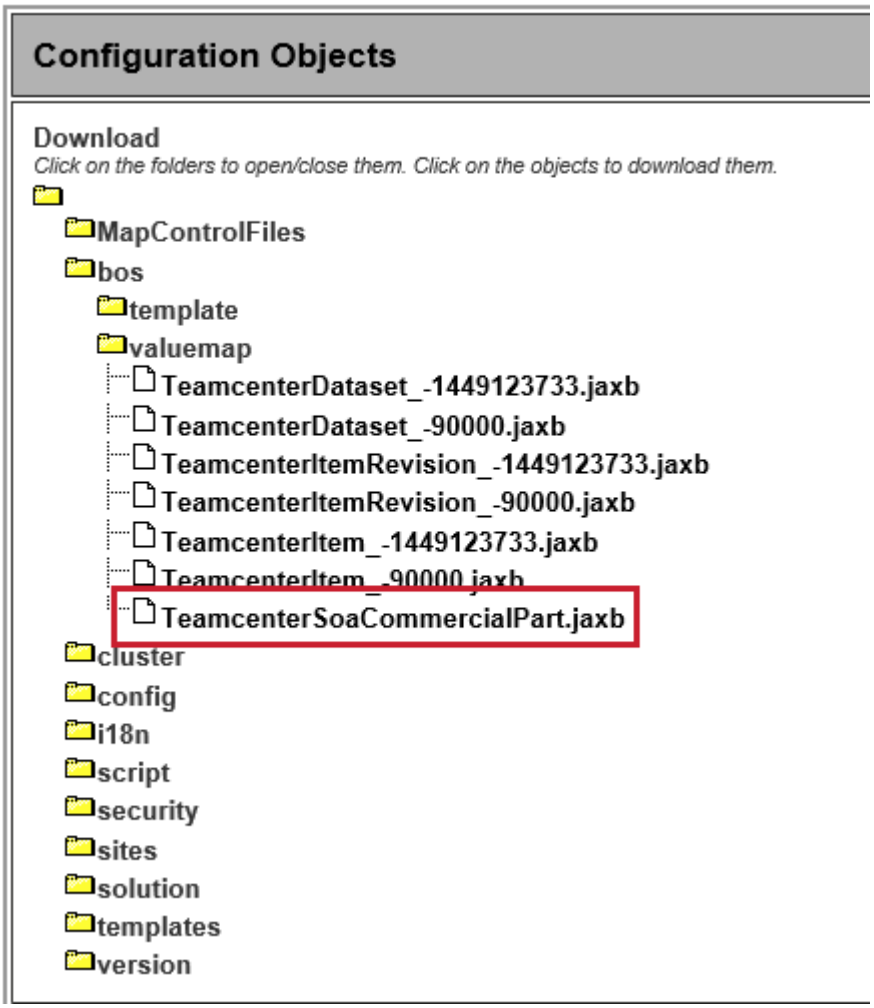
Connect the Teamcenter and CPM sites

After creating the Teamcenter and Compliance Process Manager (CPM) sites that participate in the integration, you must select the Teamcenter site as the source site and the CPM site as the target site. The Teamcenter site is set as the source site because the substance compliance check is initiated from Teamcenter.

Connect the Teamcenter and CPM sites

1. Click **Configure→Data Store**.

2. In the **Datastore** tab, click the **bos** folder and download the **TeamcenterSoaCommercialPart.jaxb** file.

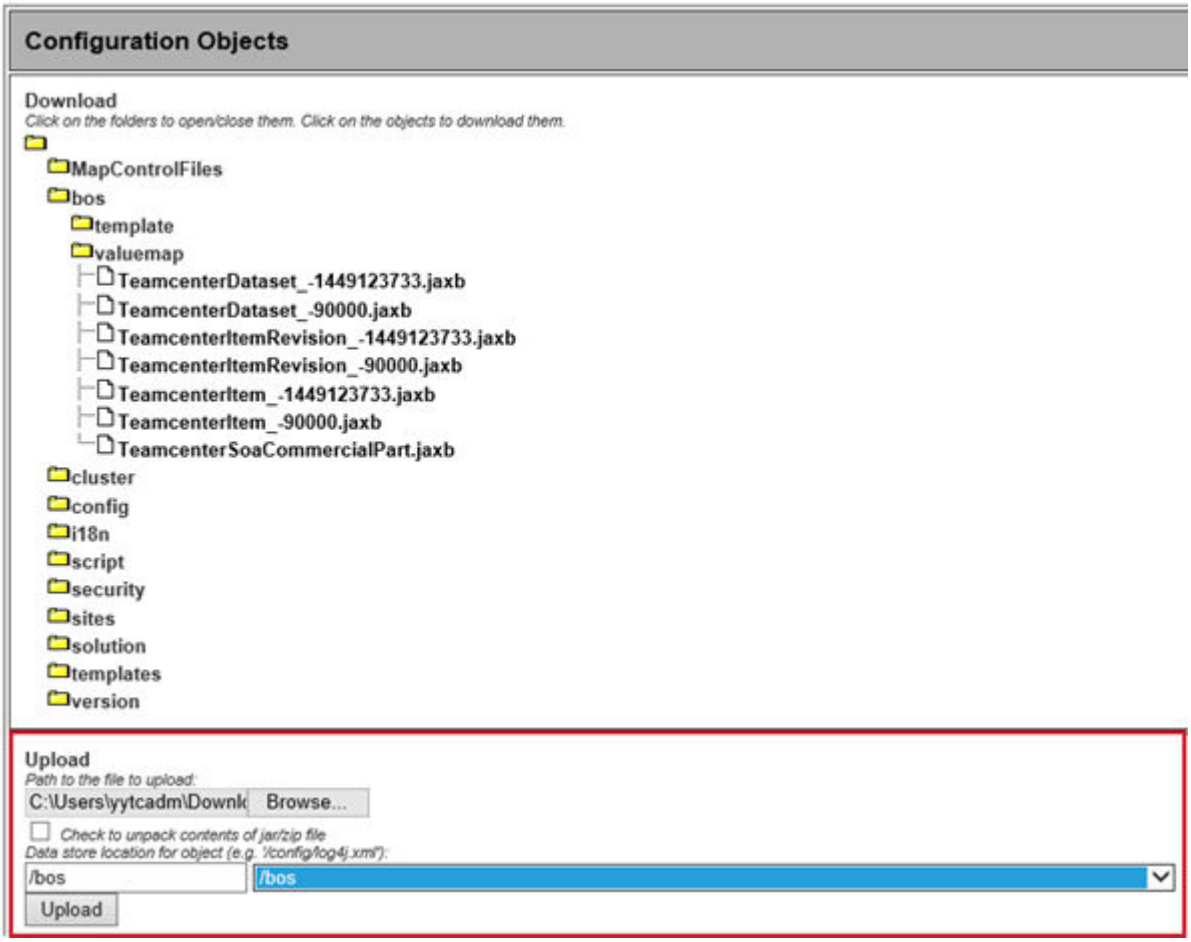


3. In the **TeamcenterSoaCommercialPart.jaxb** file, replace **[tc-site-id]** with the Teamcenter site ID, for example, *-1449123733*. To obtain the Teamcenter site ID, navigate to the **TC_ROOT/fsc** folder and open the **fmsmaster_FSC_xxxx.xml** file. Note the value of the **id** attribute of the **fmsenterprise** element.

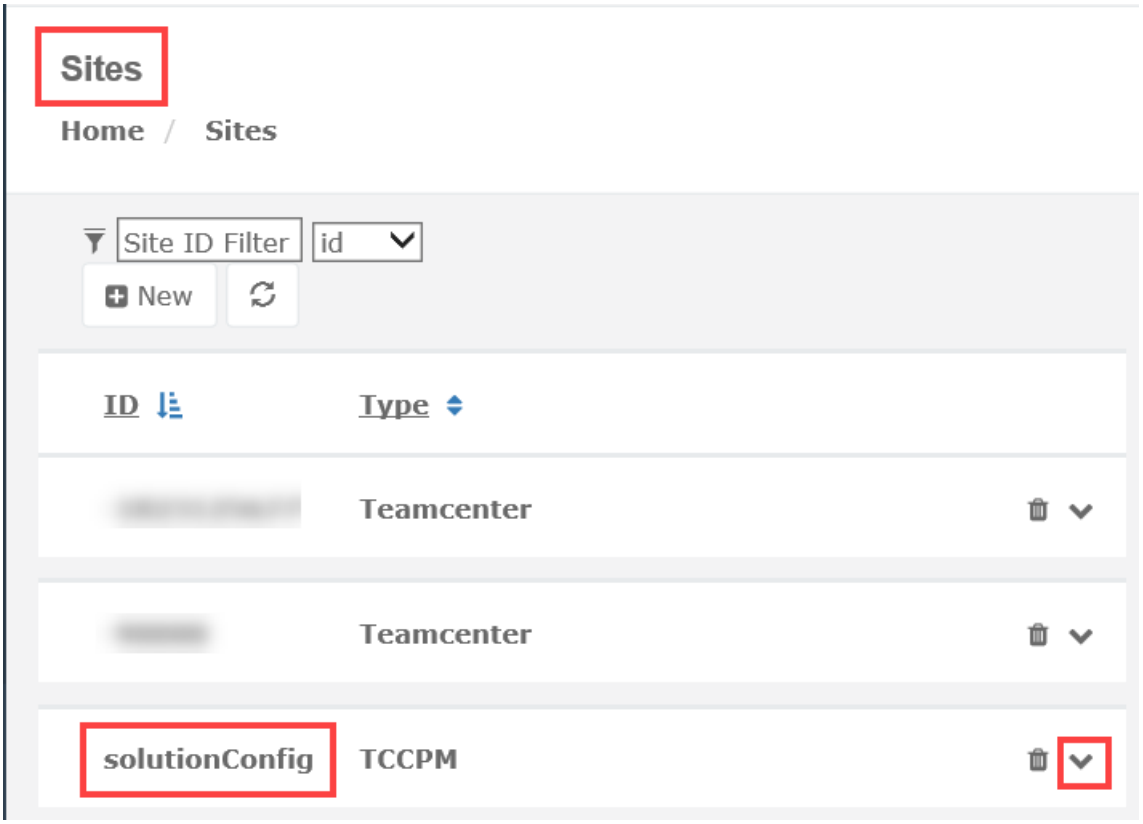
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE fmsworld SYSTEM "fmsmasterconfig.dtd">

<fmsworld>
  <fmsenterprise id="-1449123733" volumestate="normal">
    <fccdefaults>
```

4. Upload the **TeamcenterSoaCommercialPart.jaxb** file to the **bos** folder.



5. In the **Sites** tab, expand the **solutionConfig** section.



6. Update the values for the following attributes:

   - **TeamcenterSite** : The Teamcenter site ID. An example is *-1449123733*.
   - **CPMSite**: The value specified in Teamcenter while creating the CPM site, for example, *-90000*.

     To obtain the CPM site ID, open the Teamcenter Organization application, and click the site you created for CPM under **Sites**. Note the **Site ID** value.
   - **notification_from_email**: The email address of the user sending the notification email.

7. Click **Save**.

8. Restart Teamcenter Integration Framework.

Configure Teamcenter Integration Framework for encrypted communication with Compliance Process Manager

First, **create a Compliance Process Manager (CPM) site** in Teamcenter Integration Framework.

Based on the requirements of your organization, you may want to configure CPM for HTTPS (encrypted) communication. To do so:

1. Navigate to *TC_ROOT/tcif/container/bin* and run the *trun.bat* file to start Teamcenter Integration Framework. Here, *TC_ROOT* is the directory where Teamcenter Integration Framework is installed. An example is *C:/Program Files/Siemens/Teamcenter2412*.

2. Open the Teamcenter Integration Framework web console by typing the following URL in a browser:

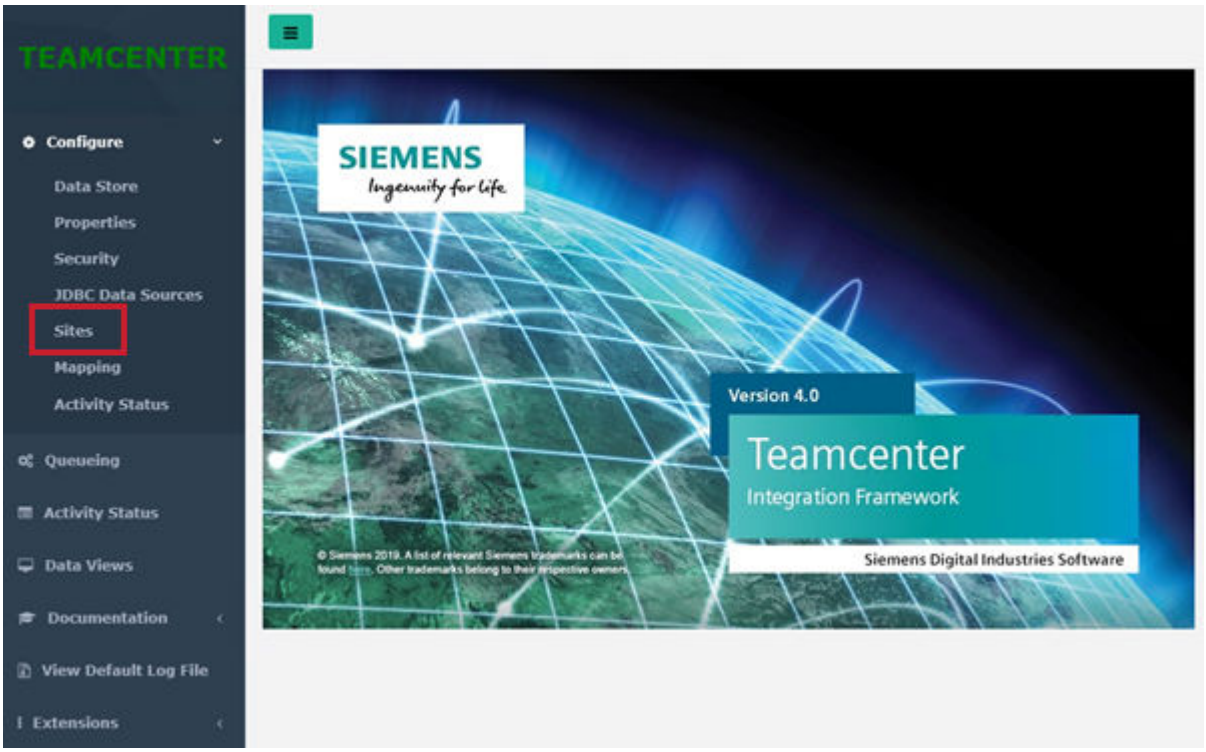
   `http://`*TcIF_host*`:`*TcIF_port*`/tcif/rest/login`

   Here, *TcIF_host* is the name of the computer that hosts Teamcenter Integration Framework, and *TcIF_port* is the web UI port number of Teamcenter Integration Framework. An example is **http://vc6s004:8090/tcif/rest/login**.

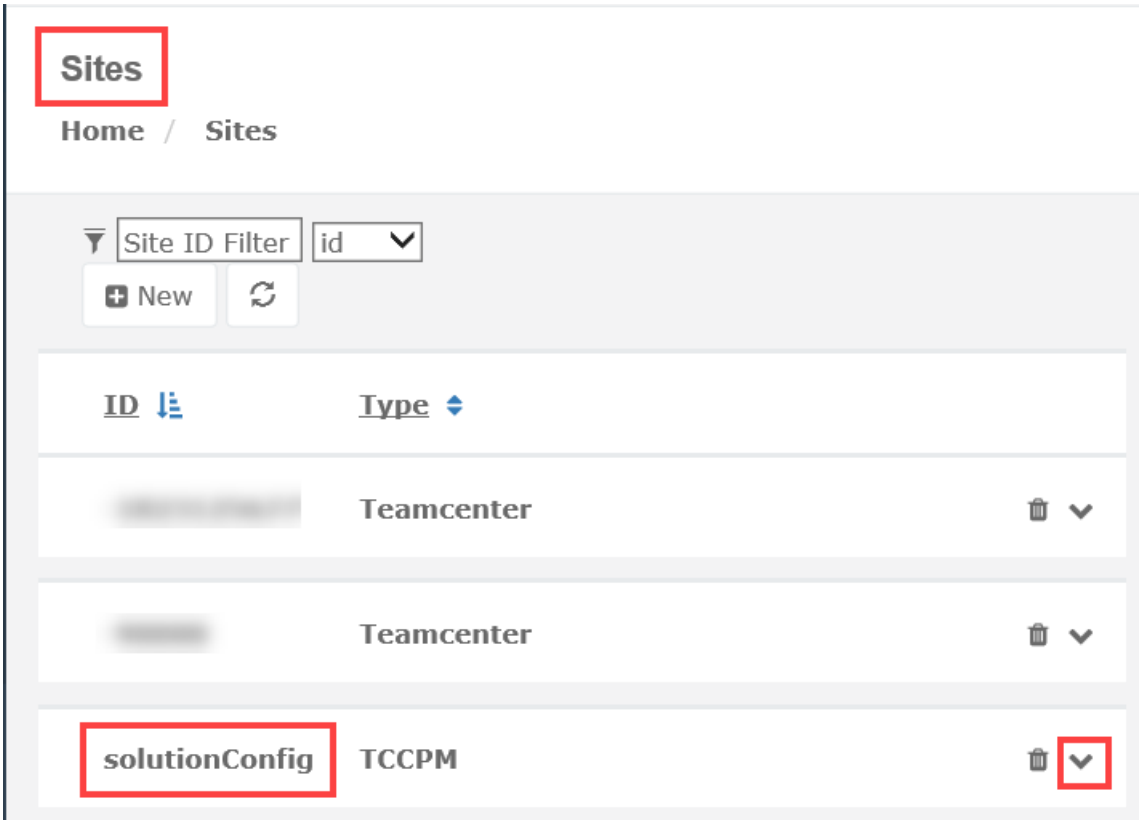
   To obtain the web UI port number, navigate to the *TC_ROOT/tcif/container/etc* folder and open the *system.properties* file. Note the value of **restservices.port**.

   Enter the credentials to log on. By default, the **User ID** and **Password** are **IFAdmin** and **admin**, respectively.

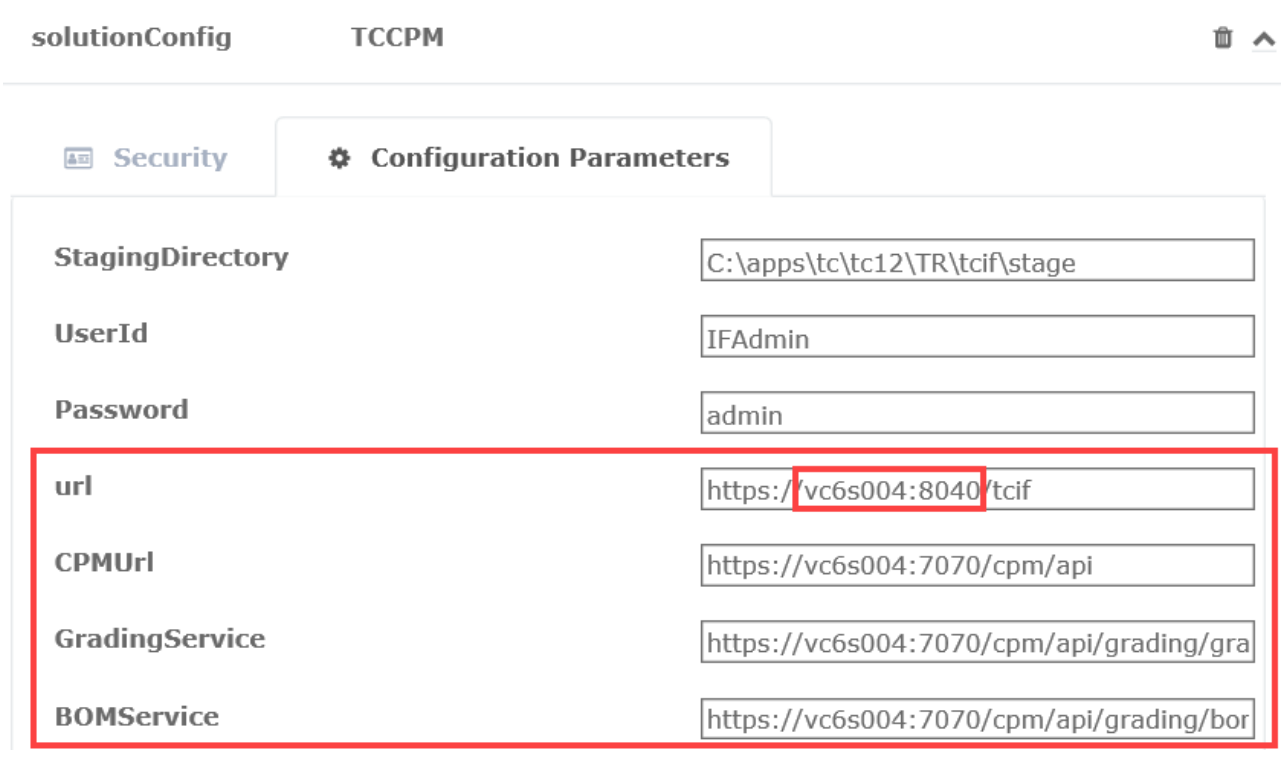
3. Click **Configure→Sites**.



4. In the **Sites** tab, expand the **solutionConfig** section.



5. Modify the following attributes to specify the SSL-enabled CPM server and port details:



Here, `vc6s004` is the CPM server, and `8040` is the CPM port configured for SSL communication. Ensure that the URL starts with `https` and not `http`.

Make sure you create a staging directory and assign it to the **StagingDirectory** parameter.

6. Click **Save**.

7. Find the value of the `JAVA_HOME` attribute in the *TCIF_HOME_PATH\container\bin\tcenv.bat* file used by Teamcenter Integration Framework. For example, in the *C:\apps\tc\tc2412\TR\tcif\container\bin\tcenv.bat* file, `JAVA_HOME` is set to *C:\apps\java\jdkx64*.

8. Navigate to the path specified in the `JAVA_HOME` attribute and search for *cacerts*, the security certificates collection file. For example, the *cacerts* file could be located in the *C:\apps\java\jdkx64\jre\lib\security* directory.

   > Note:
   >
   > The Java Development Kit maintains a certification authority (CA) keystore file named cacerts, which is a repository of security certificates (either authorization certificates or public key certificates, including the corresponding private keys) used in SSL encryption. Java uses cacerts to authenticate the servers.

9. Open the *cacerts* repository file using either the Java keytool command line utility or any other tool that is used to create and navigate keystores.

10. Ensure that you have generated a trust certificate for encrypted communication.

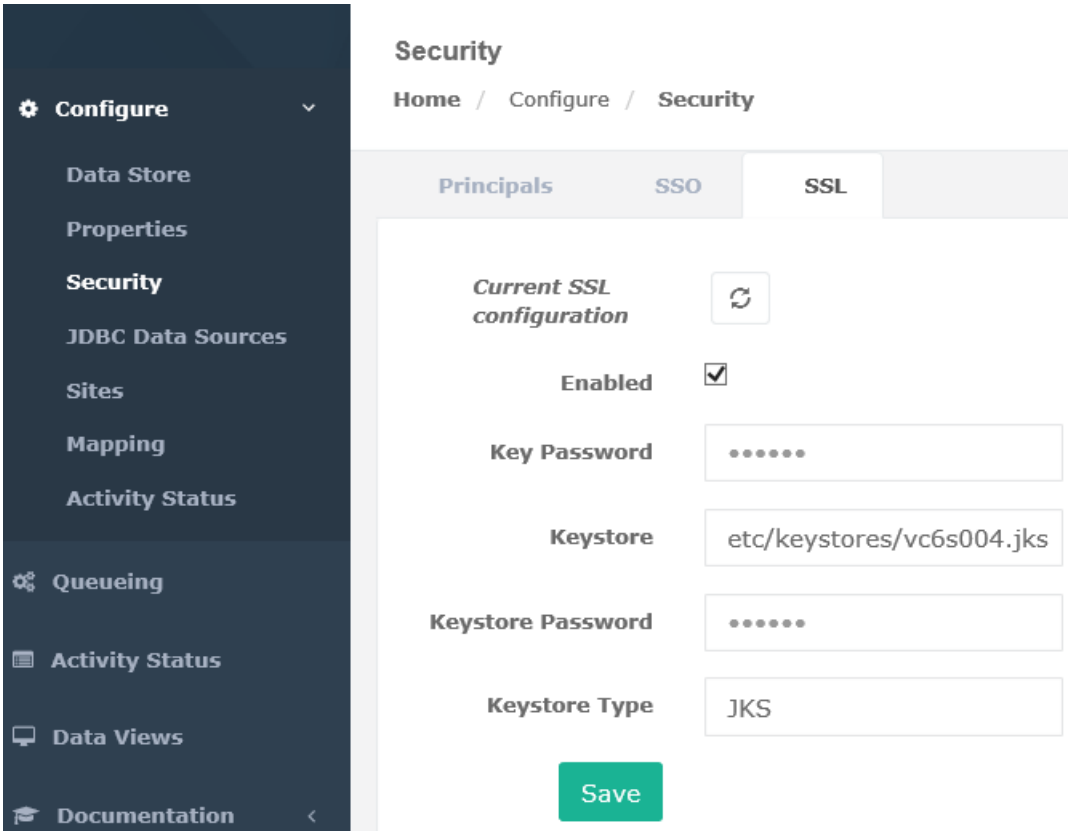
    Import the trust certificate file (for example, *C:\apps\tc\tc2412\TD\subscmpl_data\config\vc6s004.cer*) into the *cacerts* file. Ensure that the certificate has a valid end date.

    For secure communication, the server being contacted must supply a certificate that the client subsequently validates. Certificates can be obtained through various means and installed on a web server or in a local certificate store. Clients receiving the certificate validate it against its certificate store, and on that basis, accept or reject the connection. See the Teamcenter Security Services help for details about certificates.

11. In the Teamcenter Integration Framework web console, click **Configure → Security**.

12. On the **Security** page, click the **SSL** tab.

13. Select the **Enabled** check box to specify that an SSL communication mode must be used.



14. Provide the values for **Key Password** and **Keystore Password**.

    For details about the values that you must provide here, see the *SSL* documentation in the Teamcenter Integration Framework help.

15. In **Keystore**, specify the location of the repository for the security certificates used for SSL encryption and the name of the certificate.

    An example is the *C:\apps\tc\tc2412\TR\tcif\container\etc\keystores\vc6s004.jks* file.

16. Set the **Keystore Type**. As Teamcenter Integration Framework is Java-based, the default is **JKS**. Another commonly used keystore type is *PKCS#12*, which is not Java-specific.

17. Click **Save**.

18. Restart Teamcenter Integration Framework to ensure that the configuration is saved.

Configure Compliance Process Manager for encrypted communication

1. On the Compliance Process Manager (CPM) server (for example, a Tomcat application server), navigate to and open the *<CPM_HOME>\conf\server.xml* configuration file.

2. Create a keystore file to store the server's private key and self-signed certificate by using the Java keytool command line utility or any other tool that is used to create and navigate keystores.

3. Copy this keystore file (for example, *vc6s004.jks*) from your local machine to the *<CPM_HOME>\conf* folder on the CPM server.

   For example, copy the *vc6s004.jks* keystore file to the *C:\apps\tc\cpm\conf* folder.

4. Disable the connector block supporting a non-SSL (http) connection by commenting it out.

   For example, disable the following connector block:

```
<!--
            <Connector port="7070" protocol="HTTP/1.1"
            connectionTimeout="20000"
            redirectPort="8443" />
-->
```

5. Enable the connector block supporting an SSL (https) connection by removing the comments and editing it.

   > Note:
   >
   > An example `<Connector>` element for an SSL connector is included in the default *server.xml* file installed with Tomcat.

   For example, the edited SSL connector block is as follows:

```
<Connector port="8443"
         protocol="org.apache.coyote.http11.Http11NioProtocol"
         maxThreads="200" SSLEnabled="true" scheme="https"
secure="true"
         clientAuth="false" sslProtocol="TLS"
keystoreFile="C:\apps\tc\cpm\conf\vc6s004.jks"
         keystorePass="password">
</Connector>
```

   Ensure that you set the following attributes.

Attribute	Description
port	Specify the port number of the CPM server, for example, **8443**.
keystoreFile	Specify the complete path and file name of the keystore file, for example, *C:\apps\tc\cpm\conf\vc6s004.jks*

6. Restart the CPM server to ensure that the configuration is saved.

Configure Teamcenter for encrypted communication

You require a client certification authentication to allow Teamcenter to use a digital certificate to authenticate a secure communication with Teamcenter Integration Framework. This client certification authentication uses HTTP over SSL (HTTPS) in which the server and the client authenticate each other using a public key certificate. Client-certificate authentication provides data confidentiality, data integrity, and client and server authentication for a TCP/IP connection.

After you configure Teamcenter Integration Framework for **secure socket layer (SSL) communication**, perform the following steps to configure Teamcenter to communicate in the SSL mode:

1. Obtain a copy of the authentication certificate. See the Teamcenter help for information about obtaining SSL certificates.

2. Copy the certificate to the *TC_DATA\subscmpl_data\config* folder on the Teamcenter server, for example, *C:\apps\tc\tc2412\TD\subscmpl_data\config\vc6s004.cer*.

3. Set the **SUBSCMPL_ssl_cert_full_file_path** preference to specify the name and the location of the certificate.

   For example, set **SUBSCMPL_ssl_cert_full_file_path** to *C:\apps\tc\tc2412\TD\subscmpl_data\config\vc6s004.cer*.

4. Set the **EPM_task_execution_mode** preference to **CONFIGURABLE**.

5. In Workflow Designer, for the compliance check task, select the **Process in Background** check box to enable the task to run in the background.

   For details about running a task in the background, see *Configure tasks for background processing* in the Teamcenter help.

6. Start the Dispatcher Client.

7. Restart Teamcenter Pool Manager.

11. Verify the Teamcenter and Compliance Process Manager integration

After connecting Teamcenter Integration Framework with Teamcenter and Compliance Process Manager, you must verify the integration:

1. In My Teamcenter, click **Edit→Options**.

2. In the **Options** dialog box, search for the following preferences and ensure that their values are set correctly:

Preference	Description	Sample value
SUBSCMPL_compliance_-server_host	Specifies the host name of Teamcenter Integration Framework.	*Tc_host*
SUBSCMPL_compliance_-server_port	Specifies the REST services port number for Teamcenter Integration Framework.	*8090*
TCIF_url	Specifies the URL of the Teamcenter Integration Framework web service.	*http://Tc_host:8080/tcif*
TC_gms_server	Specifies the URL of the Teamcenter Integration Framework REST service.	*http://Tc_host:8090/tcif*
GS_USER_NAME	Specifies the name of the administrative user for Teamcenter Integration Framework.	**IFAdmin**
GS_USER_PASSWORD	Specifies the password of the Teamcenter Integration Framework administrator user.	**admin**

12. Set up grading properties in Compliance Process Manager

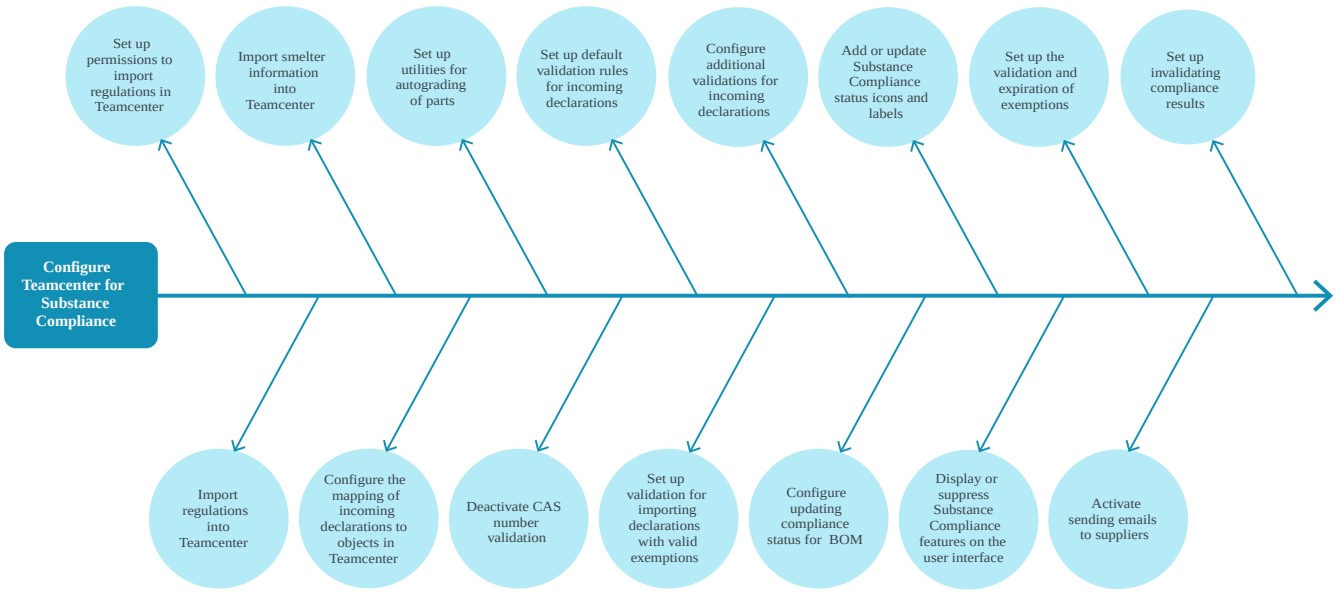
A compliance officer performs a compliance check against one or more regulations to verify if a part used in a product is environmentally compliant. To perform a compliance check on a part, the part must have a non-zero measured mass with an appropriate unit of measure.

You can set the **cpm.grading.zero.mass.allowed** property to *true* in Compliance Process Manager (*cpm.properties* file) to bypass the non-zero measured mass requirement. For more details about which properties to set in the *cpm.properties* file, see the Compliance Process Manager documentation available with the Compliance Process Manager installation kit on Support Center.

Additionally, you can set the **cpm.grading.empty.parts.allowed** property to control if an item revision (for example for an internal part) can have no mass specified for the topmost node.

13. Configure Teamcenter for Substance Compliance

Perform the following tasks to configure Teamcenter for Substance Compliance.



- **Set up permissions to import regulations** in Teamcenter
- **Import regulations** into Teamcenter.
- **Import smelter information into Teamcenter**
- **Configure the mapping of incoming declarations** to objects in Teamcenter.
- **Set up utilities for autograding**
- **Deactivate CAS number validation**.
- **Set up default validations for incoming declarations**
- **Set up validation for importing declarations** with valid exemptions.
- **Configure additional validations** for incoming declarations.
- Configure **updating compliance status for a BOM**.
- **Add or update Substance Compliance status icons and labels**.
- **Display or suppress** Substance Compliance features on the user interface.
- Set up the **validation and expiration of exemptions**.
- **Activate or deactivate sending emails to suppliers**
- Set up **invalidating compliance results**.

14. Set up permissions to import regulations in Teamcenter

An environmental regulation is a directive that restricts the usage of banned or hazardous substances. The environmental regulation:

- Lists the restricted substances
- Lists the rules that define the scope in which a restricted substance can be used
- Specifies the reasons for the restrictions

To enable a compliance officer to perform a compliance check on a vendor part or assembly, you should first **import the regulations in Teamcenter**. To do so, you must be added to certain Organization groups and roles with administrator privileges.

To do this, set the values of the **SUBSCMPL_regulation_creator_groups** and **SUBSCMPL_regulation_creator_roles** preferences as the group name and role of the user importing the regulations, respectively. For example, the group could be *dba* and the role could be *Administrator*.

15. Import regulations into Teamcenter

Prerequisites to importing regulations

- Teamcenter and Compliance Process Manager (CPM) must be installed and configured for communication.
- For Teamcenter, ensure that the FMS Server Cache (FSC) and pool manager services are started.
- The **TC_ROOT** and **TC_DATA** environment variables point to the Teamcenter application root directory and Teamcenter application data directory, respectively.
- The environment variables set while installing Teamcenter are correct. To do this, run the **tc_profilevars** script located at *TC_DATA\tc_profilevars*.
- The **JAVA_HOME**, **JRE_HOME**, and **PATH** environment variables are set with the correct Java version and path.
- You have the necessary permissions to import regulations.

To import the regulations:

1. Download the appropriate regulations available on Support Center > **Teamcenter** > **Downloads** > **Substance Compliance Regulations**.
2. Navigate to and open the*TC_DATA\subscmpl_data\xsl\regulation_to_tcxml.xsl* file.
3. Extract the regulation ZIP file to a temporary location. Copy the extracted regulation files to the *CPM_HOME\regulations\install* folder. An example of *CPM_HOME* is *C:\apps\tc\cpm*.
4. Start Teamcenter Integration Framework and the CPM service:

   - Run the *trun.bat* or *trun.sh* file to start Teamcenter Integration Framework.
   - Run *startup.bat* or *startup.sh* to start the CPM service.

   Once you run the *startup.bat* or the *startup.sh* command, CPM generates the following files:

   - The successfully imported regulation files in the *archive* folder located in the *CPM_HOME\regulations* directory.
   - The regulations that failed the import in the *error* folder located in the *CPM_HOME\regulations* directory.

- The *.xml* files for the regulations (in the *archive* folder) in the *descriptors* folder located in the *CPM_HOME* directory.

5. Launch Teamcenter command prompt, navigate to *TC_ROOT\bin*, and run the *regulation_import.pl* utility:

```
tcperl regulation_import.pl -u=user id -p=password -g=group -dir|-
file
```

Enter a value for *–file* to import the specific regulation descriptor file, or enter a value for *–dir* to import all the files located in the *descriptors* folder.

Alternatively, you can use:

```
call perl %TC_ROOT%\bin\regulation_import.pl -u=user -p=password
-g=group -dir|-file
```

Example:

`call perl %TC_ROOT%\bin\regulation_import.pl -u=`*Tc-admin-user* `-p=`*password* `-g=`*group* `-dir=C:\apps\tc\cpm\descriptors`

Now:

- The successfully imported files are moved to the *archive* folder created in the *descriptors* directory.
- The ones that are not imported successfully are moved to the *error* folder in the *descriptors* directory.
- The ones that are being processed are moved to the *processing* folder in the *descriptors* directory.
- The log files are generated in the *processing* folder located in the *descriptors* folder.

Verify if the regulations are imported correctly into Teamcenter

1. Log on to Teamcenter.
2. In My Teamcenter, click **Perform Search** →**Advanced**.
3. In the **Search** view, click **Select a Search** →**More**.
4. In the **Change Search** dialog box, click **System Defined Searches**→**Substance Compliance-Regulations**.

5. Enter the search criteria and click **Search**  .

   The search result displays the regulations that were imported successfully.

6. Additionally, you can search for the following objects that are created in Teamcenter on a successful import of the regulation file:

   - Regulation
   - Substance Check (Rule)
   - Substance Group
   - Substances
   - Exemption List
   - Exemptions
   - Substance Category List and Substance Category
   - Abstract Declaration List and Abstract Declarations

7. Choose the regulation object in Teamcenter to display the details in the regulation summary view.

16. Import smelter information into Teamcenter

The Responsible Minerals Initiative (RMI) maintains a list of active and conformant smelters. To enable the compliance officer review conflict mineral declarations, as an administrator, you must first download the smelter information from the RMI portal.

1. On the RMI portal, accept the terms and conditions to get the smelter list.

2. Download the following:

   - 3TG Standard Smelter List
   - Revisions History

   The *CMRT_Export.xml* and *Revisions_StdSmelterList.xml* files are downloaded.

3. You can import this information using the **SMELTERS** tile available on the **Active Admin** workspace. Click this tile to open the **SMELTERS** page where you can **Add**, **Delete** or **Import** smelters information.

   OR

   On the Teamcenter command prompt, go to *TC_ROOT/bin* and run the following command to import each of the smelter files:

   ```
   subscmpl_populate_smelters -u=<administrator ID> -p=<administrator
   password> -g=dba -type=XML -file=<file path>\<file name>.xml
   ```

   Example:

   ```
   subscmpl_populate_smelters -u=tcadmin -p=tcadmin -g=dba -type=XML
   -file=C:\downloads\TcSC\CMRT_Export.xml
   ```

   ```
   subscmpl_populate_smelters -u=tcadmin -p=tcadmin -g=dba -type=XML
   -file=C:\downloads\TcSC\Revisions_StdSmelterList.xml
   ```

4. Download the conformant smelter information for each of the 3TG metals in the following sequence:

   - Tantalum
   - Tin
   - Tungsten

- Gold

a. On the **RMI** portal, from the list of links on the right, click the link applicable to the relevant metal in the sequence mentioned earlier.

b. Click the **Export All Conformant** for the respective metal.

c. On the **Export All Conformant Smelter** page, download the smelter list.

   Rename the downloaded XML file with the name of the particular metal, for example, *tantalum.xml*.

Repeat these steps to download the conformant smelter information for each of the remaining metals in the prescribed sequence.

5. You can import this information using the **SMELTERS** tile available on the **Active Admin** workspace. Click this tile to open the **SMELTERS** page where you can **Add**, **Delete** or **Import** smelters information.

   OR

   On the Teamcenter command prompt, go to *TC_ROOT/bin* and run the following command to import each of the conformant smelter files in the following sequence: tantalum, tin, tungsten, and gold.

   ```
   subscmpl_populate_smelters -u=<administrator ID> -p=<administrator
   password> -g=dba -type=XML -file=<file path>\<conformant smelter
   file>
   ```

   ```
   subscmpl_populate_smelters -u=tcadmin -p=tcadmin -g=dba -type=XML
   -file=C:\downloads\TcSC\tantalum.xml
   ```

   Verify the importer logs or search for smelters in the rich client to ensure that the import is successful.

   You can also download the latest template for declaring conflict minerals, namely, Conflict Minerals Reporting Template (CMRT), from the **portal**.

17. Configure the mapping of incoming declarations to objects in Teamcenter

The Teamcenter Substance Compliance solution uses queries to search for commercial and vendor parts or materials in Teamcenter and also to map incoming supplier declarations to the respective object (vendor, vendor part, or materials) in Teamcenter.

By default, when a declaration is received in Teamcenter, based on the type of declaration (material substance declaration (MSD), conflict mineral declaration (CMD), or lab reports, the system uses the query saved in the **SUBSCMPL_<declaration_type>_TARGET_QUERY_NAMES** preference to find the target object in Teamcenter. Here, **<declaration_type>** could be *MSD*, *CMD*, or *LRD*.

The following queries are available OOTB:

- Substance Compliance MSD - Get Target Object From Commercial Part and Vendor
- Substance Compliance MSD - Get Target Object From Vendor Part
- Substance Compliance CMD - Get Target Object From Vendor
- Substance Compliance CMD - Get Target Object From Vendor Part
- Substance Compliance LRD - Get Target Object From Material Info
- Substance Compliance LRD - Get Manufacturer
- Substance Compliance LRD - Get Laboratory
- Substance Compliance LRD - Get Supplier
- Substance Compliance LRD - Get Material Lab Report

These queries use attributes, such as a vendor part name, a vendor ID, or a material ID to search for the parts or materials in Teamcenter. These attributes are also used to find the appropriate commercial or vendor parts, or materials in Teamcenter that match the parts or materials in the incoming supplier declarations. By default, for an MSD or CMD, the *Substance Compliance MSD - Get Target Object From Vendor Part* query is used to map the incoming declarations to a Teamcenter object. For a lab report, the *Substance Compliance LRD - Get Target Object From Material Info* is the default query.

Based on your organization's requirement, you can change the existing search criteria by:

1. **Replacing the existing query** with a different OOTB query or by creating a new query to search for a Teamcenter object.

2. **Updating the TCXML style sheet** to specify which attributes to include from the search queries.

Update preferences to map query attributes with Teamcenter objects

Based on the type of declaration for which you wish to use a different query, set the value of the **SUBSCMPL_MSD_TARGET_QUERY_NAMES**, the **SUBSCMPL_CMD_TARGET_QUERY_NAMES**, or the **SUBSCMPL_LRD_TARGET_QUERY_NAMES** preference to the name of the search query of your choice. Additionally, provide the number of attributes to be mapped.

> Tip:
>
> Use the Teamcenter Query Builder application to view the details about a particular query.

> Example:
>
> Consider that you wish to map a material and substance declaration to parts in Teamcenter based on a vendor part ID and vendor:
> You set the **SUBSCMPL_MSD_TARGET_QUERY_NAMES** preference to **Get Target Object From Commercial Part and Vendor:2**. Here:
>
> - **Get Target Object From Commercial Part and Vendor** is the name of the query.
> - The colon (**:**) in **Find Target Object From Vendor Part:2** is the delimiter.
>
> > Note:
> >
> > You can change the delimiter by setting the value of the **SUBSCMPL_target_finder_delimeter** preference to the delimiter of your choice.
>
> - The numeral **2** denotes the number of attributes from the incoming supplier declaration to map to the vendor part attributes in Teamcenter.

Update the TCXML style sheet to specify which attributes to include from the search queries

The attributes that you can use in a query are defined in the style sheet that converts the incoming supplier declaration XML file to the TC-XML format. The *<dscl_type>_to_tcxml.xsl* style sheet (where *<dscl_type>* is the declaration type, namely: *msd*, *cmd*, or *lrd*) is located in the *TC_DATA* directory on the Teamcenter server. Set the value of **scp0unique_id** in the *<dscl_type>_to_tcxml.xsl* style sheet to the attributes that you add in the search queries. For example:

Example:

```
<xsl:attribute name="scp0unique_id">
<xsl:value-of select="concat($mPartId,':',$venId)"/>
</xsl:attribute>
```

Here, `$mPartId` maps to a vendor part ID and `$venId` maps to a vendor.

18. Set up utilities for autograding

To autograde or regrade parts and assemblies, set the following utilities to run in this order.

> Note:
>
> Because the output of one utility is used as an input for the next utility, you must run the utilities in this order. You can also set these utilities to be run as a cron job.

Procedure

1. Run the **subscmpl_auto_regrading_parts** utility without the *regrade_assembly* parameter.

   ```
   subscmpl_auto_regrading_parts -u=ed -p=ed -g=dba
   ```

   This utility retrieves and grades the parts based on the presence of the *regrade_assembly* parameter.

2. Run the **subscmpl_mark_assembly_for_regrade** utility. This utility works depending on the preference value **SUBSCMPL_set_intermediate_parents_regradable** (See the preference description for more details.)

   ```
   subscmpl_mark_assembly_for_regrade -u=ed -p=ed -g=dba
   ```

   This utility retrieves all lookup candidates and finds the corresponding *regradable* and *autograding* candidates

3. Run the **subscmpl_auto_regrading_parts** utility with the *regrade_assembly* parameter.

   ```
   subscmpl_auto_regrading_parts -u=ed -p=ed -g=dba -regrade_assembly
   ```

   This utility retrieves and grades the parts based on the presence of the *regrade_assembly* parameter.

19. Deactivate CAS number validation

By default, the supplier declarations are validated to verify whether the Chemical Abstracts Service (CAS) number specified for a substance in a declaration is correct. CAS numbers are also validated when a materials manager creates substances in Teamcenter.

Based on your organization's requirement, you can deactivate this validation by:

- **Specifying patterns to ignore during validation**

  Set the **MATERIALMGMT_wild_card_substance_cas_number_patterns** preference to specify a pattern of CAS numbers for which the in-built validation is deactivated when creating substances in the Materials Management application. You must specify which characters to include as wild cards in the pattern. For details about the pattern to specify and which wild cards to use, see the preference details in the Teamcenter client.

  > Example:
  >
  > If you specify *?7439.*.?* as the value of the **MATERIALMGMT_wild_card_substance_cas_number_patterns** preference and the CAS number of a substance is *7439-92-1*, the system skips the in-built validation for this substance. This is because the string *?.*.?* finds all character sequences with the prefix *7439* and skips the validation for these substances.

- **Specifying the CAS numbers that must be treated as wild cards**

  Set the **MATERIALMGMT_wild_card_substance_cas_numbers** preference to specify which CAS numbers must be treated as wild cards by the Teamcenter Materials Management application. The CAS numbers then skip the in-built validation for the given values while creating the substances in the Teamcenter Materials Management application.

20. Set up default validations for incoming declarations

While importing data, Teamcenter provides some default validations. Some of these can be configured. The following table lists all the available validations, including the ones that can be configured and the details on how to configure them. It also categorizes these validations based on when they are run.

Validations before the import	Applicable class (Class A/C/D)	Configurable	Configuration details
Validate XML is in correct format.	All	No	
Validate against schema (XSD).	All	Yes	This validation is turned off by default. To enable, set the preference **SUBSCMPL_IPC1752_perform_schema_validation** to *true*. This allows validation of your XML file against the schema file (XSD) specified in the preference **SUBSCMPL_IPC1752_xsd_file**.
Validate if the XML contains at least one product element.	All	No	
Validate if the product has its mass value specified, that is, `<Product>/<ProductID>/<Amount>/Value` attributes are specified.	All	No	
Validate if the product mass is disclosed or declared in full for each product element.	All	Yes	Use the preference **SUBSCMPL_msd_partial_disclosure_limit** to specify a percentage limit. A part's material disclosure is not allowed in the material substance declaration import if it is below this limit.
Validate if the material mass exceeds the part mass.	All	No	

Validations before the import	Applicable class (Class A/C/D)	Configurable	Configuration details
Validate if the substance CAS number is valid.	All	Yes	Set the value of the preference **MATERIALMGMT_bypass_CAS_validation** to *False*.
Validate if the material mass is empty.	All	No	
Validate if the substance mass is empty.	All	No	

Validations during the import	Applicable class (Class A/C/D)	Configurable	Configuration details
Validate if the vendor object exists in Teamcenter.	All	Yes	Specify a saved query in the value of the preference **SUBSCMPL_MSD_TARGET_QUERY_NAMES**. This query is run to find the vendor object.
Validate if the vendor part object exists in Teamcenter.	All	Yes	Specify a saved query in the value of the preference **SUBSCMPL_MSD_TARGET_QUERY_NAMES**. This query is run to find the vendor part object.
Validate if `<Declaration>/supplierAcceptance` is *true*.	All	No	
Validate if `<Declaration>/legalType="Custom"`. If yes, then `<Declaration>/legalDef` is also specified.	All	No	
Validate if the supplier exemption object exists in Teamcenter.	All	Yes	Set the value of the preference **SUBSCMPL_msd_enable_exemption_validation** to *true*.

Validations during the import	Applicable class (Class A/C/D)	Configurable	Configuration details
Validate if the exemption is expected, but has not been provided.	Class A	Yes	Set the value of the preference **SUBSCMPL_msd_enable_exemption_validation** to *true*.
Validate the hyperlink in the supported documents section of the form.	All	No	

21. Set up validation for importing declarations with valid exemptions

Sometimes, the IPC declaration sent by suppliers can contain exemptions applicable to certain substances used in the part. In some cases, there may be a mismatch between the exemption and the substance to which this exemption applies. To avoid importing such declarations, you must ensure that only declarations that contain valid exemptions are imported.

To do this, set the **SUBSCMPL_msd_enable_exemption_validation** preference to **true**. This verifies that the exemption mentioned in the IPC file sent by the supplier matches the substance category for which it is to be applied when importing declarations.

22. Configure additional validations for incoming declarations

When importing supplier declarations such as material substance declarations, conflict mineral declarations, or lab reports in Teamcenter, certain validations are carried out on them. These include, among others, verifying whether the vendor part, vendor, or manufacturer mentioned in the declaration is available in Teamcenter, the IPC XML is complete (no missing or incomplete tags), or the vendor details are not missing in the declaration. Certain Teamcenter processing rules are available by default to perform these validations.

Based on your organization's requirement, you can apply additional validations to the declarations, such as verifying specific data (or attributes) in the IPC XML declarations. Currently, additional validations are not applicable for lab reports.

To configure additional validations for the incoming declarations:

1. Create a custom validation utility using a tool of your choice.

2. **Specify the name of this utility as an input** to the appropriate Teamcenter declaration processing rule.

For the custom utility, ensure the following:

- Specify the absolute path of the input declaration file as the first argument of the utility.
- Specify the location where the utility must generate the log files as the second argument of the utility.
- Save the utility in the *TC_ROOT/bin* folder, for example, *C:/Siemens/Teamcenter13/bin*.

During the validation process, all the files generated at the log file location are archived in a folder with the process ID as the name. This folder is also located in the *TC_ROOT/bin* folder. A log file is created for each declaration.

If the declarations are validated as correct and complete, the utility returns **0** to indicate success. Else, it returns **-1** to indicate failure. This validation result is merged with the validation result returned by the default validation-processing rules.

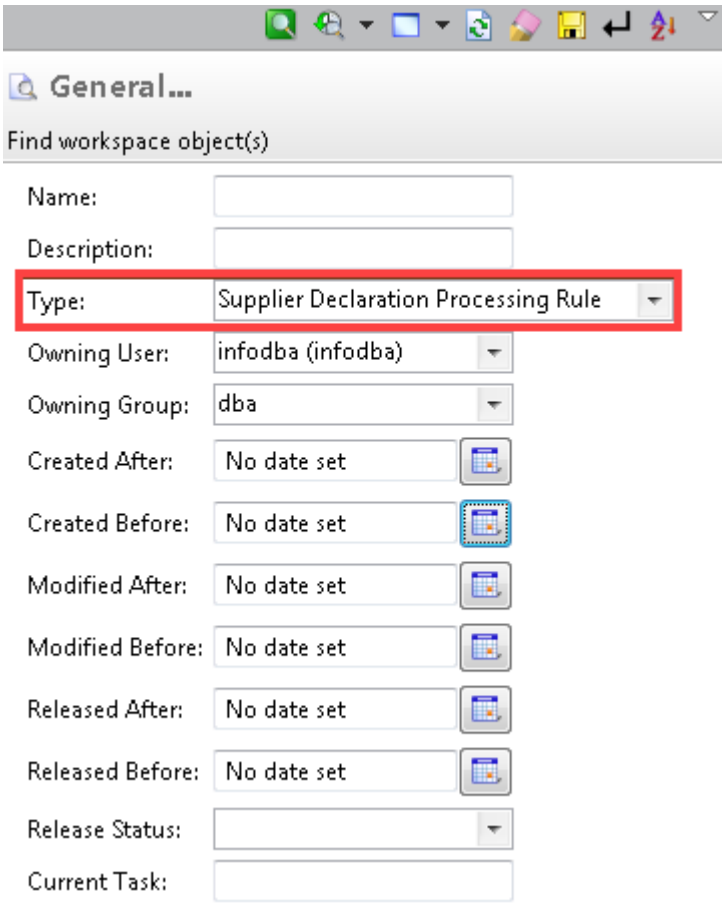
Once you create the custom validation utility, update the existing validation processing rule to run this utility.

Update the existing declaration processing rule to run the custom validation utility

1. In **My Teamcenter**, under **Search**, expand **Perform Search** and click **Advanced**.

2. In the **Search** view, expand **Select a Search** and click **General**.

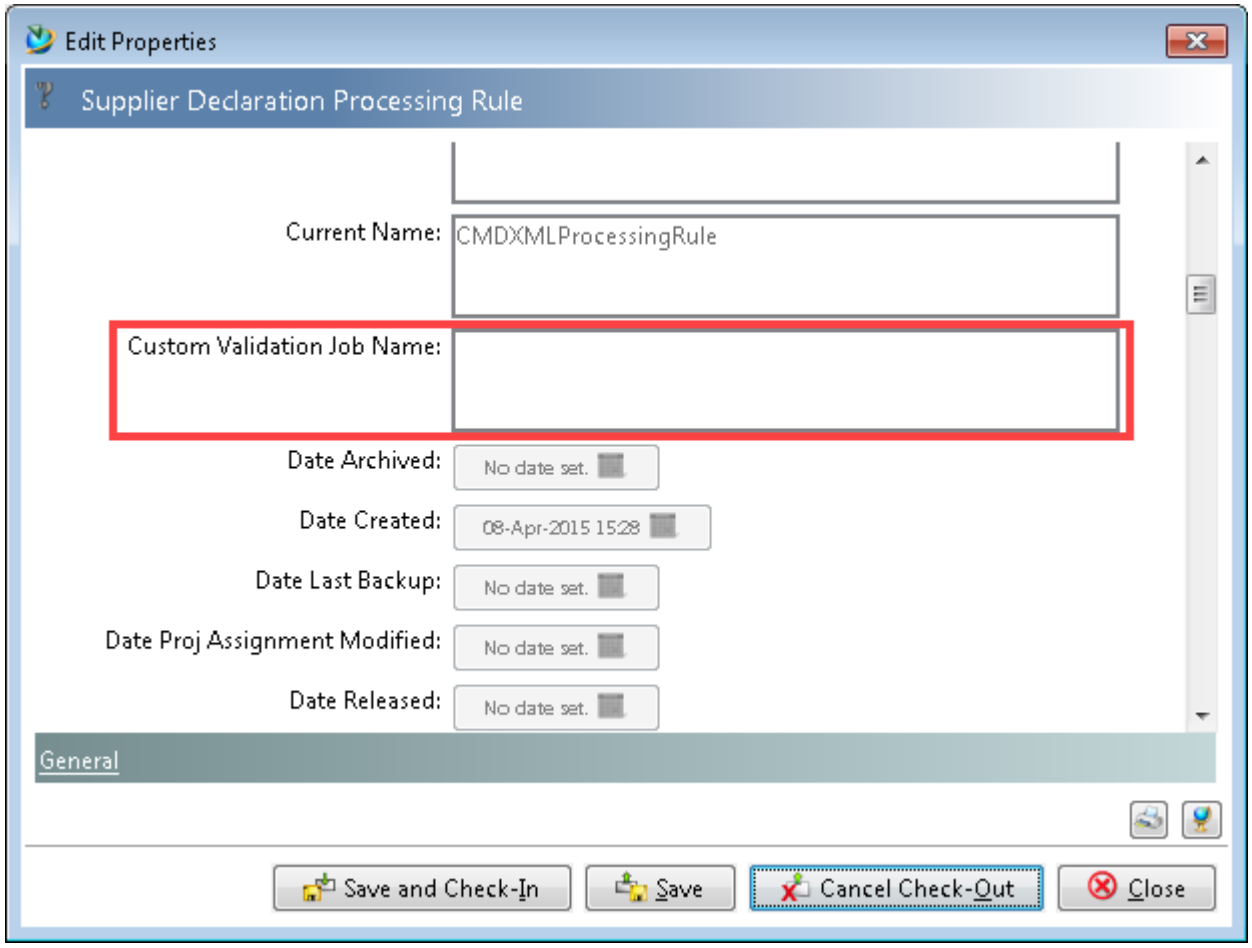
3. In **Type**, select **Supplier Declaration Processing Rule** and click **Execute Search**.



4. In the **Search Results** view, right-click the supplier declaration processing rule that you want to customize, for example, **CMDXMLProcessingRule** and click **Edit Properties**.

5. In the **Check-Out** dialog box, enter the **Change ID** and **Comments**, and click **Yes**.

6. In the **Edit Properties** dialog box, in **Custom Validation Job Name**, enter the name of the custom validation utility.



7. In **Validation Execution Preference**, select **Custom** if you wish to execute the custom utility. If you wish to execute both, custom as well as the default validation, select **BOTH**.

8. Click **Save and Check-In** .

23. Configure updating compliance status for a BOM

Parts with expired exemptions have the compliance status **INVALID**. In some cases, the exemptions for a part in an assembly may have expired. However, the compliance status of the BOM in which the part is used is not changed to **INVALID** automatically. To invalidate the expired exemptions on time, you must periodically validate the compliance results:

1. In **My Teamcenter**, choose **Tools→Substance Compliance→Initiate Compliance Results Validation**.

2. In the **Compliance Results Validation** dialog box, click one of the following:

   - **Call now only**: For a single, instant validation.

   - **Schedule**: For enabling scheduling the compliance results validation functionality periodically.

3. If you click **Schedule**, enter the **Start Time** and **End Time**, and specify the **Interval (in days)**.

4. Click **OK**.

   The compliance results are validated during the specified time duration. If you do not specify the end date, the validation process runs continuously, rendering the compliance objects with expired exemptions invalid.

24. Configure adding or updating compliance status icons

You can add or change the icons associated with a given Substance Compliance status value. For example, the icon associated with the **PASS** compliance status can be changed to a plus sign, check mark, or some other icon.

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

2. On the **Dependent Templates** page, select the **Substance Compliance** template besides the other required templates (as prompted) when creating the template project.

3. Access the **Advanced** perspective by choosing **Window→Open Perspective→Other→Advanced**.

4. Search for the **Scp0SubstanceCmplResult** object.

5. In the **Business Objects** tab, right-click **Scp0SubstanceCmplResult** and choose **Open**.

6. In the **Main** tab, in the **Business Objects Constants** table, select **Fnd0Icon** and click **Edit**.

7. In the **Modify Business Object Constant** dialog box, click **Browse** and select your icon of choice for the compliance result business object.

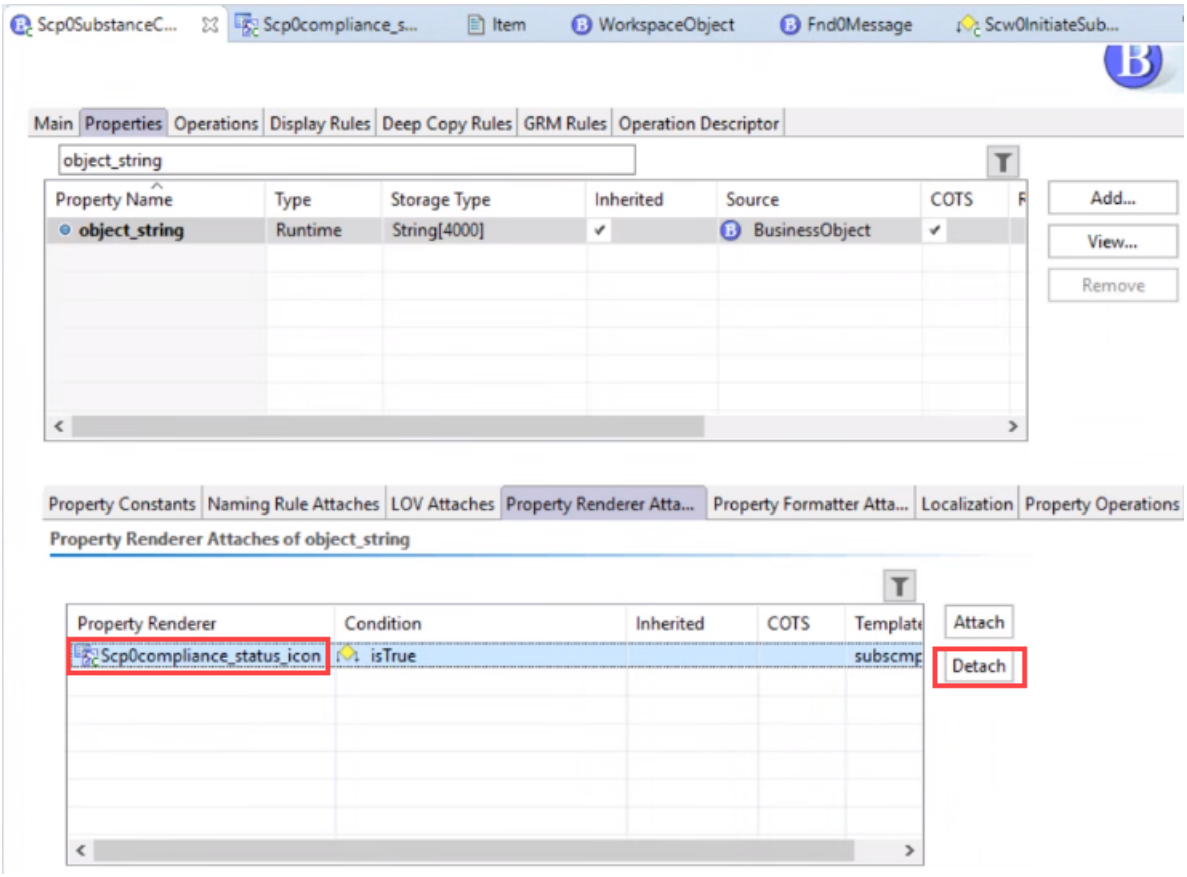
   The icon appears in the **Value** column of the **Fnd0Icon** business object constant row of the table.

8. To modify the icons for the different compliance statuses:

   a. In the **Properties** tab of the **Scp0SubstanceCmplResult** object, select the **object_string** row.

   b. From the **Property Renderer Attaches** tab of the **object_string** business object constant, get the name of the property renderer. In this case it is **Scp0compliance_status_icon**.

   c. Select the **Scp0compliance_status_icon** property renderer and click **Detach**.



d. To add custom compliance icons, create and attach a new property renderer to the **object_string** business object constant.

9. Choose **BMIDE→Save Data Model** to save the changes to the data model.

10. Choose **BMIDE→Deploy Template** to deploy the changes to the server.

25. Display or suppress Substance Compliance features on the user interface

By default, the *compliance officer* role performs various substance compliance-related activities.

You can display or suppress the available Substance Compliance features on the user interface for a specific Teamcenter user by using the Command Suppression application.

26. Set the expiration date for exemptions

Exemptions applied on parts have expiration dates after which they become invalid.

In some cases, the exemptions may not contain an expiration date. To ensure that all exemptions have valid expiration dates, you can specify the number of days after which an exemption will expire. To do this, set the value of the **SUBSCMPL_days_for_apply_exemption** preference to specify the number of days (typically set as 30, 90, or 180 days) after which the exemption expires.

In case an exemption contains an expiration date, this date overrides the number of days specified by the **SUBSCMPL_days_for_apply_exemption** preference.

27. Activate or deactivate sending emails to suppliers

Based on your organization's practices, as a compliance office, you may have to send emails requesting a supplier declaration, informing suppliers about the result of declaration import or validation, and so on.

Procedure

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

   > Note:
   >
   > You may need administrative privileges to set preferences.

2. Set the **SUBSCMPL_supplier_mail_functionality_activated** preference based on your organization's requirement.

Value	Purpose
true	Activates sending emails to suppliers.
false (default)	Deactivates sending emails to suppliers.

28. Set up the system to invalidate compliance results

Based on changes made to the properties of vendors parts or item revisions after a compliance check, the compliance results for those vendors parts or items should be considered invalid.

Based on your organizational practices, you can specify whether you choose to do this by setting the **SUBSCMPL_enable_compliance_results_inactivation** preference to *true* (default value) or *false*.

OOTB, the Substance Compliance solution provides a list of scenarios based on which the compliance results are invalidated. You can choose the scenarios for which you want the compliance results to be invalidated. To do this, specify the appropriate scenario numbers as values for the **SUBSCMPL_inactivate_compliance_results_triggers** preference.

The preference details provide a list of all scenarios for which compliance results can be invalidated.

Consider the scenario where you want to invalidate compliance results if the part mass has changed, a new substance is added to the material, or the substance composition of the material is changed. In this case, you set **SUBSCMPL_inactivate_compliance_results_triggers** to *1*, *17*, and *19*.

Value	Description
1	Implies that the part mass has changed. The **Mass** attribute on a part has changed.
17	Implies that a new substance is added to the material which is attached to the part.
19	Implies that the substance composition of the material which is attached to the part has changed.

In addition to the OOTB scenarios, based on the needs of your organization, you can add another scenario to the existing ones to invalidate compliance results:

- An attribute for the primary object (the vendor part or the item revision) to which compliance results are directly attached is modified, for example, a change in the unit of measure of the vendor part.
- An attribute for the secondary object (materials or smelters) that is related to the primary object is modified. This modification could be a change in the smelter address.
- An attribute for the tertiary object (a substance attached to a material revision) is modified, for example, a substance is removed from a material revision.
- An attribute for the primary-secondary relation, which links a primary and a secondary object, is modified. An example of this scenario is when the Mat1UsesMaterial relation (called as the primary

relation), which links the material revision to a part or item revision, is modified. This can occur when a new material is attached to the vendor part.

- An attribute for the secondary-tertiary relation, which links a secondary and a tertiary object, is modified. An example of this scenario is when the Mat1UsesSubstance relation (called as the secondary relation), which relates a substance to a material revision, is modified. This can occur when a substance is removed from a material that is attached to a vendor part.

Consider the scenario where you want to invalidate compliance results if the **Is Certified Smelter** attribute is changed for a smelter:

1. In BMIDE, search for the **Scp0InactiveSCResultReasons** LOV and add the scenario to it:

   - **Value**: A unique positive integer subsequent to the existing last scenario number. In this case, **37**.

   - **Description**: The condition for which you want to invalidate compliance results. In this case, **Is Certified Smelter attribute changed on Smelter related to vendor part**.

2. Search for the **Scp0InactivateComplianceResults** extension, and set the following:

   - **Object**: The Teamcenter object for which to invalidate compliance results. In this case, it will be **Scp0Smelter**.

   - **Property Name**: scp0IsCertifiedSmelter

   - **Operation Name**: PROP_set_value_logical

   - **Operation Type**: PostAction

3. Add the **Scp0InactivateComplianceResults** extension to the **Scp0Smelter** class by specifying the following:

Attribute	Value to specify
Declaration Type	Depending on the type of result that you want to inactivate, select *MSD* or *CMD*.
Inactivation Reason	Specify the value from the **cp0InactiveSCResultReasons** LOV.
Object Modified	Depending on the type of object, specify the appropriate value: • **P**: Indicates that an attribute of the primary object is being modified, or a primary relation is being created or deleted or that its attribute is being updated.

Attribute	Value to specify
	• **S**: Indicates that an attribute of the secondary object is being modified, or a secondary relation is being created or deleted or that its attribute is being updated. • **T**: Indicates that an attribute of the tertiary object is being modified.
Object Type	Based on the type, specify the appropriate value: • **O**: Use this for an object. • **R**: Use this for a relation.
Operation	Based on what action you want to implement on the attribute, specify the appropriate value: • **U**: Updates the attribute. • **C**: Creates a relation. • **D**: Deletes a relation.
Primary Relation Type	Specify the internal name of relation.
Secondary Relation Type	Specify the internal name of relation.

To invalidate compliance results when the **Is Certified Smelter** attribute is changed for a smelter, the appropriate values are as follows.

Attribute	Value to specify
Declaration Type	CMD
Inactivation Reason	37
Object Modified	S (Smelter is a secondary object related to the vendor part)
Object Type	O (#3 is an object)
Operation	U (The **scp0IsCertifiedSmelter** attribute is updated)
Primary Relation Type	Scp0PartToSmelterRel (relates a smelter to a vendor part)
Secondary Relation Type	Not required

29. Enable notifications for compliance checks

Based on your organization's practices, as a compliance officer, you can enable notifications on the completion of a compliance check, informing the users about the results by setting a preference. By default, the value of this preference is *false*, implying that these notifications are disabled.

Procedure

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

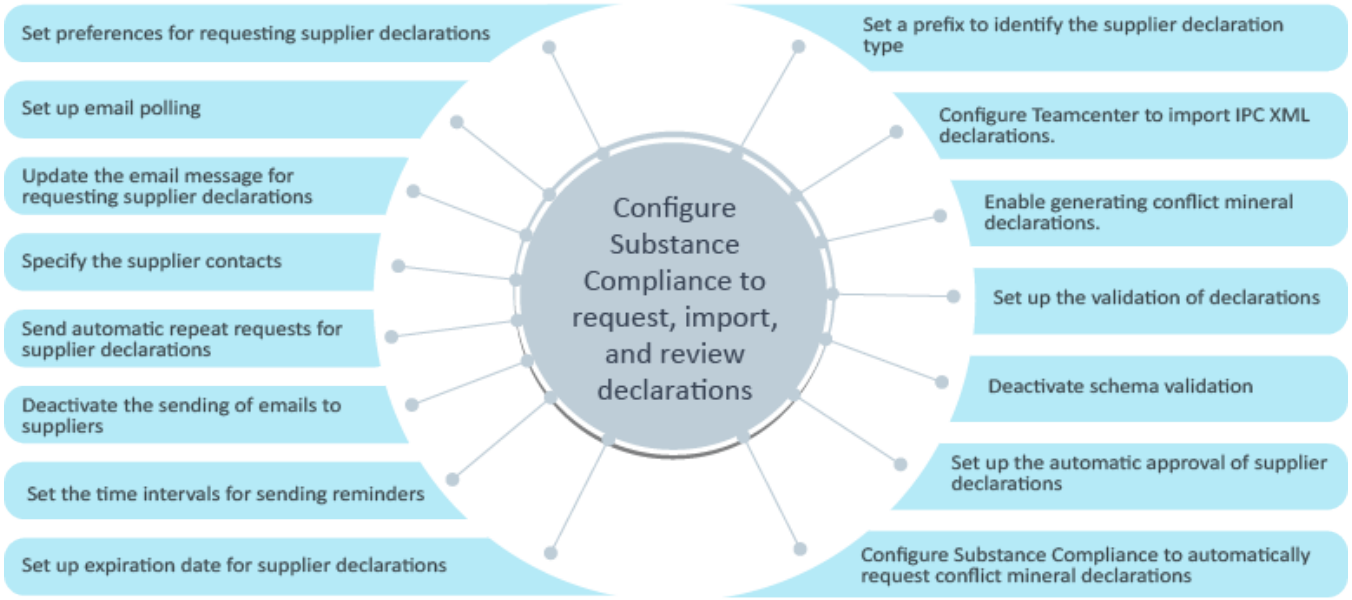
2. Set the **SUBSCMPL_enable_compliance_check_notification** preference based on your organization's requirement.

Value	Purpose
true	Enable notifications on the completion of a compliance check
false (default)	Disable notifications on the completion of a compliance check

30. Configuring Substance Compliance to request, import, and review supplier declarations

The tasks to configure Substance Compliance

Perform the following tasks to set up Substance Compliance to enable a compliance officer to use to request, import, validate, and review supplier declarations.



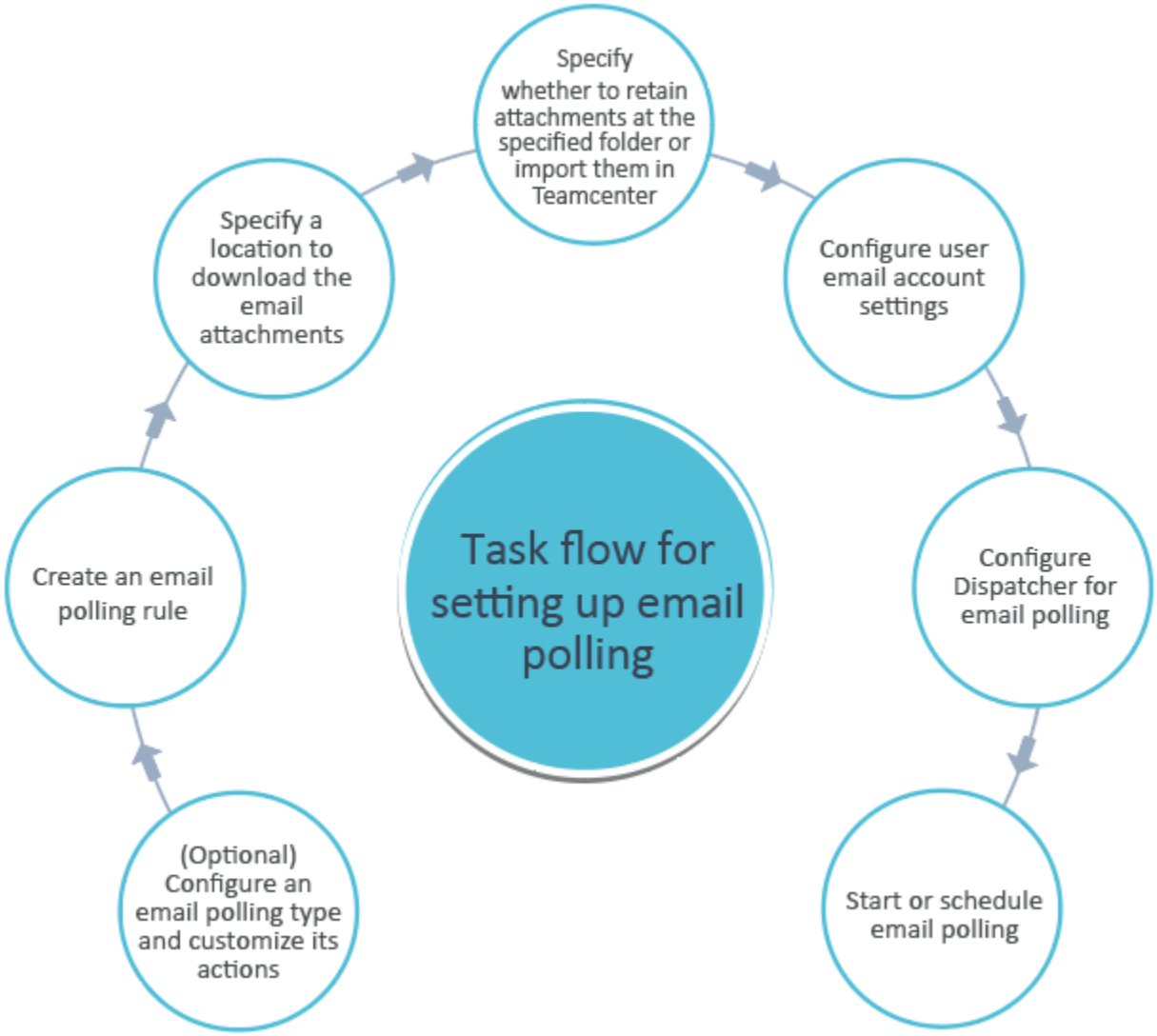
- **Set up email polling** to poll the email server at regular intervals to automatically download the declarations received from the suppliers.
- **Set preferences for requesting supplier declarations**.
- **Update the email message** for requesting supplier declarations.
- **Specify the supplier contacts** to whom the emails for requesting supplier declarations must be sent.
- **Send automatic repeat requests** for supplier declarations.
- **Deactivate the sending of emails** to suppliers.
- **Set the time intervals for sending reminders** to suppliers requesting declarations.
- **Set a prefix to identify the supplier declaration type**.

- Configure Teamcenter to **import IPC XML declarations**.
- Create an object in Teamcenter to **enable generating conflict mineral declarations**.
- **Set up the validation of declarations** sent by the suppliers.
- **Deactivate schema validation** for incoming supplier declarations.
- **Set up the automatic approval of supplier declarations** imported in Teamcenter.
- **Set up expiration date for supplier declarations**.
- **Configure Substance Compliance to automatically request conflict mineral declarations** if the material substance declaration contains any conflict minerals.

Setting up email polling

Workflow to set up email polling

Email polling is an asynchronous process that uses the standard Teamcenter Dispatcher services to poll the email server at regular intervals to automatically download the declarations received from the suppliers. The system uses a utility to poll the given email address at a specified frequency. To do this, it logs on using single sign-on (SSO) or uses the provided arguments. The utility obtains the other inputs from configuration settings.



To enable email polling, perform the following configurations:

1. (Optional) Based on the organization's requirements, you can configure an email polling type and then customize the actions performed by the type. The types are referenced by email polling rules.

   Substance Compliance provides you the following email polling types out of the box:

   - **msd**
   - **cmd**

2. Create an email polling rule to filter and validate Substance Compliance emails.

   An email polling rule distinguishes Substance Compliance emails from other Teamcenter emails and moves these emails to specific folders in an email client for processing.

3. Specify a location to download the email attachments in the **Email_polling_download_dir** preference.

4. Set the **EMLPOLLING_keep_review_mail_attachments** preference to:

   - **true** (default): The email polling facility will poll for and download attachments from incoming emails from the supplier at the location specified in the **Email_polling_download_dir** preference. The declarations are not imported in Teamcenter automatically.

     The compliance officer must import the *IPC XML* declarations in Teamcenter using any one of the available options.

     The synchronous import automatically creates Teamcenter objects, such as materials and substances, from the individual declaration files imported in Teamcenter. Additionally, the declaration and the materials and substances are automatically associated with the appropriate vendor part.

   - **false**: The email polling facility will poll for and download attachments from incoming emails from the supplier at the location specified in the **Email_polling_download_dir** preference. It then imports the *IPC XML* declarations in Teamcenter.

     The compliance officer must, however, run the **SUBSCMPL_import_supplier_declarations** command line utility in a managed mode (`mode=managed`) to complete the import action and associate the materials and substances with the appropriate vendor part.

5. Specify the details of the email server from where the material substance declaration must be downloaded.

   You must enable the Teamcenter polling functionality to communicate with an email server. Additionally, user email account information must be specified before starting or scheduling email polling.

6. Specify the email polling settings for Dispatcher to activate the **EmailPollingService** service.

7. Enable email polling to collect email responses.

   Enable email polling to automatically download material substance declarations received from the suppliers to a specific location. You can schedule when the email server must be polled to download the material substance declarations. You must also specify which email polling rule to use to filter and validate incoming supplier declaration emails.

Configure email polling types

System administrators or customizers configure email polling types and can customize the actions performed by a type. The types are referenced by email polling rules.

Prerequisites

- Teamcenter is installed and configured to work correctly.
- BMIDE is installed and is working property.
- The system administrator or customizer performing the configuration:
  - has sufficient privileges (dba) to create and install templates or make changes to the Teamcenter database.
  - has write access to all Teamcenter installation folders.
- If scheduled polling using Teamcenter Dispatcher is to be used, when installing or updating Dispatcher, in the **Select Translators** panel, **Email Polling→Email Polling** is selected.

Configuration steps

1. In BMIDE, for the e-mail polling type that you want to configure:
   a. Create or open a template project.
   b. In the classic LOV list **Fnd0EmailResponseTypes**, create a list value to identify the polling type that you want to define.

      Only the *value* parameter of the list value is used for polling; its *description* and *condition* parameters are not used.
   c. If in your application you want to persist more data than just e-mail body text and attachments, or to impart additional behavior, then create a subtype of the object **Fnd0EmailResponseRecord**.

      Add your custom actions to your new object subtype.
   d. Save and deploy the template.
2. In the rich client:
   a. Log on using an account with dba privileges.
   b. Choose **Edit→Options**.
   c. Find the preference **Email_polling_download_dir**, and set the preference value to the desired location for downloaded attachments in the server's file system. This location is used by all email polling types.

The specified location must exist in the server's file system; the polling functionality does not create the folder.

d. For each value that you added to the classic LOV list **Fnd0EmailResponseTypes**, do the following:

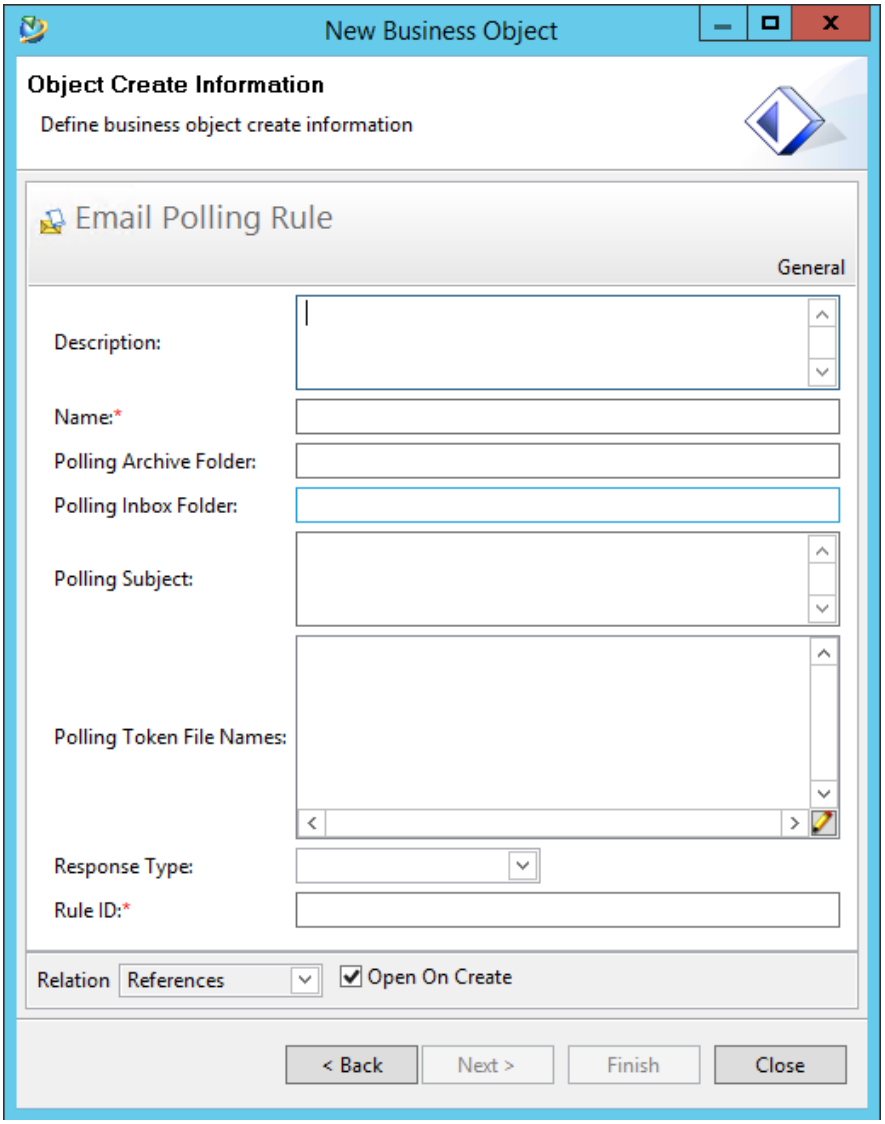
   A. Create a new preference named *<LOV value>***_Response_Record_Object**.

   B. Set the preference value to **Fnd0EmailResponseRecord** or, if you created a subtype of the object **Fnd0EmailResponseRecord** and you want to associate the LOV value with that object subtype, set the preference value to the name of the object subtype.

Create an email polling rule

Business users create email polling rules to configure checks for incoming email messages and attachments, and to specify the polling type to apply to qualified messages. Multiple rules can use the same polling type.

1. In My Teamcenter, choose **File→New→Other→Email Polling Rule**.



2. In the **Email Polling Rule** dialog box, enter the following information.

Field	Description
Description	A brief description of the email polling rule and its usage.
Name	A name for the email polling rule.
Polling Archive folder	The destination user email folder for archived email messages. The folder must exist. The polling functionality does not create the folder.
Polling Inbox folder	The email user folder containing the messages to test.

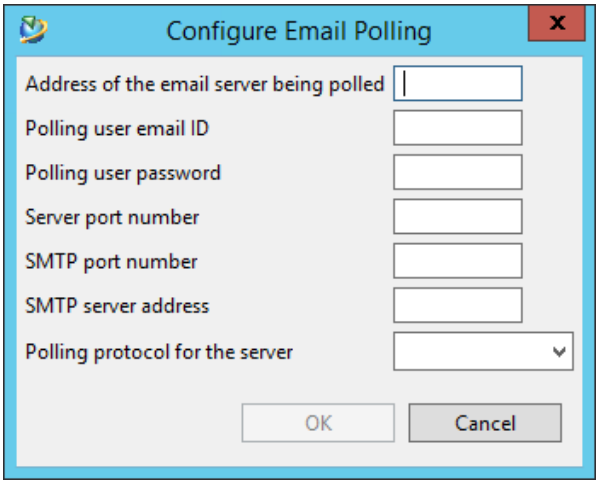
Field	Description
Polling Subject	The words at the beginning of the email message subject that qualify it for action by the rule.
Polling Token File Names	The names of files provided to responders for required attachment to response emails. Required attachments may include digitally signed request-identification-documents or pre-encrypted binary files. Token files are a means of enhancing security. Leave blank if token files are not used.
Response Type	The type of email response to which this rule applies. This is a value contained in the application template classic LOV (list of values) **Fnd0EmailResponseTypes** as configured by the system administrator/ customizer. For Substance Compliance emails, you must select **MSD** as the response type.
Rule ID	The ID for the newly created rule. The ID is used to identify the rule when starting email polling.

3. Click **Finish**.

Configure user email account settings

To enable Teamcenter polling functionality to communicate with an email server, user email account information must be specified before starting or scheduling email polling.

1. In My Teamcenter, choose **Tools→Email Polling→Configure Email Polling**.



2. In the **Configure Email Polling** dialog box, enter the following information:

Field	Description
Address of the email server being polled	The address of the email server for your email account. Example: mycasa001.net.acme.com
Polling user email ID	Your email account address. Example: john.smith@acme.com
Polling user password	The password for your email account.
Server port number	The email server port number for messages sent to your account (incoming). Example: 993
SMTP port number	The email server port number for uploading messages that you want to send from your account (outgoing).

Field	Description
	Example: 465
SMTP server address	The host name of the SMTP (Simple Mail Transfer Protocol) server for outgoing mail. Example: smtp.acme.com
Polling protocol for the server	The protocol for connecting with the email server, either **POP3** or **IMAP**.

3. Click **OK**.

Configure Dispatcher for email polling

Note:

Dispatcher settings for email polling may have been set by Teamcenter Environment Manager (TEM). In that case, confirm the following configuration.

1. To activate the **EmailPollingService** service, set the **isactive** attribute to **true** in the *DISP_ROOT***Module\conf\translator.xml** file.

```
<EmailPollingService provider="SIEMENS" service="emailpolling" isactive="true">
```

Note:

DISP_ROOT is the dispatcher root directory provided in Teamcenter Environment Manager (TEM).

2. In the *DISP_ROOT***Module\Translators\emailpolling\emailpolling.bat** file, set the following variables to your installation locations:

   - *TC_ROOT*
   - *TC_DATA*
   - *JRE_HOME*

3. In the *TC_DATA***EmailPolling.conf** file, remove the comments before these settings:

- **EmailPolling_JAVA_XMS=16m**
- **EmailPolling_JAVA_XMX=128m**

4. Run the **genregxml.bat** utility.

   - Open a Teamcenter command prompt and type the following command:

     TC_ROOT`\portal\registry\genregxml.bat`

5. For each Teamcenter user who performs email polling actions, set the **E-Mail Address** property.

   a. Using an account with dba privileges, log on to the rich client and open the Organization application.

   b. Expand the **Persons** node and select the person who performs email polling actions.

   c. Set the **E-Mail Address** property.

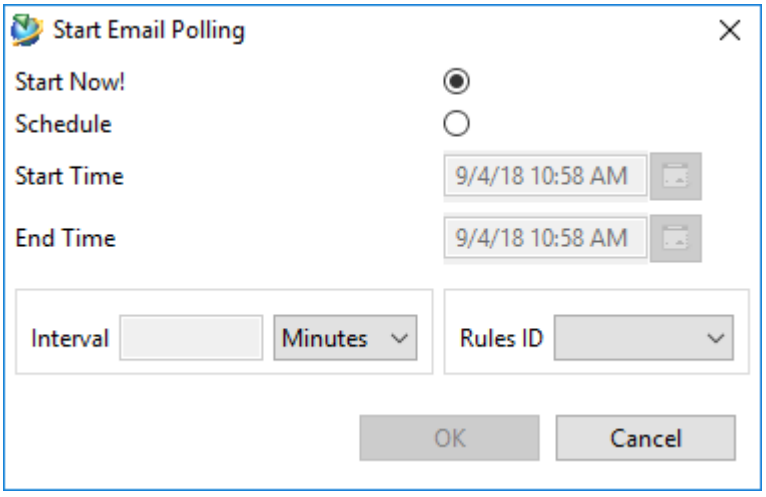
Start or schedule email polling

Prerequisites

- **User email account information is configured**
- **Dispatcher is configured for email polling**

Procedure

1. In My Teamcenter, choose **Tools**>**Email Polling**>**Start Email Polling**.



2. In the **Start Email Polling** dialog box, enter the following information:

Field	Description
Start now! **Schedule**	Select one of these choices. • **Start now!** runs a single on-demand poll. • **Schedule** enables scheduling periodic polling.
Start Time	The date and time to start scheduled polling.
End Time	The date and time to end scheduled polling.
Interval	The interval of time to repeat the poll.
Rules ID	The ID of the email polling rule to use.

3. Click **OK**.

You can administer scheduled polling requests using the Dispatcher request administration console.

Set preferences for requesting supplier declarations

The Teamcenter Substance Compliance solution supports the following formats for declarations.

Declaration type	Supported formats
Material substance declaration (MSD)	IPC XML
Lab report	IPC XML
Conflict mineral declaration (CMD)	IPC XML (default format) Microsoft Excel

Set the following preferences to specify the options for requesting supplier declarations.

> Note:
>
> Currently, you cannot request declarations for lab reports.

Preference	Description
Preferences for MSDs	
SUBSCMPL_request_msd_mode	Specifies that an IPC XML file is the mode of requesting a declaration. **Valid values: 1**
SUBSCMPL_msd_-always_send_blank	Specifies whether to: • Send a blank IPC XML document to the supplier on the first and subsequent MSD requests. Or • Send a blank IPC XML document on the first MSD request and the most recently declared IPC XML document for the subsequent requests. **Valid values:** **true** **false**
SUBSCMPL_msd_-default_xml_file	Specifies the default IPC XML file name for an MSD request. **Valid values: IPC_1752A.xml** Default file name: **IPC_1752-2v1.1.xml**
SUBSCMPL_msd_request_xsl_file	Specifies the path to the XSL file used to convert the TC-XML file into an XML file for requesting the MSD. The list of valid values is as follows:

Value	Meaning
File path to *tcxml_to_msd_request_1752a.xsl*	Use this *XSL* if the **SUBSCMPL_request_msd_format** preference specifies the **IPC_1752A** value. This is the default value. Example, *%TC_DATA%\subscmpl_data\xsl\tcxml_to_msd_request_1752a.xsl*
File path to *tcxml_to_msd_request_1752_2v1_1.xsl*	Use this *XSL* if the **SUBSCMPL_request_msd_format**

<table>
<tr><th>Preference</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td></td><td>preference specifies the IPC_1752-2 value.</td></tr>
<tr><td>File path to tcxml_to_msd_request_1752b.xsl</td><td>Use this XSL if the SUBSCMPL_request_msd_format preference specifies the IPC_1752B value.</td></tr>
</table>
</td></tr>
<tr><td>SUBSCMPL_msd_-default_pdf_file</td><td>Specifies the default IPC 1752-2 v1.1PDF file name for an MSD request.

As the IPC 1752-2 v1.1 PDF template does not get installed by default, you must copy the IPC 1752-2 v1.1 PDF template to TC_DATA. Next, specify the file name of the IPC 1752-2 v1.1 PDF template as the value.

Valid values: Any valid file name with the .pdf file name extension.</td></tr>
<tr><td>SUBSCMPL_msd_-include_pdf</td><td>Specifies whether to send a blank IPC PDF file to the supplier along with the IPC XML document as a part of the MSD request.

Valid values:

true

false</td></tr>
<tr><td>SUBSCMPL_request_-msd_format</td><td>Specifies whether to send the MSD in the IPC 1752A XML format or the IPC 1752-2 v1.1 format or IPC 1752B XML format.

Valid values:

IPC_1752A (default format)

IPC_1752-2

IPC_1752B</td></tr>
<tr><td colspan="2">Preferences for CMDs</td></tr>
<tr><td>SUBSCMPL_request_cmd_mode</td><td>Specifies the mode in which to request a declaration.

Valid values:

1: Set the request mode as IPC XML (default mode).</td></tr>
</table>

Preference	Description
	0: Set the request mode as Microsoft Excel.
SUBSCMPL_cmd_-always_send_blank	Specifies whether to: • Send a blank IPC XML document to the supplier on the first and subsequent CMD requests. Or • Send a blank IPC XML document on the first CMD request and the most recently declared IPC XML document for the subsequent requests. **Valid values:** **true** **false**
SUBSCMPL_cmd_-default_xml_file	Specifies the default IPC XML file name for a CMD request. **Valid values: IPC_1755.xml** (default file name)
SUBSCMPL_cmd_-default_excel_file	Specifies the default Microsoft Excel file name for a CMD request.

Update the email message for requesting declarations

You can update the body of the email message sent to the suppliers, requesting for the declarations, such as material substance declaration (MSD) and conflict mineral declaration (CMD).

> Note:
>
> Request emails are not sent to suppliers for lab reports.

To update the message, change the values of the following keys in the *TC_ROOT***lang\textserver***language**\subscmpl_text_locale.xml** file.

```
<!--Messages for Request Substance Declaration Email-->
<!--This line will form the salutation using contact details.
The arguments are Title, First Name and Last Name respectively.-->
<key id="k_subscmpl_MSD_req_salutation">%1$ %2$ %3$,
</key>
<key id="k_subscmpl_MSD_req_body">Please provide the substance declaration
details for the Parts listed in the attached Excel file.</key>
<key id="k_subscmpl_MSD_req_supplier">Supplier</key>
```

```
<key id="k_subscmpl_MSD_req_subject">Request for substance declaration of
Parts to Vendor Name</key>


**********************************************************************
**
      This is system generated message. Please do not reply.

**********************************************************************
**



<key id="k_subscmpl_MSD_IPC_req_body">You have received this notification,
because your part or component is under consideration for use by the Company
Please provide the substance declaration details for the Parts listed
in the attached IPC XML files based on IPC 1752A standard. The attached
XML files may be imported to IPC generator tool to further edit.the contents.
Once finalized, the data needs to be saved and exported as an IPC XML file.</key>
<key id="k_subscmpl_MSD_polling_info_body">Please send the filled
Material Substance Declaration (MSD) XML files back to the
following email address:
%1$. Any supporting documents should also be sent back through
the same response email.
Please DO NOT reply to this email. Please set the subject of your
response email to "Response for substance declaration".
<key id="k_subscmpl_vendorPart_list">List of Part:</key>
<key id="k_subscmpl_vendorPart_dueDate">Request Due Date:</key>
```

Next, clear your web browser cache before you launch the Teamcenter Substance Compliance solution.

Specify supplier contacts for sending declaration request emails

To specify supplier contacts to whom the supplier declaration request emails must be sent:

1. In **My Teamcenter**, search for **Company Contact**.
2. Copy the company contact you wish to associate the supplier with.
3. Choose **Edit→Paste Special→Paste as** and select one of the following options:
   - **MSD Contact**
   - **CMD Contact**

Send automatic repeat requests for supplier declarations

There may be situations in which the supplier must resubmit a declaration: for example, in cases where the request expires, the declaration itself expires, or if the declaration was rejected earlier. In such cases, the compliance officer can manually schedule another request for the declaration.

> Note:
>
> Request emails are not sent to suppliers for lab reports.
>
> This functionality is not available for lab reports.

To automate repeat requests, you can use the **subscmpl_process_declaration_reminders** utility:

```
subscmpl_process_declaration_reminders -u=tcadmin -p=tcadmin -encrypt=true
-type=MSD
```

Deactivate the sending of emails to suppliers

By default, as an administrator, you get an email when a supplier declaration, such as a material substance declaration (MSD) or a conflict mineral declaration (CMD) import in Teamcenter fails.

As a supplier, you get an email when:

- The validation of an MSD or CMD fails.
- The MSD or CMD is approved.
- The compliance officer reviews and rejects the MSD or CMD.

> Note:
>
> The email functionality is not available for lab reports.

As an administrator, you can disable sending email notifications to suppliers by setting the **SUBSCMPL_supplier_mail_functionality_activated** preference to **false**.

Set time intervals for sending request reminders to suppliers

Once you send a request for a supplier declaration, you can send reminder mails to the suppliers as a follow up. You can set this up in one of two ways.

Note:

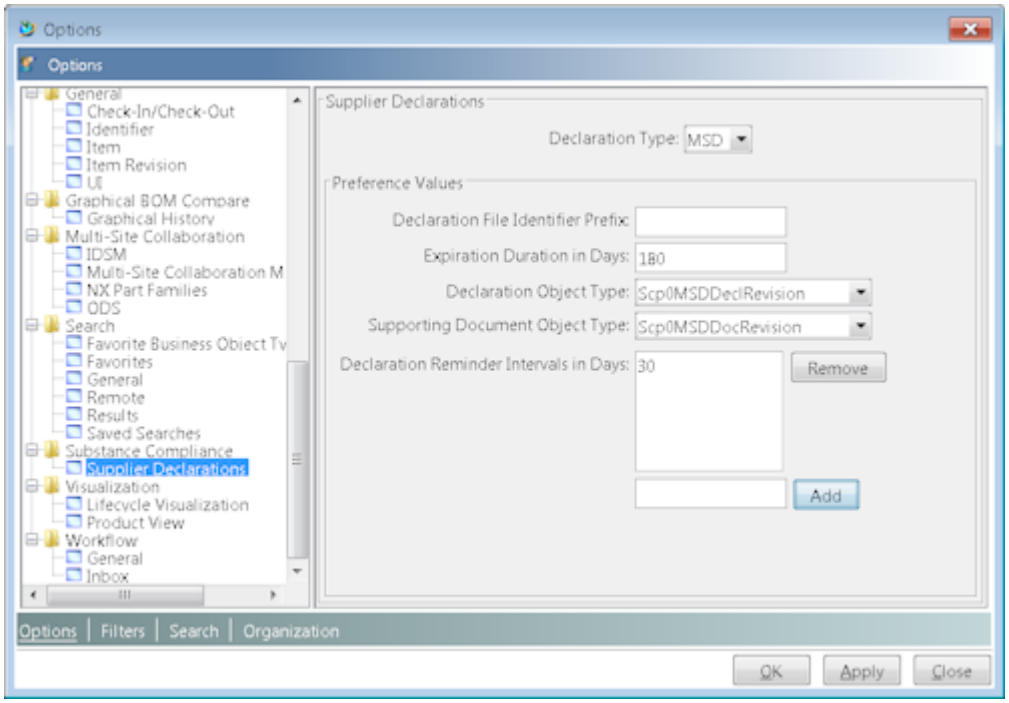
This functionality is not available for lab reports.

- You can set the relevant preference: **SUBSCMPL_CMD_reminder_intervals** for conflict mineral declarations (CMDs) and **SUBSCMPL_MSD_reminder_intervals** for material substance declarations (MSDs).

- You can specify the duration as follows:

  1. Choose **Edit→Options→Substance Compliance→Supplier Declaration**.

  2. In the **Supplier Declarations** dialog box, enter the following information:



Field	Action
Declaration Type	Select the type of supplier declaration: MSD or CMD.
Expiration Duration in Days	Enter the duration for when the MSD or CMD will expire.
Declaration Object Type	Select the object type based on whether the declaration is an MSD or CMD.

Field	Action
	If not sure of which object type to choose, retain the default values.
Declaration Reminder Intervals in Days	Enter a value to denote the number of days before the declaration expires, when a reminder should be sent for a new declaration. Click **Add**. For example: Consider that the reminder interval is set to 60 days. Now, a reminder will be sent for a new declaration on March 1, when the expiry of the declaration is on May 1. You can specify multiple values for repeat reminders or remove existing values for reminders.

3. Click **Apply** and **OK**.

Set a prefix to identify the supplier declaration type

You must specify a prefix for identifying a substance declaration received from the supplier. You can do this by setting the following preferences.

Declaration	Preference	Prefix value
Material substance declaration	**SUBSCMPL_MSD_declaration_file_prefix**	**IPC_**
Lab report	**SUBSCMPL_LRD_declarations_file_prefix**	**LRD_**
Conflict mineral declaration	**SUBSCMPL_CMD_declarations_file_prefix**	**CMRT_**

1. Choose **Edit→Options→Substance Compliance→Supplier Declarations**.

2. In the **Supplier Declarations** dialog box, enter the following information:

Field	Value
Declaration Type	Select the option to select the type of vendor declaration. You can choose either MSD, LRD, or CMD.
Declaration File Identifier Prefix	(Optional) Specify a prefix for the substance declaration file, for example, IPC.

3. Click **Apply** and click **OK**.

Configure Teamcenter to import IPC XML declarations

Perform the following steps to enable importing IPC XML declarations:

1. Update the following preferences to specify the locations that the IPC XML documents will be copied to during the import of declarations received from the suppliers. Though the preference name is **SUBSCMPL_msd_*_dir**, these preferences support material substance declarations (MSDs), conflict mineral declarations (CMDs), and lab reports.

Preference	Description	Values
SUBSCMPL_msd_-processing_dir	Specifies the location of the processing directory to which all the files are first moved while importing the declarations.	Any valid directory string. The default value is *import directory***processing**. Example: *C:\SC\Import\processing*
SUBSCMPL_msd_-done_dir	Specifies the location of the final directory to which all the files are moved after successfully importing the declarations.	Any valid directory string. The default value is *import directory***done**. Example: *C:\SC\Import\done*
SUBSCMPL_msd_-error_dir	Specifies the location of the directory to which all the files are moved in case the import of the declaration fails.	Any valid directory string. The default value is *import directory***error**. Example: *C:\SC\Import\error*

2. If you want to configure Teamcenter for scheduling the import of declarations at a specific time, update the *subscmplmsdimport.bat* file located at *C:\apps\tc\tc2412\DR\Module\Translators\subscmplmsdimport*.

   a. Specify the user credentials in the `"%TC_ROOT%\bin\subscmpl_import_supplier_declarations.exe"` utility.

b. Specify the appropriate `mode` based on the requirement of your organization:

- *file*: To import a specific file.
- *directory*: To import all files in a specific directory.

c. Specify the `type` of declaration; for example, **MSD**.

d. Specify the `path` of the file (or all files in the directory) to be imported.

For example, `"%TC_ROOT%\bin\subscmpl_import_supplier_declarations.exe" -u=username -p=password -g=Engineering -mode=file -type=MSD -path="C:\sc\Import\lamp.xml"`.

3. Ensure that the scheduler, module, and Dispatcher Client services are started.

4. Specify the prefix of the import files as the value for the **SUBSCMPL_<declaration_type>_declaration_file_prefix** preference. Here, **<declaration_type>** could be *MSD*, *CMD*, or *LRD*.

The default value for the **SUBSCMPL_MSD_declaration_file_prefix** preference is **IPC_**. This means that all files with a prefix **IPC_** in the specified directory will be processed. For the **SUBSCMPL_CMD_declaration_file_prefix** preference, the default value is **CMRT_** and for the **SUBSCMPL_LRD_declaration_file_prefix** preference, the default value is **LRD_**.

Note:

To import the IPC XML declarations with exemption, specify the list of regulations which are considered for exemption validation as the value for the **SUBSCMPL_msd_exemption_validation_regulation_list** preference. Valid values are in the format *RegulationName:RegulationVersion*.If no value is specified, the exemption validation fails. For example, **RoHS EU:1907**.

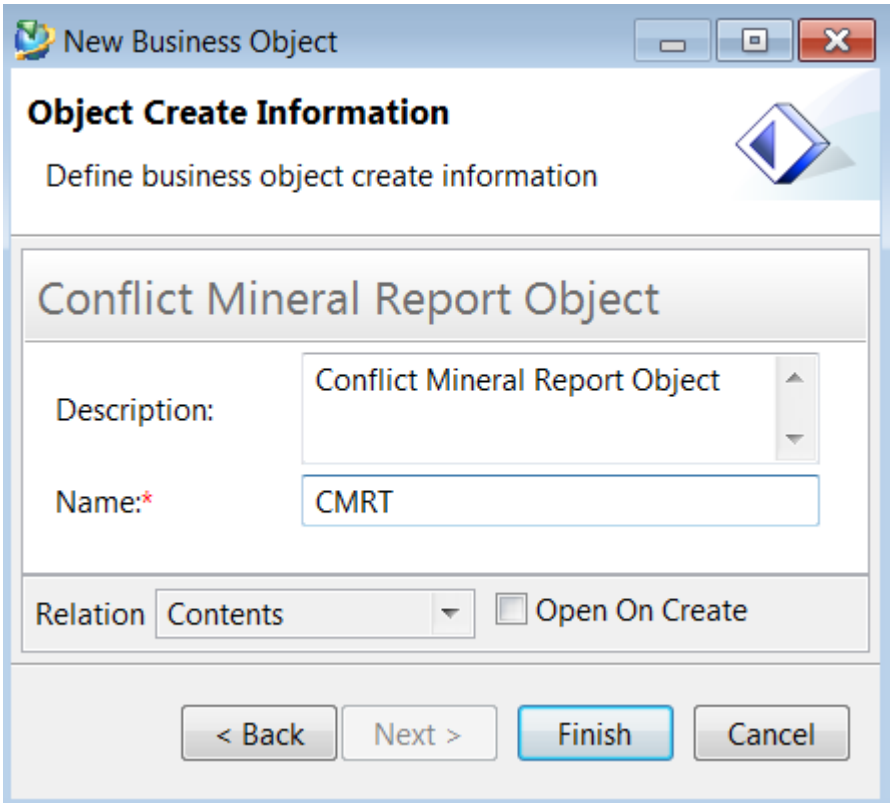
Configure Teamcenter for generating conflict mineral declarations

If the parts supplied by your company use any of the 3TG metals (tin, tantalum, tungsten, and gold) or their alloys, a compliance officer must send a conflict mineral declaration (CMD) to the OEM specifying the different 3TG metals.

To be able to do so, a Teamcenter object must pre-exist to which the CMD can be linked. As an administrator, you need to create a conflict mineral report object in Teamcenter to enable the compliance officer to generate a CMD, if required.

1. Choose **File→New→Other** and search for **Conflict Mineral Report Object**.

2. Select **Conflict Mineral Report Object** and click **Next**.



3. Provide the **Description** and the **Name** for the object.

4. Click **Finish**.

Validate the declarations sent by suppliers

Declarations such as material substance declaration (MSD) or conflict mineral declaration (CMD) sent by the suppliers are downloaded from the email server to a specific location that you set while creating the email polling rule. An email is sent to the supplier acknowledging the receipt of the declaration and that its validation is in process.

Any exemption mentioned in the declaration (IPC file) must match the substance category for which it is to be applied. For example, if the substance is cadmium, some of the applicable RoHS exemptions are 8(a), 8(b), and 13(b). If the IPC file contains any other exemptions, these are invalid. To perform this validation, ensure that the **SUBSCMPL_msd_enable_exemption_validation** preference is set to **true**. If there is a mismatch in the exemption provided by the supplier and the substance category, an error is reported in the validation log file.

When the declarations are saved at the specified location, a task to validate the declarations is available in your worklist. Go to the location, run a virus scan, and validate the declarations. Once this is done, complete the task available in your worklist as follows:

1. In **My Teamcenter**, click **My Worklist→Tasks To Perform→Review Mail Attachments**.

2. In the **Summary** tab, click **Actions→Perform**.

3. In **Email Polling Rev Form**, select a declaration and choose **Approve** or **Reject**.

4. Click **Complete** and then click **OK**.

On completing the validation task, if you wish to notify the suppliers of the validation results, set the **SUBSCMPL_notify_suppliers_validation_verdict** preference to **Yes**.

Deactivate schema validation for incoming material substance declarations

The supplier declaration validation process verifies whether the information in the material substance declaration (MSD) received from the supplier is correct and complete.

To deactivate the schema validation for incoming MSD declarations, set the **SUBSCMPL_IPC1752_perform_schema_validation** preference to **false**.

Set up the approval of supplier declarations

By default, the imported supplier declarations, such as the material substance declaration (MSD), the conflict mineral declaration (CMD), or lab reports are in an *unapproved* state and must be approved manually. However, based on your organization's practices, you can set the declaration to be approved automatically during import.

To enable the end users to approve a supplier declaration manually, you must add them to the group and role set for implementing the Substance Compliance solution, for example, a *compliance officer* role. All users belonging to this group and role can then approve the supplier declarations irrespective of who imports the declarations in Teamcenter.

To approve a declaration automatically, set the following preferences to **true**:

- **SUBSCMPL_MSD_auto_approve**
- **SUBSCMPL_LRD_auto_approve**
- **SUBSCMPL_CMD_auto_approve**

Now, the declarations are automatically approved during import, the part to material relationship is created in an approved state, and an email is sent to the supplier (not applicable for lab reports), notifying that the declaration is approved.

Set up expiration date for supplier declarations

Material substance declarations (MSDs) expire after a time period specified by your organization. Set the **SUBSCMPL_MSD_expiry_duration** preference to specify, in days, when an MSD should expire.

Configure Substance Compliance to send automatic requests for conflict mineral declarations

When a material substance declaration (MSD) listing a conflict mineral is approved, a conflict mineral declaration (CMD) request must be sent to the supplier to obtain the smelter information.

You can set the CMD request to be sent automatically on MSD approval by setting the **SUBSCMPL_cmd_auto_request_on_msd_approve** preference to **true**.

31. Troubleshoot Substance Compliance

The following table lists some problems, which you may encounter while working with the Substance Compliance solution, and their resolutions.

Problem	Solution
While performing a substance compliance check, Compliance Process Manager (CPM) stops responding intermittently and does not send the compliance status to Teamcenter.	Clear the Teamcenter Integration Framework server data: 1. Stop the Teamcenter Integration Framework server. 2. Clear the contents from the following directories by deleting them: • */container/activemq-data* • */container/data* • */container/log* • */container/logs* 3. Restart the Teamcenter Integration Framework server. Clear the CPM server data: 1. Stop the CPM server. 2. Clear the contents from the following directories by deleting them: • */CPM_HOME/data* • */CPM_HOME/logs* • */CPM_HOME/temp* • */CPM_HOME/work* 3. Delete the folder */CPM_HOME/webapps/cpm*. 4. Start the CPM server.

Problem	Solution
	5. Restart Pool Manager.
After installing a new Teamcenter patch, you are unable to log on to the Teamcenter Integration Framework web console to **set up the connection with the Compliance Process Manager** site.	Reinstall the Teamcenter Integration Framework in the existing Teamcenter environment.

32. Action handlers in Substance Compliance

List-Vendor-parts-and-vendors

Description

The **List-Vendor-parts-and-vendors** handler is used by the **Request Substance Declaration** workflow.

For a given item revision or a BOM, the action handler:

- Traverses the item revision or BOM attached to the workflow process and extracts (retrieves) all those vendor parts that are related to the item revision or the BOM using the **VMRepresents** relation. For a conflict mineral declaration request for a particular vendor, the handler retrieves a vendor object.
- The handler then saves the retrieved information in the **Scp0ReqSubsDeclForm** form.

> Caution:
>
> Do not add this handler to any other workflow process template.

Syntax

List-Vendor-parts-and-vendors

Arguments

None.

Placement

By default, this handler is placed in the correct location of the **Request Substance Declaration** workflow process template. Do not change the placement.

Restrictions

Adding this handler to any other workflow process template may result in errors.

Perform-Compliance-Check

Description

Performs substance compliance check on the target attachment objects. The handler accepts one or more objects.

Syntax

Perform-Compliance-Check

Arguments

None.

Placement

Place on the **Complete** action.

Restrictions

Requires Compliance process manager is configured in the environment.

Populate-Material-Substance-Declaration-Form

Description

Adds the material and substance details to the declaration form available in the compliance officer's review task list. Details about the materials and substances in the part, including the mass and unit of measure are added to the **Review Substance Declaration Form**.

> Caution:
>
> Do not add this handler to any other workflow process template.

Syntax

Populate-Material-Substance-Declaration-Form

Arguments

None.

Placement

By default, this handler is placed in the correct location of the **Review Substance Declaration** workflow process template. Do not change the placement.

Restrictions

Adding this handler to any other workflow process template may result in errors.

Review-Substance-Declaration

Description

Reviews the declaration sent by the supplier to ensure that the information is correct and complete. Verifies that all stakeholders have signed off on the declaration. Once the review is complete:

- It adds the property and relation values from the part declaration and part declaration revision to the vendor part in Teamcenter.
- If auto compliance check is set to **true**, it sends the part for a compliance check.
- It adds a release status of approved or rejected to the part declaration revision in Teamcenter.
- It sends an approval status email to stakeholders if the **SUBSCMPL_mail_approval_status** preference is set to **true**.

> Caution:
>
> Do not add this handler to any other workflow process template.

Syntax

Review-Substance-Declaration

Arguments

None.

Placement

By default, this handler is placed in the correct location of the **Review Substance Declaration** workflow process template. Do not change the placement.

Restrictions

Adding this handler to any other workflow process template may result in errors.

Update_Compliance_Result

Description

Updates the substance compliance result status and the exemption remark on the compliance result object in Teamcenter and displays the compliance result and the applied exemption in the **Compliance** tab. Additionally, the handler also relates the applied exemption to the compliance result for the selected regulation.

> Caution:
>
> Do not add this handler to any other workflow process template.

Syntax

Update_Compliance_Result

Arguments

None.

Placement

By default, this handler is placed in the correct location of the **Apply Exemptions** workflow process template. Do not change the placement.

Restrictions

Adding this handler to any other workflow process template may result in errors.

33. Deploying Substance Compliance documentation on your local drive or network

You can deploy the Substance Compliance documentation on your local drive or network. See the **Siemens Help Server documentation** for instructions to deploy the documentation on your local drive or network.

34. Delete the declaration data

You can delete the declaration documents or imported declaration records depending on their status or date range.

1. Open the **Active Admin** workspace.

2. Click the **DELETE DECLARATION DATA** tile.

3. Select the criteria for the deletion of data and its date range.

   You can either specify the date range or enter the **End Date**. Doing so deletes all the data for the given criteria present in the system till **End Date**.

   Imported Declaration Records option is for deleting to all the failure records listed on the **Failures** tab of the **Declarations** page which qualify the given date criteria. It will also delete associated records like related **Reference Records**, **Declaration File** and **Failure Logs**.

   Choose the **Imported Declaration Records** option to delete all the failure records listed on the **Failures** tab of the **Declarations** page, which meet the given date criteria. It also deletes associated records such as related **Reference Records**, **Declaration File**, and **Failure Logs**.

4. Click **Delete**.

> Note:
>
> You can also use the **subscmpl_purge_supplier_declarations** utility to delete the declaration data.

A. Substance Compliance utilities

email_polling

Performs email polling using a specified rule. The email_polling utility is useful for testing polling configuration, or can be called by a cron job as an alternative to using Teamcenter Dispatcher.

PREREQUISITES

- Email polling type is configured.
- Email polling rule is created.
- Email polling settings are configured.

SYNTAX

email_polling [**-u=***user-id* {**-p=***password* | **-pf=***password-file*} **-g=***group-name*]
[**-rule_id=***email poll rule object ID*] [**-h**]

ARGUMENTS

-u

Specifies the user ID.

This is a user with Teamcenter administration privileges. If this argument is used without a value, the operating system user name is used.

> Note:
>
> If Security Services single sign-on (SSO) is enabled for your server, the **-u** and **-p** arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-p

Specifies the user's password.

If used without a value, the system assumes a null value. If this argument is not used, the system assumes the *user-ID* value to be the password.

This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file. If used without a value, the system assumes a null value. If this argument is not used, the system assumes the *user-ID* value to be the password.

For more information about managing password files, see *Manage password files*.

This argument is mutually exclusive with the **-p** argument.

-g

Specifies the group associated with the user.

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

-rule_id

Specifies the email poll rule object id.

-h

Displays help for this utility.

ENVIRONMENT

As specified in Manually configure the Teamcenter environment..

FILES

As specified in Log files produced by Teamcenter.

RESTRICTIONS

None.

EXAMPLES

- To poll an email folder using the **CustomApplicationRule1**:

```
email_polling -u=myusername -p=mypassword -rule_id=

CustomApplicationRule1
```

subscmpl_import_supplier_declarations

Imports supplier declarations into Teamcenter.

SYNTAX

SUBSCMPL_import_supplier_declarations
[**-u**=*user-id*
{**-p**=*password* | **-pf**=*password-file*}
[**-g**=*group*]
[**-xsl**=*xsl-file-path*]
[**-path**]
[**-mode**]
[**-decl_type**]
[**-h**]

ARGUMENTS

-u

Specifies the user ID.

This is a user with Teamcenter administration privileges.

> Note:
>
> If Security Services single sign-on (SSO) is enabled for your server, the **-u** and **-p** arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-p

Specifies the password.

This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file.

This argument is mutually exclusive with the **-p** argument.

-g

Specifies the group associated with the user.

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

-xsl

Specifies the absolute file name of the *xsl* file.

-path

Specifies the path of the directory that contains the supplier declaration file and supporting files.

-mode

Specifies whether to run the utility in managed, file, or directory modes.

- **managed**: Use the **managed** mode to import declarations using the email polling functionality.
- **file**: Use the **file** mode to select and import a single declaration.
- **directory**: Use the **directory** mode to import all declarations in the specified directory.

-decl_type

Specifies the type of the supplier declaration to be imported.

-h

Displays help for this utility.

RESTRICTIONS

None.

EXAMPLES

```
SUBSCMPL_import_supplier_declarations -u=tcadmin -p=tcadmin -g=dba
-xsl=TC_DATA\msd_to_tcxml.xsl
-mode=managed

SUBSCMPL_import_supplier_declarations -u=tcadmin -p=tcadmin -g=dba
-xsl=TC_DATA\msd_to_tcxml.xsl -path=directory_path
-mode=directory

SUBSCMPL_import_supplier_declarations -u=tcadmin -p=tcadmin -g=dba
-xsl=TC_DATA\msd_to_tcxml.xsl -path=file_path
-mode=file
```

subscmpl_import_template

Imports the default user templates to work with Microsoft Office components that are required in Substance Compliance.

SYNTAX

subscmpl_import_template
[**-u**=*user-id*
{**-p**=*password* | **-pf**=*password-file*}
[**-g**=*group*]
[**-f**=*path of the folder*]
[**-i**=*path of the template file*]
[**-t**=*type of template being imported*]
[**-h**]

ARGUMENTS

-u

Specifies the user ID.

This is a user with Teamcenter administration privileges.

> Note:
>
> If Security Services single sign-on (SSO) is enabled for your server, the **-u** and **-p** arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-p

Specifies the password.

This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file.

This argument is mutually exclusive with the **-p** argument.

-g

Specifies the group associated with the user.

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

-f

Specifies the path of the folder from which templates are imported.

-i

Specifies the path of the template file to be imported.

-t

Specifies the type of the template being imported using **-I** or **-f** option, for example, **ExcelTemplate**.

-h

Displays help for this utility.

RESTRICTIONS

None.

subscmpl_migrate_supplier_declarations

SYNTAX

SUBSCMPL_migrate_supplier_declarations
[**-u**=*user-id*
{**-p**=*password* | **-pf**=*password-file*}
[**-g**=*group*]
Pub _newline[**-h**]

ARGUMENTS

-u

Specifies the user ID.

This is a user with Teamcenter administration privileges.

> Note:
>
> If Security Services single sign-on (SSO) is enabled for your server, the **-u** and **-p** arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-p

Specifies the password.

This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file.

This argument is mutually exclusive with the **-p** argument.

-g

Specifies the group associated with the user.

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

-h

Displays help for this utility.

RESTRICTIONS

None.

EXAMPLES

```
SUBSCMPL_migrate_supplier_declarations -u=tcadmin -p=tcadmin -g=dba
```

subscmpl_purge_supplier_declarations

Purges the metadata generated during various operations such as importing external data.

SYNTAX

SUBSCMPL_purge_supplier_declarations
[**-u**=*user-id*
{**-p**=*password* | **-pf**=*password-file*}
[**-g**=*group*]
[**-class=***class-name* | **ALL**]
[**-status=Archive**| **Rejected**]
[**-h**]

ARGUMENTS

-u

Specifies the user ID.

This is a user with Teamcenter administration privileges.

> Note:
>
> If Security Services single sign-on (SSO) is enabled for your server, the **-u** and **-p** arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-p

Specifies the password.

This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file.

This argument is mutually exclusive with the **-p** argument.

-g

Specifies the group associated with the user.

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

-class

Specifies the class name. You can enter a valid Business Modeler IDE class or type name, or enter **ALL**. **ALL** indicates that all the supporting documents must be purged.

-status

Indicates that the documents with the specified status must be purged. You can specify the status as either **Archive** or **Rejected**.

-h

Displays help for this utility.

RESTRICTIONS

None.

EXAMPLES

```
SUBSCMPL_purge_supplier_declarations -u=tcadmin -p=tcadmin -g=dba
-class=Scp0CMDDoc -status=Archive
```

```
SUBSCMPL_purge_supplier_declarations -u=tcadmin -p=tcadmin -g=dba
-class=ALL -status=Rejected
```

subscmpl_validate_compliance_results

Validates the compliance results in Teamcenter based on the expiry dates.

SYNTAX

material_import
[**-u**=*user-id*
{**-p**=*password* | **-pf**=*password-file*}
[**-g**=*group*]
[**-locales**=*language codes*]
[**-h**]

ARGUMENTS

-u

Specifies the user ID.

This is a user with Teamcenter administration privileges.

> Note:
>
> If Security Services single sign-on (SSO) is enabled for your server, the **-u** and **-p** arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-p

Specifies the password.

This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file.

This argument is mutually exclusive with the **-p** argument.

-g

Specifies the group associated with the user.

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

-locales

Specifies the language codes separated by a comma.

-h

Displays help for this utility.

RESTRICTIONS

None.

EXAMPLES

Translations for query name and descriptions will be added for the specified languages. User can specify single or multiple language codes separated with comma (,). Specifying ALL will add translations in all supported languages.

`[-locales=`*language codes/ALL*`]`

subscmpl_validate_supplier_declarations

Validates the compliance results in Teamcenter based on the expiry dates.

SYNTAX

SUBSCMPL_validate_supplier_declarations
[**-u**=*user-id*
{**-p**=*password* | **-pf**=*password-file*}
[**-g**=*group*]
[**-xsl**=*xsl-file-path*]
[**-path**]
[**-mode**]
[**-decl_type**]
[**-h**]

ARGUMENTS

-u

Specifies the user ID.

This is a user with Teamcenter administration privileges.

> Note:
>
> If Security Services single sign-on (SSO) is enabled for your server, the **-u** and **-p** arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-p

Specifies the password.

This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file.

This argument is mutually exclusive with the **-p** argument.

-g

Specifies the group associated with the user.

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

-xsl

Specifies the absolute file name of the *xsl* file.

-path

Specifies the path of the directory that contains the supplier declaration file and supporting files.

-mode

Specifies whether to run the utility in managed, file, or directory modes:

- **managed**: Use the **managed** mode to validate declarations imported using the **email polling functionality**.
- **file**: Use the **file** mode to select and validate a single declaration.
- **directory**: Use the **directory** mode to validate all declarations in the specified directory.

-type

Specifies the type of the supplier declaration to be imported.

This argument is a mandatory argument.

-h

Displays help for this utility.

RESTRICTIONS

None.

EXAMPLES

```
SUBSCMPL_validate_supplier_declarations -u=tcadmin -p=tcadmin -g=dba
-xsl=TC_DATA\msd_to_tcxml.xsl -mode=managed -type=msd

SUBSCMPL_validate_supplier_declarations -u=tcadmin -p=tcadmin -g=dba
-xsl=TC_DATA\msd_to_tcxml.xsl -path=directory_path
-mode=directory -type=msd

SUBSCMPL_validate_supplier_declarations -u=tcadmin -p=tcadmin -g=dba
-xsl=TC_DATA\msd_to_tcxml.xsl -path=file_path
-mode=file -type=msd
```

subscmpl_auto_regrading_parts

This utility retrieves and grades the parts based on the presence of the *regrade_assembly* parameter.

If the *regrade_assembly* parameter is absent, then the utility retrieves and grades all node parts with a value of *False* for the **Is Active** compliance result property. This implies that there is an impact from recent substance or material change and that the parts are not graded since the change.

Additionally, the utility marks the compliance result property **Lookup Candidate** as *True* for the respective compliance results on the node.

If the *regrade_assembly* parameter is included, then the utility performs the compliance check by calling the workflow *Initiate substance compliance check*. This workflow grades the parts with a value of *False* for the **Is Active** compliance result property or a value of **True** for the **Autograding Candidate** property.

Syntax

subscmpl_auto_regrading_parts
[**-u=***user-id*
{**-p=***password* | **-pf=***password-file*}
[**-g=***group*] [**-batch_size=***number of objects per batch*] **[-regrade_assembly**] [**-grade_individually**]

[**-h**]

Arguments

-u

Specifies the user ID.

This is a user with Teamcenter administration privileges.

> Note:
>
> If Security Services single sign-on (SSO) is enabled for your server, the **-u** and **-p** arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-p

Specifies the password.

This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file.

This argument is mutually exclusive with the **-p** argument.

-g

Specifies the group associated with the user.

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

-batch_size

Specifies the number of objects per batch. This is most useful when grading thousands of parts because it helps avoid memory and disk space shortage problems. It must be a positive integer.

-regrade_assembly

Specifies which compliance results are to be retrieved. If not specified, the utility retrieves the compliance results having **Is Active** property value as *False*. Otherwise, if the specified utility retrieves the compliance results having **Autograding Candidate** property value as *True*.

-grade_individually

Specifies whether to grade the parts in bulk or whether to grade them individually If used as a parameter, the utility grades a part individually. If not specified as a parameter, the utility grades a specific number of parts depending on the batch size in a single request.

-h

Displays help for this utility.

Restrictions

None.

Examples

```
subscmpl_auto_regrading_parts -u=tcadmin -p=tcadmin -g=dba

subscmpl_auto_regrading_parts -u=tcadmin -p=tcadmin -g=dba -batch_size=500

subscmpl_auto_regrading_parts -u=tcadmin -p=tcadmin -g=dba.-
regrade_assembly

subscmpl_auto_regrading_parts -u=tcadmin -p=tcadmin -g=dba.-
regrade_assembly -batch_size=500

subscmpl_auto_regrading_parts -u=tcadmin -p=tcadmin -g=dba
-regrade_assembly.-grade_individually
```

subscmpl_mark_assembly_for_regrade

This utility first retrieves all the lookup candidates for an assembly. **Lookup candidates** are parts with compliance results that display **Lookup Candidate**, **Is Active**, and **Is Latest** property values as *True*.

The utility finds the corresponding *regradable* and *autograding* candidates referenced by each lookup candidate, indicating that the lookup candidate is part of the associated assembly.

The **Regradable Candidates** are parts which need grading (compliance check) because of the corresponding lookup candidate change. The **Autograding Candidates** are parts against which a compliance check needs to be performed.

The utility sets the **Regradable Candidate** property as *True* on related compliance results based on the **SUBSCMPL_set_intermediate_parents_regradable** preference value (See the preference description for more details.)

The utility sets the **Autograding Candidate** property as *True* on related compliance results.

Syntax

subscmpl_mark_assembly_for_regrade
[**-u=***user-id*
{**-p=***password* | **-pf=***password-file*}
[**-g=***group*]

[**-h**]

Arguments

-u

Specifies the user ID.

This is a user with Teamcenter administration privileges.

> Note:
>
> If Security Services single sign-on (SSO) is enabled for your server, the **-u** and **-p** arguments are authenticated externally through SSO rather than being authenticated against the Teamcenter database. If you do not supply these arguments, the utility attempts to join an existing SSO session. If no session is found, you are prompted to enter a user ID and password.

-p

Specifies the password.

This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file.

This argument is mutually exclusive with the **-p** argument.

-g

Specifies the group associated with the user.

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

-h

Displays help for this utility.

Restrictions

None.

Examples

```
subscmpl_mark_assembly_for_regrade -u=tcadmin -p=tcadmin -g=dba
```

subscmpl_process_declaration_reminders

Validates the compliance results in Teamcenter based on the expiry dates.

SYNTAX

subscmpl_process_declaration_reminders
[**-u**=*user-id*
{**-p**=*password* | **-pf**=*password-file*}
[**-g**=*group*]
[**-encrypt**=*true*]
[**-type**=*declaration-type*]

ARGUMENTS

-u

Specifies the user ID.

This is a user with Teamcenter administration privileges.

-p

Specifies the password.

This argument is mutually exclusive with the **-pf** argument.

-pf

Specifies the password file. The file must be a single line ASCII file.

This argument is mutually exclusive with the **-p** argument.

-g

Specifies the group associated with the user.

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

-encrypt

Specifies if the password is encrypted.

-type

Specifies the supplier declaration type. The valid values are **CMD** for conflict mineral declaration and **MSD** for material substance declaration.

RESTRICTIONS

None.

EXAMPLES

```
subscmpl_process_delcaration_reminders -u=tcadmin -p=tcadmin -encrypt=true
-type=MSD

subscmpl_process_delcaration_reminders -u=tcadmin -p=tcadmin -encrypt=true
-type=CMD
```