TEAMCENTER

Teamcenter Environment Manager — Usage

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

Microservice framework

Active Workspace

Quick preconfigured installation

Business Modeler IDE

File Management System

Teamcenter client communication system

Web tier

Security Services

Server manager

Dispatcher

Teamcenter Reporting and Analytics

Repeatable Digital Validation

Rich client

Lifecycle Visualization

Teamcenter integrations

Multi-Site Collaboration

Archive and Restore

Additional features

Updates Manager

Upgrade

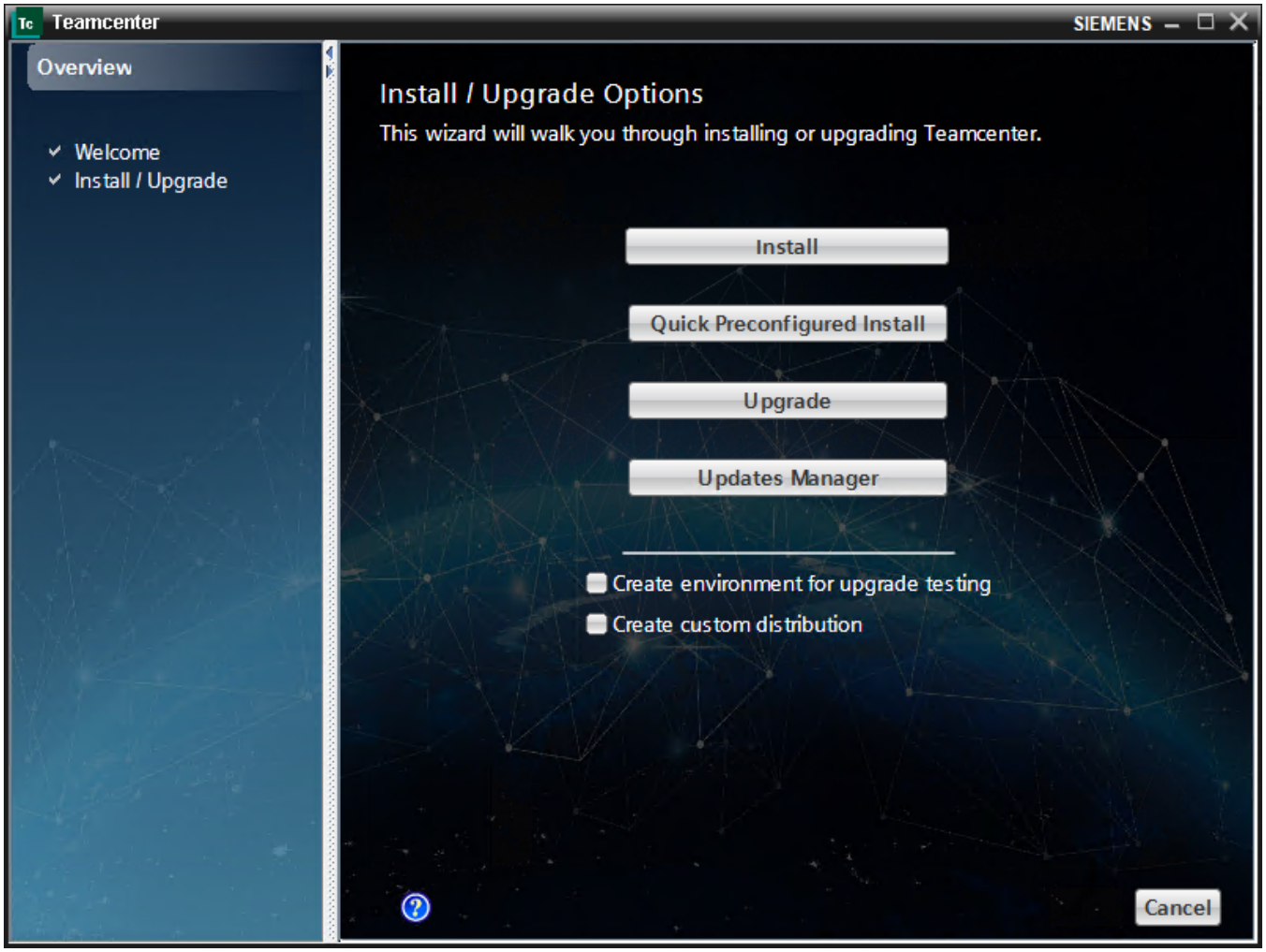
1. Introduction to Teamcenter Environment Manager

Teamcenter Environment Manager (TEM) is an installation wizard that installs, upgrades, and updates Teamcenter configurations. For each installation step, TEM displays a panel requesting information from the installer. Each panel provides online help that describes the content of the panel. To view the online help for a given panel, click the help button  .

This guide contains all online help displayed in the TEM user interface, organized for reference from the Teamcenter online help collection. Online help topics for TEM panels are organized by features (such as *File Management System*) and general configuration areas (such as *Database configuration*). Because of this organization, the sequence of TEM help topics differs from the sequence of panels displayed in TEM.

This guide contains TEM help topics included in the Teamcenter software kit.

The first TEM panel displayed during Teamcenter installation is the **Install/Upgrade Options** panel.

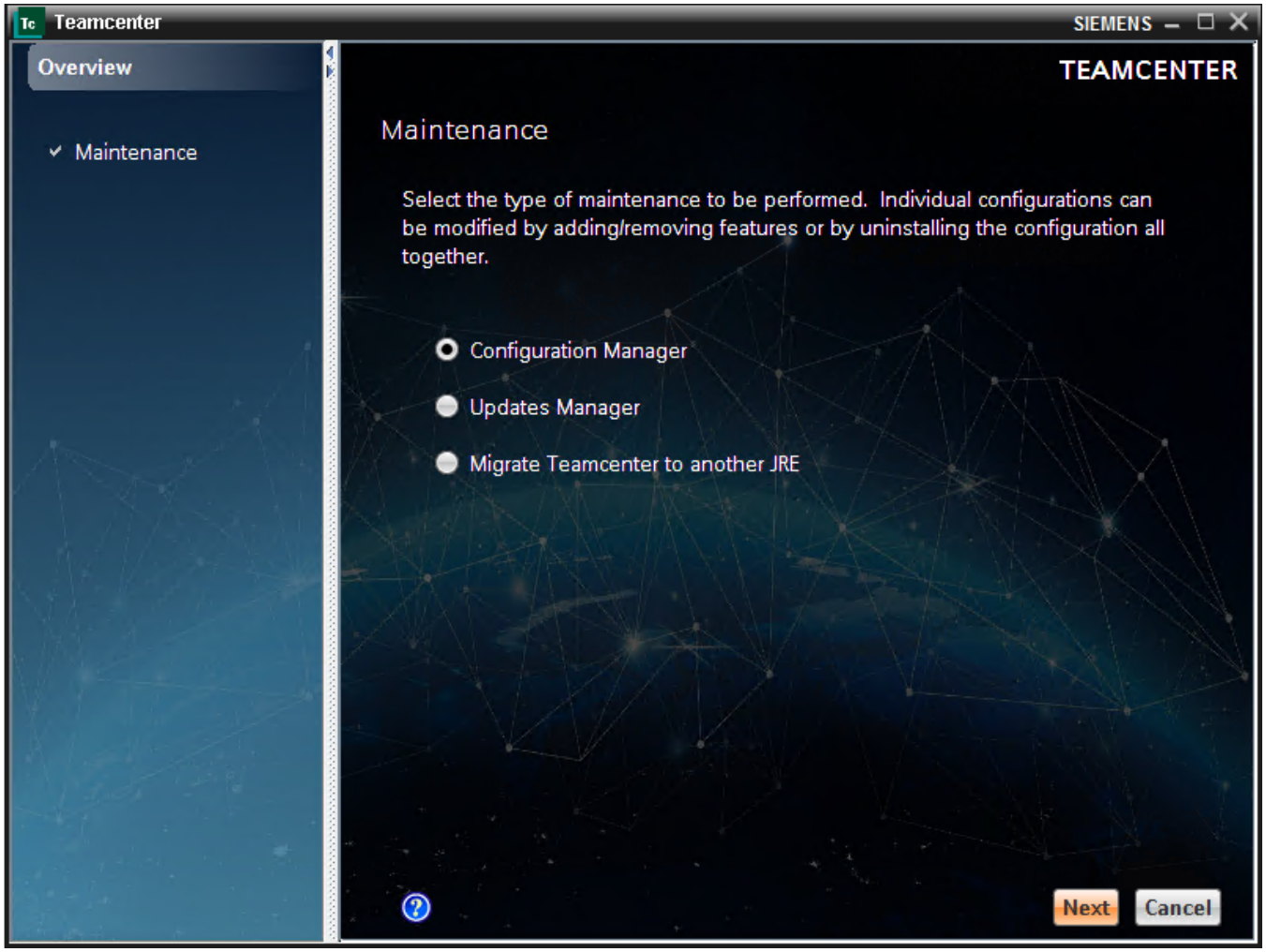


Install/Upgrade Options panel

From this panel, you choose whether to create a new installation or **upgrade an existing installation**. **Quick preconfigured installation** offers common Teamcenter server and client configurations you can install quickly, and then update features or settings later.

You can also create a *silent distribution*, a Teamcenter configuration with preselected features you can install on other hosts with minimal user interaction, or a *compact distribution*, a Teamcenter installation package that contains only selected features and is therefore smaller and more easily distributed than a full Teamcenter software kit.

When you launch TEM from an installed Teamcenter home directory, the first panel displayed is the **Maintenance** panel.



Maintenance panel

From this panel, you can perform maintenance on your Teamcenter configuration, such as adding or removing features, changing FMS settings, or even uninstalling a configuration, by selecting **Configuration Manager**.

To apply patches to a Teamcenter configuration, choose **Updates Manager**.

> Note:
>
> Some panels are not displayed in all platforms. Some features are not available on all platforms.

2. Database configuration

About database configuration in TEM

The following TEM help topics describe panels that allow you to create and configure databases for Teamcenter. For more information about creating and configuring Teamcenter databases, see the appropriate server installation guide (for Windows or Linux) or see the *System Administration* guide.

Configure the database for Teamcenter Foundation

In this step, you provide the information that Teamcenter requires to connect to the Teamcenter Foundation database. The contents of this panel depend on your selection in the **Foundation** panel.

Prerequisites:

- You must install a database server. Teamcenter supports Oracle and Microsoft SQL Server databases.
- If you use Oracle, you must create a database instance, either a specific instance configured for Teamcenter or a multipurpose instance to be configured in this step.

References:

For information about installing a database server and configuring databases for use with Teamcenter, see the *Teamcenter Installation on Windows Using TEM* and the *Teamcenter Installation on Linux Using TEM* available in the Teamcenter documentation.

In the **Data Directory** box, enter a location for the Teamcenter data directory (*TC_DATA*). TEM creates shared data subdirectories and files in this location.

> Note:
>
> TEM creates a security directory within the *TC_DATA* directory to store password files. In a distributed environment, you may place this directory on a network share, provided the location is secured. When you share a Teamcenter data directory, all secondary servers have access to the same files. Make sure the configuration IDs are consistent across those machines.
>
> As an alternative to shared Teamcenter data directories, you can create local data directories. Local data directories do not need to have matching configuration IDs, and password files do not need to be on a share, but you must ensure the separate data directories are kept synchronized.

In the **Database Server** box, select your database vendor (**Oracle** or **Microsoft SQL Server**).

Enter the following database configuration values, depending on the database vendor you select.

Oracle database server values

Value	Description
Host	Specifies the name of the host on which the Oracle server runs. This host must exist, and the Oracle server must be installed.
Service	Specifies the name of the service for the Oracle instance. The service name was determined when the Oracle server was installed.
Port	Specifies the number of the port on which the Oracle server listens. The port number was determined when the Oracle server was installed.
User	Specifies a database user name: • To connect to an existing database configured for use with Teamcenter, enter the name defined for a database user when the database was configured. • To create and configure a database for use with Teamcenter, enter the name of the database user you want to create.
Password	Specifies a database password: • To connect to an existing database configured for use with Teamcenter, enter the password defined for the database user when the database was configured. • To configure a new database for use with Teamcenter, enter a password for the database user you are creating.

If you chose to create a new database instead of using an existing database, provide the following values:

System User	Specifies a user name of the Oracle system administrator account. The default value is **system**.
Password	Specifies a password for the Oracle system administrator account.

> Caution:
>
> The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab.
>
> In addition, the password must not contain any of the following characters:

Value	Description
	! # @ $ % = & ' " ^ : ; . _ < > ( ) { }
Database Path	Specifies the location of the tablespaces for the Teamcenter database on the Oracle server. This is typically *ORACLE_HOME***oradata***Oracle_SID* (on Windows systems) or *ORACLE_HOME*/**oradata**/*Oracle_SID* (on Linux systems). Note: The **Database Path** must exist and you must have write permission to the directory.
Data Directory	Specifies the path to the Teamcenter data (*TC_DATA*) directory. This value is stored in the **TC_DATA** variable in your Teamcenter configuration. TEM creates shared data subdirectories and files in this location. Each data directory is associated with a single database user within a database instance. Note: Do not create a **TC_DATA** variable in the system environment. TEM sets this variable as required in Teamcenter scripts. Setting this variable in the operating system causes conflicts if you install more than one configuration.
Enable TCPS	If you want to use secured communication with the database using secure TCP (TCPS), select the **Enable TCPS** check box, and then enter the following values. If you do not select this check box, Teamcenter uses TCP by default.
Wallet Location	Specifies the location of the secure wallet that stores CA certificates. This is the Oracle **auto_login** wallet configured on the file system. The user under which the deployer is triggered should have read access to this folder.
SSL Version	Specifies the installed TLS version.

Microsoft SQL Server values

Value	Description
Instance	If you connect to Microsoft SQL Server using a named instance, select this option and enter the instance name you defined when you installed MS SQL Server.
Port	If you connect to Microsoft SQL Server using a specific port, select this option and enter the port number you specified when you installed MS SQL Server.
Login Name	Specifies a database user name: • To connect to an existing database configured for use with Teamcenter, enter the name defined for a database user when the database was configured. • To create and configure a new database for use with Teamcenter, enter the name of the database user you want to create.
Login Password	Specifies the password for the database user: • To connect to an existing database configured for use with Teamcenter, enter the password defined for the database user when the database was configured. • To configure a new database for use with Teamcenter, enter a password for the database user you are creating.
Database Name	Specifies the name of the MS SQL Server database. The database name was determined when database was created.

If you chose to create a new database instead of using an existing database, provide the following values:

System User	Specifies the user name of the SQL Server system administrator account. The default value is **sa**.
Password	Specifies the password for the SQL Server system administrator account.

> Caution:
>
> The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab.
>
> Make sure the password does not contain space characters or any of the following characters:

Value	Description
	! @ $ % ' " : ; . < > ( ) { }
Database Path	Specifies the directory in which to create the Teamcenter database on the SQL Server server.
Collation	Specifies the collation used by the Teamcenter database on the Microsoft SQL Server server. *Collation* defines the alphabet or language whose rules are applied when data is sorted or compared.
Enable UTF-8	Specifies whether to enable support for UTF-8 encoding in the Teamcenter database. Microsoft SQL Server does not provide native support for UTF-8. The **Enable UTF-8** option enables the Teamcenter server to convert character encoding to and from UTF-8 when interacting with the database. For information about configuring your Teamcenter host to support UTF-8, see the Teamcenter installation guides for Windows and Linux.
Data Directory	Specifies the path to the Teamcenter data (*TC_DATA*) directory. This value is stored in the **TC_DATA** variable in your Teamcenter configuration. TEM creates shared data subdirectories and files in this location. Each data directory is associated with a single database user within a database instance. Note: Do not create a **TC_DATA** variable in the system environment. TEM sets this variable as required in Teamcenter scripts. Setting this variable in the operating system causes conflicts if you install more than one configuration.

Rebuilding a Database

This panel displays a list of templates to be applied when TEM rebuilds the database. The **Installed Templates** table shows templates that have been applied to the current database.

The **Candidate Templates** table shows the latest templates available to apply when rebuilding the database. Select the candidate templates you want to apply to the database.

Note:

You cannot select templates that were not previously installed. In the **Candidate Templates** table, you can only select templates listed in the **Installed Templates** table.

To locate additional candidate templates, click **Browse**. TEM searches for **.zip** files that contain Teamcenter templates. For example, the Teamcenter Foundation template, **foundation_template.xml**, is in the file **foundation_template.zip**.

Updating a database

This panel allows you to apply updated database templates when performing maintenance on your Teamcenter configuration.

The database update mode depends on the option you select under **Teamcenter Foundation** in the **Feature Maintenance** panel:

- **Update Database (Full Model)**

  Updates the database with Business Modeler IDE templates that contains all the custom data model, including schema items such as business objects and classes.

- **Update Database (Perform Live Updates)**

  Updates the database with live update templates that contain only nonschema data such as LOVs and rules.

The template list shows currently installed templates. If a template is present and is the correct version, the **Status** column displays a checkmark icon for that template.

To query the database for installed templates and refresh the list of templates, click **Refresh**.

Full model updates

To add a template to the list, or to update an existing template, click the **Browse** button to navigate to the directory where your packaged template files are located. Select the updated **feature_***template-name***.xml** file.

The **Status** column displays a refreshed status icon for templates to be refreshed.

Note:

- You can also update a template using the **tem** command line utility, for example.

  ```
  tem -update -full -templates=template-name-1,template-name-2 -path=location-of-template-files
  -pass=password
  ```

- If you are fixing a COTS template (for example, the Foundation template) using a new template file provided in a patch, you must copy the template's **feature_***template-name***.xml** and the

*template-name*_**install.zip** files to the same temporary directory containing the new *template-name*_**template.zip** file.

For more information about packaging template files and updating database templates, see *BMIDE for Data Model Design*.

Live updates

Click the **Browse** button to navigate to the directory where your packaged template files are located. Select the updated *template-name*_**template_live_update.zip** file.

Select the template in the table to receive live updates, and then click **Next** to proceed with the update.

Note:

The system checks if the live update project is synchronized with the server. If there is data on the server that is not in the live update project, the update fails. You must synchronize the data model from the Business Modeler IDE, repackage, and attempt the update once more.

If installation of the live updates fails, check the message in the TEM panel. Installation may have failed because the server you are attempting to install to does not have the **Live Update** preference set to accept live changes. In this case, you must ask the administrator of that production server to change the preference to accept the live updates.

For more information about live updates, see *BMIDE for Data Model Design*.

Microsoft SQL Server connection

In this step, you specify whether your Microsoft SQL Server server is accessible through a named instance or a port. Select the appropriate option and type the name of the instance or the port your server uses.

Teamcenter Integration Framework datastore

This panel displays the contents of the Teamcenter Integration Framework datastore. Modifications may be made to this datastore for the purpose of tracking status of Teamcenter Integration Framework's Business Modeler IDE extension actions on the Teamcenter Integration Framework.

A new Teamcenter Integration Framework datastore with the same structure as its Teamcenter counterpart must be created to store tracking entries.

After checking entries on the Teamcenter side, the Teamcenter Integration Framework daemon checks the datastore entries to complete synchronization between a Teamcenter instance and its corresponding instance.

For more information on Teamcenter Integration Framework, see the Teamcenter Integration Framework help collection available on the Siemens Digital Industries Software Support Center.

Database User

In this step, you specify the user name and password for the Teamcenter database user.

Value	Description
User	Specifies the user name for the database user account.
Password	Specifies the password for the database user account.

Database System User

In this step, you specify the user name and password for the database system user.

Value	Description
User	Specifies the user name for the database system user account.
Password	Specifies the password for the database system user account.

Locking Mechanism

In this step, you choose whether to enable the enhanced database locking mechanism.

Enhanced locking executes locks in groups instead of in series like Teamcenter's default locking behavior. Applying enhanced locking requires additional time during initial upgrade or patching. However, during runtime, enhanced locking reduces numbers of SQL calls, improving network performance.

If you want to enable this feature, select the **Enable enhanced locking** check box.

> Note:
>
> If you want to enable enhanced locking outside of TEM to save time during installation, you can enable it by executing the following commands as a Teamcenter administrator in a Teamcenter command prompt:
>
> ```
> install -disable_lock_serialization -u=username -pf=password-file-path -g=dba
> install -set_pom_param -u=username -pf=password-file-path -g=dba
> POM_ENABLE_LOCK_SERIALIZATION NULL
> ```

3. License management

About license management in TEM

The following TEM help topics describe panels in which you enter Teamcenter license settings.

Information about configuring the Teamcenter licensing client is available in *Teamcenter Installation on Windows Using TEM* and *Teamcenter Installation on Linux Using TEM*. Information about managing Teamcenter licenses is available in *Teamcenter Administration*.

Information about installing the Siemens Digital Industries Software Common Licensing Server is available in the Licensing Server documentation in the product download page on Support Center. This documentation is available under **Siemens PLM Licensing→Product updates→Documentation**.

See also the Siemens Digital Industries Software licensing frequently asked questions:

http://support.industrysoftware.automation.siemens.com/license/license_faq.pdf

Configuring FLEX license client

In this step, you configure the Teamcenter FLEX license client to provide license authorizations for Teamcenter and NX.

Prerequisite:

The Siemens License Server (**ugslmd**) must be installed and configured.

Information about installing the license server is available in the Siemens License Server documentation on Support Center.

Add the port and host values of the Siemens License Server to the table of license servers.

To add a license server to the list, click **Add**. TEM adds a row to the table of license servers. Double-click the **Port** or **Host** boxes to enter the host name and the port for the host serving the Teamcenter license file.

To modify a value in the table, double-click the box and enter the new value.

To remove a server from the table, select the row and click **Delete**.

TEM stores the license server host and port values in the **SPLM_LICENSE_SERVER** environment variable on the local host.

Note:

If you set the **SPLM_LICENSE_SERVER** environment variable before launching TEM, the table of license servers is prepopulated from the value of this variable.

4. Teamcenter Foundation

Installation and upgrade options

In this step, you begin a Teamcenter installation or update. Click one of the following buttons.

Button	Description
Install	Creates a new installation of Teamcenter. This option allows you to select and configure features before you begin installing.
Quick Preconfigured Install	Installs one of several predefined common Teamcenter configurations that require minimal user input to install. You choose a configuration in the next panel.
Upgrade	Upgrades an existing installation of Teamcenter.
Updates Manager	Installs Teamcenter updates and patches. This button is available only when you launch TEM from an update software kit.
Create environment for upgrade testing	Specifies you want to create a copy of a production environment for performing upgrade testing.
Create custom distribution	Specifies you want to create a *silent distribution* or a *compact distribution* for simplified deployment of Teamcenter configurations.

If you want to add a new Teamcenter configuration to an existing Teamcenter installation, launch Teamcenter Environment Manager (TEM) from the location of the Teamcenter installation, *not* from the Teamcenter software kit.

Note:

- A Teamcenter *configuration* is a collection of features associated with one Teamcenter data directory. The collection of configurations that share the same Teamcenter application root directory is a Teamcenter *installation*.

  When you install Teamcenter executables using TEM from the software kit, you create the first configuration.

- A *silent distribution* is a configuration file you can use to install Teamcenter *silently* (without user interaction) on another host. A *compact distribution* is an installable package with a selected subset of Teamcenter client features. It is much smaller than a full Teamcenter software kit and is more easily distributed to multiple hosts in an organization.

- The **Quick Preconfigured Install** button is not available if you select the **Create custom distribution** check box.

For information about issues that may affect Teamcenter installation or update, see the README file that accompanies the software kit.

Media locations

In this step, you specify locations of Teamcenter software.

Value	Description
Update Location	Specifies locations of software kits for Teamcenter product updates and optional asynchronous products. TEM applies updates during the Teamcenter installation or upgrade. You can specify multiple update locations. Click **Browse** to add an update location to the list, or click **Remove** to remove an update location.

Note:

TEM applies updates in the order you specify. If updates contain different versions of the same software component, the update closest to the bottom of the list takes precedence. To change the order in which updates are applied, select an update in the list and click **Shift Up** or **Shift Down**.

Identifying the configuration

In this step, you uniquely identify this configuration of a Teamcenter installation.

Tip:

Record the name. To modify or uninstall this configuration, you must select the configuration ID from a list displayed by Teamcenter Environment Manager.

A *Teamcenter configuration* is a collection of features associated with one Teamcenter data directory. A *Teamcenter installation* is a collection of Teamcenter configurations that share the same Teamcenter application root directory.

Teamcenter Foundation installation

In this step, you select how you want to create or designate the database and data directory (*TC_DATA*) for the Teamcenter server. Select the option that suits your environment and deployment plans.

Database exists?	Database populated?	TC_DATA exists?	Select this option
No	*N/A*	No	**Create and populate database, create new data directory** No Teamcenter database or data directory exists and you want TEM to create both. This option is selected by default.
Yes	No	No	**Populate database, create new data directory** A database exists but is not populated with Teamcenter data. You want TEM to populate the database and create a new data directory.
Yes	Yes	No	**Create new data directory using existing populated database** A database exists and is populated. You want TEM to use this database and create a new data directory.
Yes	Yes	Yes	**Use populated database and existing data directory** A database exists and is populated, and a data directory exists. You want TEM to use both of these.

Caution:

When you enter the password for the database system user in subsequent steps, be aware of the following restrictions:

- The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab.
- In addition, the password must not contain any of the following characters:

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

Teamcenter Foundation settings

In this step, you provide additional settings for Teamcenter Foundation.

These settings include the creation of transient volumes on the local host.

A *transient volume* is an operating system directory controlled by Teamcenter and used to store temporary data for transport of reports, PLM XML data, and other nonvolume data between the enterprise tier and client tier in a deployment of the four-tier architecture. All four-tier clients accessing this installation of Teamcenter use this transient volume.

Note:

Two-tier clients do not use this transient volume, using instead a temporary directory on the client host that is defined either by the **start_server** script or by the **Transient_Volume_RootDir** environment variable on the client host.

If you plan to install another Teamcenter data server for the database you are populating, but the host is on a different platform, you must:

1. Specify the location of the transient volume for each platform on this panel.

   For example, if the local host is a Windows-based system, and you intend to install a Teamcenter data server for this database on a Linux-based system, specify the transient volume location for the additional host as well as the local host.

2. If you do not specify an existing directory for the additional Teamcenter data server, manually create the location for the transient volume.

References:

- For more information on deploying Teamcenter on heterogeneous platforms, see *Teamcenter Installation on Linux Using TEM* and *Teamcenter Installation on Windows Using TEM*.

Value	Description
Transient Volume Directories	
Windows clients	Specifies the full path to a directory to act as the transient volume when the host is Windows-based. The operating system user running the FSC and Teamcenter server processes must have a minimum of read and write privileges for this directory. This field must contain a value. If this directory does not exist, Teamcenter Environment Manager creates it if the local host is Windows-based. Tip: • If you are deploying the two-tier architecture, accept the default value. • If the local server is Linux-based, and you do not intend to install a Teamcenter data server for this database on a Windows-based system, accept the default value. • If the local server is Linux-based, and you intend to install a Teamcenter data server for this database on a Windows-based system, either enter the path to an existing directory on the Linux system or record the path you enter (you must create this directory manually).
Linux clients	Specifies the full path to a directory to act as the transient volume when the host is Linux-based. This field must contain a value.

Value	Description
	If this directory does not exist, Teamcenter Environment Manager creates it if the local host is Linux-based. Tip: • If you are deploying the two-tier architecture, accept the default value. • If the local server is Windows-based, and you do not intend to install a Teamcenter data server for this database on a Linux-based system, accept the default value. • If the local server is Windows-based, and you intend to install a Teamcenter data server for this database on a Linux-based system, either enter the path to an existing directory on the Linux system or record the path you enter (you must create this directory manually).
Generate server cache	Specifies that you want to generate a shared server cache. If you select this option, TEM runs the **generate_metadata_cache** utility at the end of the install, upgrade, or update action. This option reduces Teamcenter memory consumption by moving metadata to shared memory. Types, property descriptors, and constants are placed in a shared cache that is shared by all Teamcenter server instances. This option is selected by default in a Teamcenter server installation. For more information about managing shared server cache, see the *Teamcenter Administration* guide.
Generate client cache	Specifies that you want to generate a cache of data that rich clients can download once at initial logon and then reuse on the client host. This option reduces server demand, reduces startup time, and improves overall performance. When this option is selected, TEM generates the client cache at the end of the install, upgrade, or update action. If you clear this option, but a client cache already exists, the old client cache is deleted. This option is selected by default in a Teamcenter server installation.
Production Environment	Specifies this environment is to be used as a live environment where you will store your product data.
Test Environment	Specifies this environment is to be used for development, testing, or training. Selecting **Test Environment** enables the bulk loader tool to copy data from another environment (such as a production environment) into this test environment.

Value	Description
	Note: If you designate this environment as a test environment, the designation cannot be changed. Additionally, a test environment cannot participate in Multi-Site sharing with a production environment. For more information, see *Copying product data to test environments* in *Teamcenter Data Exchange*.

For additional advanced options, click the **Advanced** button.

Digital signature certificate settings

In this step, you import and select certificates from the file system for digital signature. To add a certificate, click **Add**, and then select the certificate.

When applying digital signatures, Teamcenter takes the user's private key (typically from the PKI card) to encrypt the signature so that it cannot be tampered with. After that signature is applied to the object, the system reads the encrypted signature to verify the signature is valid. In order to verify the encrypted signature, the system must have the root and intermediate certificate authority (CA) files.

Each user certificate (PKI card) has a chain of certificate authorities behind it. These certificate authorities can be found by opening the user's certificate in Windows and clicking the **Certification Path** tab. The certificate authorities should already be installed on the client host so that the web browser on that machine recognizes the user's certificate.

If not directly available, the certificate authorities can be exported through the **Internet Options** dialog box in the Microsoft Windows control panel. These files can then be imported into Teamcenter.

The certificates thus imported to Teamcenter are available as named references to the dataset with name **__DigitalSignature_Certificates**. If a new certificate needs to be added, or an existing one needs to be removed after installation, it can be done by modifying the named references of this dataset in the rich client. Database administrator (**dba**) privileges are required to make these changes.

Configure the multiplexing proxy (MUX)

In this step, you configure the multiplexing proxy (MUX) for the enterprise tier in Teamcenter.

Value	Description
Port	Specifies the TCP/IP port on which the MUX listens for web tier requests. This is the Jetty server connector port.
TECS Admin Port	Specifies the port used by the Teamcenter Enterprise Communication System (TECS).

The MUX listens on a single port for incoming requests from the web tier, forwarding those requests to an appropriate Teamcenter server using operating system named-pipe communication protocol, and then streaming the response back to web tier. The MUX runs as an application within the Teamcenter Enterprise Communication System (TECS). The TECS container is based on the Teamcenter client communication system (TCCS) container used in the client tier.

License agreement

In this step, you read and accept the Siemens Digital Industries Software license agreement.

Read the license agreement, then choose the option to accept the license agreement to continue with Teamcenter installation.

Selecting solutions

In this step, you optionally choose solutions to install in your Teamcenter configuration.

Solutions are preselected groups of features that provide starting points for recommended Teamcenter configurations. You can add features or deselect features in the **Features** panel in Teamcenter Environment Manager (TEM). For information about a solution, point to the solution name in the list. TEM displays a description.

Selecting features

In this step, you select features to include in your Teamcenter configuration or deselect features to remove them from your configuration. Features are grouped by related functionality.

For information about a feature, point to the feature name in the list. TEM displays a description of the feature.

To search for a feature by name, enter a keyword in the **Search** box, then click the search button. To see the next search result, click the search button again.

Note:

- Some features are disabled because they require other features. To enable a feature, select its prerequisite features. For information about feature prerequisites, see the feature description.

- Some features cannot be installed in the same configuration, so selecting one disables the other.

If this is a new installation, enter the directory in which you want to install Teamcenter in the **Installation Directory** box. Specify a directory that does *not* exist. Teamcenter Environment Manager (TEM) creates the directory you specify.

If this is a new Teamcenter configuration, or if you are adding or removing features from an existing configuration, you cannot change the installation directory. TEM creates the new configuration using the same installation root directory.

Teamcenter administrative user

In this step, you enter logon information for the Teamcenter administrative user account.

Teamcenter provides an administrative user account named **infodba** for use during installation. Teamcenter Environment Manager automatically creates this account when you install Teamcenter on a server machine. This account is used by the Teamcenter administrator to access Teamcenter system administration functions to perform setup and maintenance tasks. You create a password for this account during Teamcenter installation.

Box	Description
User	Specifies the user name of the default Teamcenter administrative user account. During installation, this value is set to **infodba**.
Password	Specifies the password for the default Teamcenter administrative user account. Type a password for this account. Caution: The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab. In addition, the password must not contain any of the following characters: **! # @ $ % = & ' " ^ : ; . _ < > ( ) { }**

Caution:

Never use the **infodba** user to create working data or initiate workflow processes. The **infodba** user is to be used *only* for certain tasks during Teamcenter installation. Using this account to create data or initiate workflow processes can cause unexpected and undesirable behaviors.

If you require a user with high-level privileges to create data, create a new user and grant database administrator privileges to that user.

Password security

In this step, you specify where to store encrypted passwords for Teamcenter users.

Value	Description
Administrative Password Directory	Specifies the path to the directory that contains the password files. Teamcenter Environment Manager (TEM) locks access to the password directory to all users except the operating system user performing the installation.

For more information about storing encrypted passwords, see *Encrypt a password file for use by daemons*.

Password security settings

In this step, you specify where to store encrypted passwords for Teamcenter users.

Value	Description
Administrative Password Directory	Specifies the path to the directory that contains the password files. Teamcenter Environment Manager (TEM) locks access to the password directory to all users except the operating system user performing the installation.
List of Known Users	Specifies a list of known Teamcenter users who can access security settings.

For more information about storing encrypted passwords, see *Encrypt a password file for use by daemons*.

Configuring the operating system user

In this step, you configure the operating system logon account for Teamcenter services. This account represents a responsibility rather than a person. All Teamcenter services run on the server as this user account. It is also the logon account Teamcenter administrators use to install and update Teamcenter.

Prerequisite:

You must define the logon account (user name and password) in the operating system with administrator privileges. This account can have any name and password. For Windows systems, this account must have administrator privileges and be granted the **Log on as service** right.

> Note:
>
> If you did not log on to this account to install Teamcenter, cancel the current installation and restart it using this user account.

Value	Description
User	Specifies the operating system user name defined to run Teamcenter services.
Password	Specifies the password defined for the Teamcenter services user name.

TcServer character encoding settings

In this step, you specify settings for character encoding in your Teamcenter rich client installation.

Value	Description
Canonical Name	Specifies by canonical name of the character encoding set the rich client uses to access the database. Caution: To prevent data corruption, this character encoding set must match the encoding set used by the Teamcenter database. Choose an appropriate value for your locale. Some values for Teamcenter are as follows: • Unicode UTF-8: **UTF8** • Chinese (Simplified): **GBK** • Chinese (Traditional): **Big5** • Czech: **Cp1250** • English: **ISO8859_1** • French: **Cp1252** • German: **Cp1252**

Value	Description
	• Hebrew: **ISO8859_8** • Italian: **Cp1252** • Japanese: **SJIS** • Korean: **Cp949** • Polish: **Cp1250** • Portuguese (Brazilian): **Cp1252** • Russian: **Cp1251** • Spanish: **Cp1252** The values specified in this field and the **Description** field are a pair: when you select a value for this field, Teamcenter Environment Manager automatically selects and displays the correct value in the **Description** field.
Description	Specifies by description the character encoding set the rich client uses to access the database. The values specified in this field and the **Canonical Name** field are a pair: when you select a value for this field, Teamcenter Environment Manager automatically selects and displays the correct value in the **Canonical Name** field.

Creating a volume

In this step, you create a *volume*, a directory that stores files managed by Teamcenter. A Teamcenter volume is controlled by one, and only one, database.

When you create or populate a database during a Teamcenter installation, you must create a volume for it. This requires an FMS server cache (FSC) that creates and serves default volumes. The volume can be created while installing a Teamcenter corporate server or a volume server.

You can optionally use Teamcenter Environment Manager to create additional volumes for a database:

- When you install the Teamcenter application directory but point to a Teamcenter data directory in another installation
- When you install Teamcenter and create a new data directory for an existing database

Additional volumes created using Teamcenter Environment Manager are not populated.

Teamcenter administrators can also use the rich client Organization application to create additional volumes for a database.

Reference:

- For information about creating volumes using the rich client user interface, see *Organization Management Using Groups, Roles, and Users*.

Value	Description
Name	Specifies the name of the volume directory.
Directory	Specifies the path to the volume directory.
Serving FSC	These fields are displayed if your configuration does *not* include an FMS server cache (FSC).
FSC Deployment Model	Specifies the FMS server and volume model deployment model you want to use. Select a model from the list.
FSC ID	Specifies the ID of the FMS server cache (FSC) for the volume. This value is needed only if you specify **Simple Model** in the **FSC Deployment Model** box.
FSC Host Name	Specifies the host name of the host on which the FSC resides.
FSC Port	Specifies the port the FSC uses.

If you define an FSC in the current Teamcenter configuration, the default values in the **Serving FSC** fields are populated with the values from that FSC. If you create a volume as part of a corporate server installation, TEM installs the FSC before Teamcenter Foundation to enable Teamcenter to create volumes.

TEM validates the FSC settings by attempting to connect to the specified host and port, and adds the specified FSC specified to the **FMS_BOOTSTRAP_URLS** preference in the new database after population.

TC_DATA proxy setting

This panel displays the *TC_DATA* proxy path. Teamcenter stores files for selected services in this location. This value is display-only.

Installing database daemons

In this step, you install optional database support services. Although the database daemons are optional, installing them is required to activate the Teamcenter Subscription Administration application and the notification of late tasks in the workflow applications and to tessellate **UGMASTER** and

UGALTREP datasets to JT datasets for use with Repeatable Digital Validation (RDV) and the Design Context application.

References:

- For general information about configuring database daemons, see the *Teamcenter Administration* guide.
- For information about configuring tessellation for Repeatable Digital Validation and the Design Context application, see *Design Context*.
- For information about the Subscription Administration application, see *Subscription Administration*.
- For information about late task notification, see *Workflow Designer on Rich Client*.

Value	Description
Install Action Manager Service	Specifies that you want to install the service that monitors the database for the creation of action objects and dispatches events that have a specific execution time and events the Subscription Manager daemon fails to process. Installing the Action Manager service is required to enable the Teamcenter Subscription Administration application. If you install the Action Manager service, you must also install the Subscription Manager service.
Install Subscription Manager Service	Specifies that you want to install the service that monitors the database event queue for the creation of subscription event objects. Installing the Subscription Manager service is required to enable the Teamcenter Subscription Administration application. If you install the Subscription Manager service, you must also install the Action Manager service.
Install Task Monitor Service	Specifies that you want to install the service that checks user inboxes for tasks that have passed due dates, notifies the delegated recipients, and marks the task as late. Installing the Task Monitor service is required to enable notification of late tasks.
Install Tesselation Service	Specifies that you want to install the service that tessellates **UGMASTER** and **UGALTREP** datasets to the JT (DirectModel) dataset and attaches the JT dataset back to the item revision and **UGMASTER** and **UGALTREP** dataset. Installing the Tessellation service is required to create the tessellated representations in Repeatable Digital Validation (RDV) that enable users of the Design Context application to quickly visualize components in context.

Value	Description
	The tessellated representations are created during the workflow release process, ensuring that JT files of the DirectModel datasets are updated as the NX files are released.
Workflow Remote Inbox Service	This service syncs the data between two sites to enable working with remote inboxes.

Configuring data

In this step, you choose whether to install Teamcenter shared data subdirectories and files on this host or point to these files installed on another host.

This directory containing the shared data subdirectories and files is referred to as the Teamcenter *data directory*. The **TC_DATA** environment variable points to this location. A data directory is associated with one (and only one) database instance.

The data directory is exported with full write access and mounted via NFS/CIFS by other Teamcenter nodes. If the data directory is a mapped drive, UNC paths are used for the **TC_ROOT** and **TC_DATA** environment variables.

Value	Description
Create a new data directory	Specifies that you want to install the Teamcenter shared data subdirectories and files on this host.
Connect to an existing data directory	Specifies that you want to point to Teamcenter shared data subdirectories and files installed on another host.
Data Directory Location	Specifies either: • The full path to the location on the local host where you want to install the Teamcenter shared data subdirectories and files. • The full path to the location where Teamcenter shared data subdirectories and files are installed on another host.

Java path

In this step, you provide the path to the Java Runtime Environment (JRE) installed on your host.

This is required to create services for the Business Modeler IDE.

Assign volume

In this step, you assign a volume to an FSC (FMS server cache) server, external load balancer, or file store group.

Value	Description
Assign to FSC Server or External Load Balancer	Select to assign the volume to an FSC server (a machine where FMS processes run) or an external load balancer (a machine designated to take some of the load of FMS processes).
Assign to File Store Group	Select to assign the volume to a file store group, which specifies volumes to be load balanced across several FSCs.

Maintenance

In this step, you choose the maintenance action you want to perform:

- **Configuration Manager**

  Select this option to add or remove features or modify settings for an existing Teamcenter configuration.

- **Updates Manager**

  Select this option to install Teamcenter product updates and patches.

- **Migrate Teamcenter to another JRE**

  Select this option to change the Java Runtime Environment (JRE) used by Teamcenter and TEM.

> Note:
>
> A *Teamcenter configuration* is a collection of features associated with one Teamcenter data directory. A *Teamcenter installation* is a collection of Teamcenter configurations that share the same Teamcenter application root directory.

Configuration maintenance

In this step, you choose the configuration action you want to perform:

- **Add new configuration**

  Select this option to create a new Teamcenter configuration.

- **Perform maintenance on an existing configuration**

  Select this option to add or remove features or update settings for an existing Teamcenter configuration.

- **Upgrade a configuration from another installation**

  Select this option to upgrade an existing configuration to Teamcenter 2412.

- **Remove configuration (uninstall)**

  Select this option to remove an existing Teamcenter configuration.

> Note:
>
> A *Teamcenter configuration* is a collection of features associated with one Teamcenter data directory. A *Teamcenter installation* is a collection of Teamcenter configurations that share the same Teamcenter application root directory.

Selecting a configuration

In this step, you choose the configuration you want to modify. Select the configuration from the list shown.

Selecting configuration to remove

In this step, you choose the Teamcenter configuration to remove.

> Note:
>
> When you remove a configuration, the database and directory for the selected configuration are removed.

Removal of the selected configuration does not begin until you confirm your selections later in the process. Teamcenter Environment Manager prompts you to confirm your selections before any changes are made.

Feature maintenance

In this step, you can select a variety of maintenance actions to perform on your Teamcenter configuration. This may include the following groups of options, depending on the features in your configuration:

- **Teamcenter**

The **Add/Remove Features** option allows you to add or remove features in your configuration.

- **FMS Server Cache**

  This group contains options to import FMS server cache (FSC) groups and update FMS master settings.

- **Business Modeler Templates**

  These options allow you to add or update templates you use within the Business Modeler IDE client.

- **Teamcenter Foundation**

  These options allow you to update database templates and settings for your Teamcenter configuration.

  - **Update Database (Full Model)**

    Updates the database with Business Modeler IDE templates that contains all the custom data model, including schema items such as business objects and classes.

  - **Update Database (Perform Live Updates)**

    Updates the database with operational data templates that contains only operational (nonschema) data such as LOVs and rules.

  - **Modify Settings**

    Allows you to modify certain Teamcenter Foundation settings.

  - **Manage Administration Data**

    Provides options for exporting or importing Teamcenter administration data.

  For more information about operational data, see *BMIDE for Data Model Design*.

  For more information about managing administration data, see *Teamcenter Data Exchange* in the Teamcenter documentation.

- **NX Integration**

  These options allow you to update settings for the Teamcenter NX Integration.

- **Online Help**

  These options allow you to change documentation access settings on your local host.

- **Client Communication System**

  This group contains options to update Teamcenter client communication system (TCCS) settings.

  - **Use Configurations and Environments**

    Allows you to enable TCCS in your Teamcenter installation.

  - **Modify Configurations**

    Allows you to modify TCCS configurations.

  - **Modify 4-tier server settings**

    Allows you to modify settings for the four-tier server.

  - **Modify FCC Parent settings**

    Allows you to modify FCC parent settings.

  - **Remove Configurations**

    Allows you to remove TCCS configurations.

- **2-tier Teamcenter server configurations**

  This group contains options to modify two-tier server settings.

- **Teamcenter Rich client 2-tier**

  This group contains options to modify settings for the two-tier rich client.

- **Dispatcher Server**

  This group contains options to modify Dispatcher Server settings.

Note:

- A *Teamcenter configuration* is a collection of features associated with one Teamcenter data directory.
- A *Teamcenter installation* is a collection of Teamcenter configurations that share the same Teamcenter application root directory.

Confirm silent distribution file name

A silent distribution file with the specified name exists on your system. Choose **Load** to load the existing file or choose **Overwrite** to replace your existing silent distribution file.

Custom distribution options

In this step, you create a custom distribution of Teamcenter software to simplify installation on other hosts. Teamcenter supports the following custom distributions:

- Silent distribution

  A *silent distribution* is an XML-based configuration file you can use to install Teamcenter *silently* (without user interaction) on another host.

  The silent installation configuration file records the selections and values you enter during Teamcenter installation and enables TEM to perform these steps noninteractively when executed on another host.

- Compact distribution

  A *compact distribution* is an installable package with a selected subset of Teamcenter client features. It is much smaller than a full Teamcenter software kit and is more easily distributed to multiple hosts in an organization.

  A compact distribution is an alternative to installing Teamcenter from a full Teamcenter software kit. A compact deployable package can contain a selected subset of Teamcenter features rather than the entire set of features in the release. This reduces network loads and simplifies large-scale Teamcenter deployments by providing an installation package that is smaller and more easily distributed to an organization. For example, a two-tier rich client installation can be packaged in a deployable media as small as 580 MB, where a full Teamcenter software kit can require several GB. A four-tier rich client compact distribution can be as small as 283 MB, and a Client for Office compact distribution can be only 93 MB.

> Note:
>
> Creating a compact distribution is supported only in Teamcenter major releases. It is not supported in minor releases, so the **Create compact deployable media** check box is disabled.

Value	Description
Create silent configuration file	Specifies the path to an existing, writable directory and the name of the silent configuration file, for example, **C:\silent.xml**.

Value	Description
	Note: The silent configuration file must have a **.xml** extension.
Create compact deployable media	Specifies the path to an existing, writable directory in which to create the compact distribution file, for example, **C:\temp**.

Note:

If your silent installation contains third-party features, set the **TEM_PATH** environment variable on client hosts before running your silent installation. Set this variable to a list of paths that contains the feature XML files and other supporting files. This ensures TEM finds the feature XML files during installation.

For information about creating, launching, and modifying a silent installation file, see the *Teamcenter Installation on Linux Using TEM* and the *Teamcenter Installation on Windows Using TEM*.

Message panel

This panel displays important information about your installation. Read the information displayed and click **Next** to continue.

Confirming selections

In this step, you review and confirm the choices you made and start the installation or uninstallation of Teamcenter:

- To change a selection:

  1. Click **Back** until Teamcenter Environment Manager displays the step containing the information you want to change.

     Teamcenter Environment Manager saves the information you entered for the various steps.

  2. Make changes where needed, and then click **Next** until you return to the **Confirmation** panel.

- To start the installation or uninstallation, click **Start**.

Installing features

In this step, you monitor the process of installing Teamcenter.

When installation completes successfully, Teamcenter Environment Manager displays **Install Successful**.

Teamcenter Environment Manager installs a version of itself (**tem.bat** or **tem.sh**) in the **install** directory of the Teamcenter root directory. This version of Teamcenter Environment Manager enables the Teamcenter administrator to perform site maintenance tasks for Teamcenter.

Value	Description
Overall Progress	Displays the progress of the entire Teamcenter installation process.
Message	Displays the progress of the current step in the installation process.
Show Details	Displays the installation details of the current step in the installation process.

Teamcenter data directory

In this step, you specify a location for the Teamcenter data directory (*TC_DATA*). TEM creates shared data subdirectories and files in this location.

In the **Data Directory** box, enter the path to the *TC_DATA* directory.

TEM creates a security directory within the *TC_DATA* directory to store password files. In a distributed environment, you may place this directory on a network share, provided the location is secured. When you share a Teamcenter data directory, all secondary servers have access to the same files. Make sure the configuration IDs are consistent across those machines.

As an alternative to shared Teamcenter data directories, you can create local data directories. Local data directories do not need to have matching configuration IDs, and password files do not need to be on a share, but you must ensure the separate data directories are kept synchronized.

Volume access

In this step, you view available volumes for use with Teamcenter. You must have write permission on the default volume before you continue with Teamcenter installation. If necessary, see your Teamcenter system administrator to obtain write permission to this volume.

To refresh the lists of available local and remote volumes, click **Scan**.

Teamcenter installation location

In this step, you specify locations for the Teamcenter installation root directory (*TC_ROOT*) and the Teamcenter data directory (*TC_DATA*).

TEM creates a security directory within the *TC_DATA* directory to store password files. In a distributed environment, you may place this directory on a network share, provided the location is secured. When

you share a Teamcenter data directory, all secondary servers have access to the same files. Make sure the configuration IDs are consistent across those machines.

As an alternative to shared Teamcenter data directories, you can create local data directories. Local data directories do not need to have matching configuration IDs, and password files do not need to be on a share, but you must ensure the separate data directories are kept synchronized.

Selecting data to import

In this step, you specify the location of the administrative data package, and select administrative data types to import.

In the **Administration Data Package Directory** box, enter the path to the directory that contains the package of administration data to be imported. The package contains XML files with Teamcenter environment specific information that you can import into another Teamcenter environment.

In the list of data types, select the check boxes for each data type you want to import. All the administrative data types registered in the client framework are displayed in the list.

For more information about importing administration data, see *Teamcenter Data Exchange* in the Teamcenter documentation.

Selecting data to merge

In this step, you specify merge behavior for each type of administrative data.

For each data type in the list, choose the rule you want to apply if data types exist in the source (the administrative data package from which you import data) *and* the target (the existing environment into which you import data):

- **Override With Source**

  Overwrites existing data with data from the source package you import.

- **Keep Target**

  Keeps the existing data in the target environment.

- **Choose Latest**

  Keeps whichever data is newer.

Note:

Not all options are available for some categories of data.

For more information about importing administration data, see *Teamcenter Data Exchange* in the Teamcenter documentation.

Manage administration data

In this step, you choose to import or export Teamcenter administration data.

Value	Description
Export Administration Data	Options for exporting administration data.
Full Export	Specifies that you want to export all classes of administration data in the categories you select in the next step.
Partial Export	Specifies that you want to export selected administration data based on criteria you choose in the next step.
Import Administration Data	Options for importing administration data.
Import	Specifies that you want to import data from a TC XML administration data file.
Dry run import	Specifies that you want to perform a test import (dry run) of data from a TC XML administration data file.
Ignore package validation	Selecting this check box indicates that you want to bypass certain validation checks of the administration data. You may select this option if you have modified the administration data file. However, any errors in the TC XML file can cause corruption and possible data loss. Therefore, to use this option, you must first obtain an authorization key from Support Center. For more information about using this option, see *Teamcenter Data Exchange* in the Teamcenter documentation.

Partial administration data export

In this step, you select types of administration data to export.

Value	Description
Administration Data Package Directory	Specifies the directory in which to create the data export file.
Category Name	Specifies the category of administration data to export.
Class	Specifies the class of administration data to export.

If you want to further specify which administration data to export, add the attributes and values to export. Click **Add** to add a row to the table, and then type the attribute and value to export.

To remove a row from the table, select the row and click **Remove**.

For more information about exporting administration data, see *Teamcenter Data Exchange* in the Teamcenter documentation.

Recovering from a failed Teamcenter installation

TEM detected that a previous Teamcenter installation was unsuccessful. In the **Current Application Root Directory**, type the path to the previously attempted installation. TEM attempts to recover and complete the installation.

Enter Java Runtime Environment location

Enter the path to the Java Runtime Environment (JRE) you want Teamcenter to use.

The JRE is used by Teamcenter applications and Teamcenter Environment Manager (TEM).

Migrating Teamcenter to another JRE

Before you update the Java Runtime Environment (JRE) Teamcenter uses, you must make sure no Teamcenter features that depend on Java are running. After you verify the features listed are not running, select **All features from the above list have been shut down**, and then continue.

Uninstall Teamcenter Foundation

In this step, you specify actions to perform during uninstallation of Teamcenter Foundation.

Select **Advanced Uninstall Options** to see available uninstallation options.

Select **Remove** to remove the Teamcenter database, volume, and *TC_DATA* directory.

Warning:

Removal of the database, volume, and *TC_DATA* directory is irreversible. Do not select this option unless you are absolutely certain you want to remove these.

Uninstall Teamcenter

In this step, you confirm whether to uninstall Teamcenter from your system.

Confirm removal of all Teamcenter data

In this step, you confirm whether to remove the Teamcenter database, volume, and *TC_DATA* directory. If you want to remove all of these, select **I want to permanently remove these items**.

Warning:

Removal of the database, volume, and *TC_DATA* directory is irreversible. Do not select this option unless you are absolutely certain you want to remove these.

Completely uninstall Teamcenter

In this step, you confirm whether to completely uninstall Teamcenter from your system. This includes all Teamcenter configurations, databases, volumes, and Teamcenter Environment Manager (TEM).

Confirm removal of all Teamcenter software and data

In this step, you confirm whether to completely uninstall your Teamcenter installation. This includes all Teamcenter configurations, databases, volumes, *TC_DATA* directory, and Teamcenter Environment Manager (TEM).

If you want to remove all of these, select **I want to permanently remove these items**.

Warning:

Removal of the Teamcenter installation is irreversible. Do not select this option unless you are absolutely certain you want to remove all Teamcenter software and data from your system.

Configure the multiplexing proxy (MUX)

In this step, you configure the multiplexing proxy (MUX) for the enterprise tier in Teamcenter.

Value	Description
Port	Specifies the TCP/IP port on which the MUX listens for web tier requests. This is the Jetty server connector port.
TECS Admin Port	Specifies the port used by the Teamcenter Enterprise Communication System (TECS).

The MUX listens on a single port for incoming requests from the web tier, forwarding those requests to an appropriate Teamcenter server using operating system named-pipe communication protocol, and then streaming the response back to web tier. The MUX runs as an application within the Teamcenter Enterprise Communication System (TECS). The TECS container is based on the Teamcenter client communication system (TCCS) container used in the client tier.

SSL configuration

In this step, you specify SSL settings for Teamcenter.

If you do not want to use SSL, clear the **Enable SSL** check box. If you want to use SSL, check the **Enable SSL** check box, and then enter the following values.

Value	Description
KeyStore	Type the full path and file name to the keystore file. A keystore file is a file used for storing private keys and certificates and their corresponding public keys.
KeyStore Type	Type the file extension for the keystore.
KeyStore Password	Type the password to the keystore.
KeyManager Password	Type the manager password to the keystore.
TrustStore	Type the full path and file name to the truststore file. A truststore file is a file used for storing certificates from other parties or from trusted certificate authorities. For example, a cacerts file is a truststore.
TrustStore Type	Type the file extension for the truststore.
TrustStore Password	Type the manager password to the truststore.

Media locations

In this step, you optionally specify additional Teamcenter software kits to apply to your Teamcenter installation. These can include Teamcenter software updates or other asynchronous Teamcenter product releases.

To add a Teamcenter update to the **Update Location** table, click **Browse** to enter the path to the desired update. You can enter locations for multiple updates. To remove a location from the table, click **Remove**.

TEM applies updates in the order you specify. If updates contain different versions of the same software component, the update closest to the *bottom* of the list takes precedence. To change the order in which updates are applied, select an update in the list and click **Shift Up** or **Shift Down**.

FOSS media location

In this step, you specify the directory and location for all third-party components used by Teamcenter.

Value	Description
FOSS Media Directory	Specifies the directory where the FOSS media is stored.
Installation Location	Specifies the path to the location where the FOSS Repository is installed.

Email server settings

In this step, provide settings required for Teamcenter to access the mail server.

Box	Description
Host	Specifies the host name of the mail server.
Port	Specifies the port used by the mail server. The default value is **25**.
Character Set	Specifies the character set used by the mail server. The default value is **ISO-8859-1**.
Connection Security	Specifies the type of connection security used by the mail server, for example, **SSL/TLS** or **STARTTLS**. The default value is **None**.
SSL Protocol	Specifies the SSL connection protocol for the mail server. The default value is **TLS V1.0**.
Authentication	Specifies whether the mail server uses authentication.
Email Id	Specifies the user ID for logging on to the mail server. This box is enabled if you select the **Authentication** check box. The user ID should be an organization-level user, for example, **tcadmin@myCompany.com**.
Email Password	Specifies the password for the mail user. This value is stored encrypted. This box is enabled if you select the **Authentication** check box.

Installing Teamcenter from a disk image

In this step, you specify the location in which to install Teamcenter from a disk image created by Teamcenter Integration Framework. The table in this panel lists Teamcenter features included in the disk image.

In the **Installation Directory** box, enter the path in which to install the disk image.

For more information about Teamcenter Integration Framework, see the Teamcenter Integration Framework documentation.

Product Excellence Program

In this step, you choose whether to participate in the Product Excellence Program.

Privacy statement

The Product Excellence Program helps Siemens Digital Industries Software understand how customers use our products and assists us in improving our products. The program is anonymous and participation is voluntary.

The Product Excellence Program is designed to protect the privacy of the user and the intellectual property created through the use of Siemens Digital Industries Software products.

How does it work?

The Product Excellence Program is used to collect data about your installation, the features you use and how you use them. The data is sent to Siemens Digital Industries Software for analysis. By examining usage patterns from a large number of people, we gain insight into how the products are used and how to improve the software in future releases. Data collection occurs in the background as you use the software and does not affect performance or functionality.

What data is sent?

The data collected can vary by product and by release as we gain more insight or add new capabilities. The Product Excellence Program may collect information on the functions utilized, the operating environment (for example, OS, RAM, graphics, etc.), product version, or other indications of user interaction. The data may also include the company name that is using the product. This data is solely used by Siemens Digital Industries Software to improve our products and is never shared with any third party.

There is no contact information in the data and Siemens Digital Industries Software will not contact you by phone or email as a result of the data collected. Absolutely no information about the data you create or manage is collected.

Participation is optional.

You can review and control your participation at any time.

A Teamcenter administrator can opt out of the Product Excellence Program during installation, or after installation by modifying the **TC_ProductExcellenceProgram** site preference in Teamcenter.

What does this mean for Teamcenter?

The following table provides examples of the type of usage data that is collected by Siemens Digital Industries Software and, as equally important, clarifies what data is *not* collected by Siemens Digital Industries Software.

What we collect	What we do *not* collect
The data collected contains information about how Teamcenter and Active Workspace are deployed and used, for example: • Active Workspace client and server version • Teamcenter server platform version, platform, and architecture • Database engine and Hosting application name, if any • Client page visits • Client browser type and locale • Command events executed (for example, **Open**) in the client • Active Workspace client locale • Summarized monthly License feature usage	The data collected *does not* contain user information or intellectual property, including: • Contact information or any data that would identify a natural person • Information about data created or managed in Active Workspace and Teamcenter • IT infrastructure identifiable information, including server IP addresses and host names

Participation in the program is enabled by default. A Teamcenter administrator can opt out of the program during installation through this panel, or after installation by modifying the **TC_ProductExcellenceProgram** site preference in Teamcenter.

AM Read Expression Service settings

In this step, you specify settings for the Access Manager Read Expression Service.

Specifying a start and end time for service ensures that the service will not burden business processes outside the specified time interval. If start and end times are *not* specified, the service runs throughout the day.

Value	Description
Start Time	Specifies the time of day, local time, that the service starts running. Type a value in 24-hour time format.
End Time	Specifies the time of day, local time, that the service stops running. Type a value in 24-hour time format.
Sleep Time	Specifies the time interval, in seconds, until the service becomes dormant. This interval begins after the latest execution has completed. By default, this value is set to **10** seconds. The recommended interval is **1800** seconds (30 minutes). Configuring sleep time helps conserve system resources during the time the service is running.

Revision Configuration Accelerator Service settings

In this step, you specify whether to install the Teamcenter Revision Configuration Accelerator Service.

The service is installed by default, so if you do *not* want to install the service, select the checkbox to *skip* installation of the service.

Configuring a microservices node

In this step, you configure a microservices node.

1. Choose a node type:

   Master Node Choose this option to configure a master microservice node.

   Exactly one master-type microservice node component is required in an environment. A master node must be configured before worker nodes.

   Worker Node Choose this option to configure a worker microservice node.

   You can add multiple worker-type microservice nodes as needed.

2. Under **Service Dispatcher**, configure the Service Dispatcher.

   The Service Dispatcher receives microservice requests from a Teamcenter client, queries the Service Registry to find an instance of the requested microservice, and then routes the request to an instance of the microservice.

Value	Description
Install Microservice	Select this check box to optionally install the Service Dispatcher on the microservice node.
Dispatcher Port	Specifies the port number for communication with the Service Dispatcher. The default value is **9090**.
Additional URLs	Specifies a comma-separated list of additional Service Dispatcher URLs.

3. Under **Service Registry**, configure the Service Registry.

   The Service Registry maintains a list of microservice instances. The Service Registry receives and processes the registration messages sent by microservice instances.

Value	Description
Install Microservice	Select this check box to optionally install the Service Registry on the microservice node.
Registry Port	Specifies the port number for communication with the Service Registry. The default value is **8787**.
Additional URLs	Specifies a comma-separated list of additional Service Registry URLs. All unique Service Registry URLs for the environment should be listed.

Configuring microservice registry and dispatcher

In this step, you configure the registry and dispatcher for the microservice node. These services are required if the microservices node is a master node, but are optional if it is a worker node.

Value	Description
Service Registry	Select this checkbox if you want to enable the service registry on the microservice node.
Registry Port	Specifies the port you want the service registry to use.
Service Dispatcher	Select this checkbox if you want to enable the service dispatcher on the microservice node.
Dispatcher Port	Specifies the port you want the service dispatcher to use.

5. Microservice framework

Deploying microservices with Docker

This panel provides information about the installation process for microservices with Docker.

Keystore settings for Microservice Framework

In this step, you specify keystore settings for Microservice Framework.

Value	Description
Keystore Password	Specifies the password for the keystore. Enter the password in the **Keystore Password** box and re-enter it in the **Confirm Password** box. The keystore password is used for generating the **.p12** files that contain keys for signing and validating authentication tokens. The tokens identify the logged-on user. Record the keystore password and keep it secure in case you want to open and edit the keys. The keystore for microservices must only be created once in the microservices framework. The signer and validator keys are zipped into a file in *TC_ROOT***jwt_config_tool**. Other microservice nodes access the keystore files from this node installation.
Keystore Zip File	Specifies the location of the keystore zip file (**keys.zip**) generated when you installed the microservice master node. The keystore file is generated in the **jwt_config_tool** directory under *TC_ROOT* on the microservice node host. For security, copy the **keys.zip** file to a directory on the Active Workspace Gateway host and specify that location here.

Configure microservice instances

In this step, you specify the number of instances to install of each microservice. Specify **0** or more for each microservice. Some microservices, such as the File Repository Service, do not support more than one instance.

Configuring a microservices node

In this step, you configure a microservices node.

1. Choose a node type:

   Master Node Choose this option to configure a master microservice node.

Exactly one master-type microservice node component is required in an environment. A master node must be configured before worker nodes.

Worker Node Choose this option to configure a worker microservice node.

You can add multiple worker-type microservice nodes as needed.

2. Under **Service Dispatcher**, configure the Service Dispatcher.

The Service Dispatcher receives microservice requests from a Teamcenter client, queries the Service Registry to find an instance of the requested microservice, and then routes the request to an instance of the microservice.

Value	Description
Install Microservice	Select this check box to optionally install the Service Dispatcher on the microservice node.
Dispatcher Port	Specifies the port number for communication with the Service Dispatcher. The default value is **9090**.
Additional URLs	Specifies a comma-separated list of additional Service Dispatcher URLs.

3. Under **Service Registry**, configure the Service Registry.

The Service Registry maintains a list of microservice instances. The Service Registry receives and processes the registration messages sent by microservice instances.

Value	Description
Install Microservice	Select this check box to optionally install the Service Registry on the microservice node.
Registry Port	Specifies the port number for communication with the Service Registry. The default value is **8787**.
Additional URLs	Specifies a comma-separated list of additional Service Registry URLs. All unique Service Registry URLs for the environment should be listed.

Configuring a microservices node

In this step, you configure a microservices node.

Microservices framework deployments on Linux require a running container registry. For environments that do not already have a container registry configured and running, you must deploy a registry

and secure it with HTTPS protocol for encrypted communication. Siemens Digital Industries Software provides scripts and sample Docker Swarm **.yml** and Kubernetes **.yaml** files to help get a container registry up and running.

For information about deploying a container registry for the Teamcenter microservices framework, see the *Teamcenter Installation on Linux Using TEM*.

For complete documentation of Docker Registry, see **https://docs.docker.com/registry/**.

Enter values for the microservices node:

Value	Description
Container Registry URL	Specifies the registry URL to store Docker images. The value should be in the form of a host name, FQDN, or *IP*:*port*. Do not include protocol, such as **http://** or **https://**. For example: **registry.example.com** This value should reference a live container registry. TEM attempts to connect to the registry. If the connection attempt fails, TEM does not allow you to continue.
Container Repository Name	Specifies the name of the container repository. The default value is **teamcenter**. This value must not contain spaces. The repository name must already exist in the container registry.
Keystore Password	Specifies the password for the keystore. Enter the password in the **Keystore Password** box and re-enter it in the **Confirm Password** box. The keystore password is used for generating the **.p12** files that contain keys for signing and validating authentication tokens. The tokens identify the logged-on user. Record the keystore password and keep it secure in case you want to open and edit the keys. The keystore for microservices must only be created once in the microservices framework. The signer and validator keys are zipped into a file in *TC_ROOT*/**jwt_config_tool**. Other microservice nodes access the keystore files from this node installation.
Dispatcher Port	Specifies a port to be used by the Service Dispatcher. The default value is **9090**.

Value	Description
	The Service Dispatcher receives microservice requests from a Teamcenter client, queries the Service Registry to find an instance of the requested microservice, and then routes the request to an instance of the microservice.

Update a microservices node

In this step, you enter settings to update a microservices node.

Value	Description
Container Registry URL	Specifies the registry URL to store Docker images. The value should be in the form of a host name, FQDN, or *IP*:*port*. Do not include protocol, such as **http://** or **https://**. For example: **registry.example.com** This value should reference a live container registry. TEM attempts to connect to the registry. If the connection attempt fails, TEM does not allow you to continue.
Container Repository Name	Specifies the name of the container repository. The default value is **teamcenter**. This value must not contain spaces. The repository name must already exist in the container registry.

Microservices framework deployments on Linux require a running container registry. For environments that do not already have a container registry configured and running, you must deploy a registry and secure it with HTTPS protocol for encrypted communication. Siemens Digital Industries Software provides scripts and sample Docker Swarm **.yml** and Kubernetes **.yaml** files to help get a container registry up and running.

For information about deploying a container registry for the Teamcenter microservices framework, see the appropriate Teamcenter installation guide for Deployment Center or TEM (Linux).

For complete documentation of Docker Registry, see **https://docs.docker.com/registry/**.

Configuring a microservices node

In this step, you configure a microservices node.

1. Choose a node type:

Master Node Choose this option to configure a master microservice node.

Exactly one master-type microservice node component is required in an environment. A master node must be configured before worker nodes.

If this is a master node, type a password in the **Keystore Password** box. The keystore password is used for generating the **.p12** files that contain keys for signing and validating authentication tokens. The tokens identify the logged-on user.

Record the keystore password and keep it secure in case you want to open and edit the keys.

Worker Node Choose this option to configure a worker microservice node.

You can add multiple worker-type microservice nodes as needed.

If this is a worker node, enter the location of the keystore zip file (**keys.zip**) in the **Keystore ZIP file** box.

The **keys.zip** file is generated when you install a microservice master node. The keystore file is generated in the **jwt_config_tool** directory under *TC_ROOT* on the microservice node host.

> Note:
>
> In TEM maintenance mode, no characters are displayed in the **Keystore Password** box to indicate that a password exists. If you enter a password in this box, TEM updates the password. If you leave this box blank, the existing password is retained.

2. Under **Service Dispatcher**, configure the Service Dispatcher.

The Service Dispatcher receives microservice requests from a Teamcenter client, queries the Service Registry to find an instance of the requested microservice, and then routes the request to an instance of the microservice.

Value	Description
Install Microservice	Select this check box to optionally install the Service Dispatcher on the microservice node.
Dispatcher Port	Specifies the port number for communication with the Service Dispatcher. The default value is **9090**.
Additional URLs	Specifies a comma-separated list of additional Service Dispatcher URLs.

3. Under **Service Registry**, configure the Service Registry.

   The Service Registry maintains a list of microservice instances. The Service Registry receives and processes the registration messages sent by microservice instances.

Value	Description
Install Microservice	Select this check box to optionally install the Service Registry on the microservice node.
Registry Port	Specifies the port number for communication with the Service Registry. The default value is **8787**.
Additional URLs	Specifies a comma-separated list of additional Service Registry URLs. All unique Service Registry URLs for the environment should be listed.

Configure the File Repository microservice

In this step, you configure the File Repository microservice.

The File Repository microservice stores Active Workspace content to delivery through the Active Workspace Gateway to client hosts.

Value	Description
File Repository Storage Location	Specifies the path to the storage location for the file repository to be used by the Active Workspace Gateway, for example, **c:\tc\file_repository**. On Linux hosts, the path to the storage location must exist on the current host. On Windows hosts, TEM creates the directory if it does not exist. If you install multiple instances of the File Repository microservice, all instances must reference the same physical storage location. Active Workspace uses a file repository microservice. To configure that service for deployment on a Linux host, parameter values Deploying User UID, Deploying User GID, and File Repository Storage Location values are required. Values entered for the master microservice node must be valid on all worker nodes.
User ID	(Linux hosts only) Specifies the user ID of user installing the File Repository Microservice. If you install master and worker microservice nodes, the user must exist on all nodes.
Group ID	(Linux hosts only) Specifies the Group ID of user installing the File Repository Microservice.

6. Active Workspace

Artifact Service settings

In this step, you specify settings for the Artifact Service for the declarative user interface.

This panel is displayed only on Windows hosts.

Value	Description
Artifact Service URL	Specifies the URL to the Artifact Service.
Artifact Repository Path	Specifies the path to declarative artifact repository used by the Artifact Service. If you do not enter a value, Teamcenter creates a repository parallel to the artifact service.
Artifact Service Port	Specifies the port on which the Artifact service runs.

Teamcenter database server for Active Workspace

In this step, you the specify settings for the Teamcenter database such as the database server and connection values.

Active Workspace translator selection

In this step, you select a type of translator to use for indexing. For example:

- **Active Workspace Object Data Translator**

  Translator for indexing object data. This is the standard search indexer.

- **Active Content Structure Translator**

  Translator for indexing structure data.

Visualization server pool assigner settings

In this step, you specify settings for the visualization server pool assigner. This panel is displayed if you selected the **Visualization Server Pool Assigner** feature.

Value	Description
Host	Specifies the host on which this Visualization Server Pool Assigner runs. This is the host on which this Visualization Server Pool Assigner is deployed. You may type the host name or IP address of the host.
Vis Assigner Port	Specifies the port used by the local Visualization Server Pool Assigner.
Gateway Connection Port	Specifies the port to use to connect to Active Workspace Gateway. The default value is **8089** .
Add pool assigner	Specifies whether additional Visualization Server Pool Assigners are used. Select the **Add pool assigner** check box to add pool assigners.
Peer Assigners	The **Peer Assigners** table lists other Visualization Server Pool Assigners known to the local Visualization Server Pool Assigners
Assigner Host	Specifies the host on which a peer Visualization Server Pool Assigner is deployed. This value can be the host name or IP address.
Assigner Port	Specifies the port number used by the peer Visualization Server Pool Assigner.
Server Side 4-tier URL	Specifies an alternate four-tier URL for the Visualization Server in case the primary four-tier URL is blocked by a firewall, or if a more direct route is needed for performance.

Visualization server pool assigner settings

In this step, you specify settings for the visualization server pool assigner. This panel is displayed if you selected the **Visualization Server Pool Assigner** feature.

Value	Description
Local Assigner Settings	Local assigner settings define the local host as a Visualization Server Pool Assigner. To define your local host as an assigner, type the host and port values of the local host.
Host	Specifies the host on which this Visualization Server Pool Assigner runs. You may type the host name or IP address of the host.

Value	Description
Port	Specifies the port used by the local Visualization Server Pool Assigner.
Add pool assigner	Specifies whether additional Visualization Server Pool Assigners are used. Select this check box to add pool assigners.
Peer Assigners	The **Peer Assigners** table lists other Visualization Server Pool Assigners known to the local Visualization Server Pool Assigners
Assigner Host	Specifies the host on which a peer Visualization Server Pool Assigner is deployed. This value can be the host name or IP address.
Assigner Port	Specifies the port number used by the peer Visualization Server Pool Assigner.

Visualization Server Manager

In this step, you specify settings for the Visualization Server Manager.

You can use the local server manager settings to override the host name and port value with the host and port values you enter in this panel.

Value	Description
Configuration	Values for configuring the Visualization Server Manager.
Local Host Alias	Specifies and alias for the local Visualization Server Manager.
Server Host	Specifies the host where the Visualization Server Manager is running. This should be the local host name and must be resolvable by the Visualization Pool Assigner machine. Do not use **localhost** or **127.0.0.1**.
Server Port	Specifies the port on which the Visualization Server Manager is running.
Max Servers in Sub-Pool	Specifies the maximum number of Visualization server processes allowed to run in this pool (for a single-host configuration) or in this subpool (for a multihost configuration). On Windows machines, the default value is **30**. On Linux machines, the default value is **200**.

Value	Description
Min Warm Servers	Specifies the minimum number of Visualization Server processes in this pool that are started but not assigned. Note: If necessary to maintain the minimum number of warm servers while not exceeding the maximum number of server processes, the server manager times out servers in use.
Visualization Data Server Configuration	Values for configuring a Visualization Data Server, which provides improved performance by caching product structure and JT parts files.
Add Visualization Data Server	Specifies you use a Visualization Data Server.
Host	Specifies the name of the host on which the Visualization Data Server is installed.
Port	Specifies the port number used by the Visualization Data Server.

Visualization Server Manager settings

In this step, you specify settings for the local Visualization Server Manager.

Value	Description
Override local node settings	Specifies whether to override the host name and port value. If you want to do this, type the host and port values of the local host in the following boxes.
Host	This can be the host name or IP address of the server or pool assigner.
Port	Specifies the port on which the server or pool assigner listens for requests.
Visualization Server Pool Assigners	The Visualization Server Pool Assigners table lists the pool assigners used by the local Visualization Server Manager.
Assigner Host	Specifies the host name of the host where the pool assigner is running.
Assigner Port	Specifies the port value of the pool assigner.

Visualization Server Manager settings

In this step, you specify settings for the local Visualization Server Manager.

Value	Description
Override local node settings	Specifies whether to override the host name and port value. If you want to do this, type the host and port values of the local host in the following boxes.
Host	This can be the host name or IP address of the server or pool assigner.
Vis Assigner Port	Specifies the port on which the server listens for requests.
Gateway Connection Port	Specifies the port through which the Active Workspace Gateway connects to the Visualization Server Manager. The default value is **3000**.
Visualization Server Pool Assigners	The Visualization Server Pool Assigners table lists the pool assigners used by the local Visualization Server Manager.
Assigner Host	Specifies the host name of the machine where the Visualization Server Pool Assigner runs.
Assigner Port	Specifies the port value of the pool assigner.

Visualization Server Manager settings

In this step, you specify settings for the local Visualization Server Manager.

Value	Description
Override local node settings	Specifies whether to override the host name and port value. If you want to do this, type the host and port values of the local host in the following boxes.
Host	This can be the host name or IP address of the server or pool assigner.
Vis Assigner Port	Specifies the port used by the local Visualization Server Pool Assigner.
Gateway Connection Port	Specifies the port through which the Active Workspace Gateway connects to the Visualization Server Pool Assigner. The default value is **3000**.
Peer Assigners	The Peer Assigners table lists the pool assigners used by the local Visualization Server Manager.

Value	Description
Assigner Host	Specifies the host name of the host where the pool assigner is running.
Assigner Port	Specifies the port value of the pool assigner.
Server Side 4-tier URL	Specifies an alternate four-tier URL for the viewer to connect to Teamcenter. The Visualization Server uses this in case the primary four-tier URL is blocked by a firewall, or if a more direct route is needed for performance.

Visualization Server Pool Assigner settings for .NET

In this step, you specify Visualization Server Pool Assigner settings for the .NET web tier.

In the **Virtual Directory Name** box, enter the name of the virtual directory you want to create for the Visualization Server Pool.

Configuring Active Workspace for the .NET web tier

In this step, you specify Active Workspace settings for the .NET web tier.

Value	Description
Teamcenter Web Tier URL	Specifies the URL for the Teamcenter web application. The URL should be of this form: **http://***host***:***port***/tc** Replace *host* with the host on which the web tier application is deployed. Replace *port* with the port used by the web application server. The default port is **7001**.
Use as Bootstrap URLs	Specifies you want to use bootstrap URLs. The Active Workspace Gateway integrates with your FMS system to download/upload Teamcenter files. The FMS FSC servers that are used are either automatically assigned by the FMS system using bootstrap URLs, or explicitly declared using assigned FSC URLs. To use bootstrap URLs, select this option and fill in the **Bootstrap URLs** and **Bootstrap Client IP** boxes. On Linux hosts, if you select **Use as Bootstrap URLs** , you need to ensure the client map is configured correctly.

Value	Description
Bootstrap URLs	Specifies a comma-separated list of one or more FMS bootstrap URLs. URLs must be of this form: **http://***host***:***port* By default, the IP address from the HTTP connection of the requestor is used unless a **Bootstrap Client IP** value is provided. (The client/requestor is the host on which Active Workspace Gateway is deployed.)
Bootstrap Client IP	Specifies the FMS bootstrap client IP address to be used for the assignment. On Linux hosts, enter the internal IP address of the Active Workspace Gateway machine.
Use Assigned FSC URLs	Specifies you want to assign FSC URLs. Select this only if you want explicit control of the FSCs used. To use assigned FSCs, select this option and fill in the **Assigned FSC URLs** box.
Assigned FSC URLs	Specifies a comma-separated list of one or more assigned FSC URL values. The URL values entered are directly used for file operations. This allows you to declare the FSC servers that should be used.

To specify additional Active Workspace settings, click **Advanced**.

Security keys and cache control settings

In this step, you specify parameters for caching static resources for the Active Workspace gateway. These settings help optimize client performance.

Value	Description
Maximum Age	Specifies the lifespan of cached items as a number of intervals. Select the interval from the dropdown list: • **Months** • **Days** • **Hours** • **Minutes** • **Seconds**

Value	Description
	For example, to specify a lifespan of seven days, type **7** and select **Days**. **Maximum Age** must be a numeric value.

Active Workspace architecture changes

Active Workspace is no longer deployed in a Java EE WAR file or the .NET framework. It now employs the Active Workspace Gateway and microservices. Before you continue, make sure you read and understand the Active Workspace deployment architecture described in the installation documentation.

Active Workspace Gateway settings

In this step, you specify parameters for Active Workspace Gateway.

Value	Description
Teamcenter Web Tier URL	Specifies the URL for the Teamcenter web application. The URL should be of this form: **http://***host***:***port***/tc** Replace *host* with the host on which the web tier application is deployed. Replace *port* with the port used by the web application server. The default port is **7001**.
Visualization Assigner URL	Specifies the URL to the Visualization Server Assigner. The URL should be of this form: **http://***host***:***port*
Easy Plan URL	Specifies the URL to the Easy Plan application, if installed. The URL should be of the following form: **http://***host***:***port***/***application-name* For example, if your server name is **myWebServer**, your port is **7007**, and the **.war** file is named **tc.war**, type: **http://myWebServer:7007/tc**
NGP URL	Specifies the URL to the Next Generation Planning (NGP) application, if installed. The URL should be of the following form:

Value	Description
	http://*host***:***port***/***application-name*
Service Dispatcher URLs	Specifies a comma-separated list of URLs to the Service Dispatcher. Use fully-qualified domain names or IP addresses in URLs.
Container Registry URL	Specifies the registry URL to store Docker images. The value should be in the form of a host name, FQDN, or *IP*:*port*. Do not include protocol, such as **http://** or **https://**. For example: **registry.example.com** This value should reference a live container registry. TEM attempts to connect to the registry. If the connection attempt fails, TEM does not allow you to continue.
Container Repository Name	Specifies the name of the container repository. The default value is **teamcenter**. This value must not contain spaces. The repository name must already exist in the container registry.
Gateway Service Port	Specifies the port used by the Active Workspace Gateway. The default value is **3000**. The URL to the Active Workspace client interface is based on this port.
FMS Settings	Settings for accessing FMS volumes.
Use as Bootstrap URLs	Specifies you want to use bootstrap URLs. The Active Workspace Gateway integrates with your FMS system to download/upload Teamcenter files. The FMS FSC servers that are used are either automatically assigned by the FMS system using bootstrap URLs, or explicitly declared using assigned FSC URLs. To use bootstrap URLs, select this option and fill in the **Bootstrap URLs** and **Bootstrap Client IP** boxes. On Linux hosts, if you select **Use as Bootstrap URLs** , you need to ensure the client map is configured correctly.
Bootstrap URLs	Specifies a comma-separated list of one or more FMS bootstrap URLs. URLs must be of this form: **http://***host***:***port*

Value	Description
	By default, the IP address from the HTTP connection of the requestor is used unless a **Bootstrap Client IP** value is provided. (The client/requestor is the host on which Active Workspace Gateway is deployed.)
Bootstrap Client IP	Specifies the FMS bootstrap client IP address to be used for the assignment. On Linux hosts, enter the internal IP address of the Active Workspace Gateway machine.
Use Assigned FSC URLs	Specifies you want to assign FSC URLs. Select this only if you want explicit control of the FSCs used. To use assigned FSCs, select this option and fill in the **Assigned FSC URLs** box.
Assigned FSC URLs	Specifies a comma-separated list of one or more assigned FSC URL values. The URL values entered are directly used for file operations. This allows you to declare the FSC servers that should be used.

To specify additional Active Workspace Gateway settings, click **Advanced**.

About the container registry

Microservices framework deployments on Linux require a running container registry. For environments that do not already have a container registry configured and running, you must deploy a registry and secure it with HTTPS protocol for encrypted communication. Siemens Digital Industries Software provides scripts and sample Docker Swarm **.yml** and Kubernetes **.yaml** files to help get a container registry up and running.

For information about deploying a container registry for the Teamcenter microservices framework, see *Active Workspace Installation*.

For complete documentation of Docker Registry, see **https://docs.docker.com/registry/**.

Active Workspace client settings

In this step, you specify additional Active Workspace client settings.

Value	Description
Publish to Gateway	Select this check box to enable automatic publishing of Active Workspace content to the Gateway.
Gateway URL	Specifies the URL to the Active Workspace Gateway. The URL should be of this form: **http://***host***:***port* Replace *host* with the host on which you installed the Gateway. Replace *port* with the port you specified when you installed the Gateway. For example: **http://localhost:3000**
Select Client Locales	Select additional locales to include in Active Workspace client file configuration.

Publish to the Active Workspace Gateway

In this step, you specify settings to enable publishing of changes to the Active Workspace Gateway.

Value	Description
Publish to Gateway	Select this check box to enable automatic publishing of changes to the Active Workspace Gateway.
Gateway URL	Specifies the URL to the Active Workspace Gateway, of the form: **http://***host***:***port*

Active Workspace Server Extensions settings

In this step, you specify parameters for configuring the Active Workspace server extensions feature.

Value	Description
Search Engine URL	Specifies the URL of the Teamcenter Solr database. Type a value in the following format: **http://***host***:***port***/solr**

Value	Description
	Replace *host* with the host on which Solr runs. Replace *port* with the port value used by Solr. The default value is **8983**.
Use additional search engine URLs	Specifies you use multiple search engines for failover. If you select the **Use additional search engine URLs** ☑ check box, type additional search engine URLs in the **Search Engine URL List** table.

Additional settings for Active Workspace Gateway

In this step, you specify additional settings for the Active Workspace Gateway.

Value	Description
Enable Teamcenter Share Collaboration	Specifies you want to enable and configure Teamcenter Share Collaboration. For more information about this feature, see *Teamcenter Share* in the Teamcenter documentation.
Teamcenter Share Collaboration	Values for configuring the Teamcenter Share Collaboration integration to Teamcenter.
Teamcenter Share URL	Specifies the URL to the Teamcenter Share site. The default value is **https://share.sws.siemens.com**.
Client ID	Specifies the SAMAuth client ID you obtained through SAM URL.
Client Secret ID	Specifies the client secret ID you obtained through SAM URL.

MBSE Integration Gateway settings

In this step, you specify the URL to the Teamcenter server in the **URL** box. This value is required by the MBSE Integration Gateway.

Active content structure translator settings

In this step, you specify settings for the active content structure translator.

TEM displays this panel only if you selected the **Active Workspace Content Structure Translator**.

Value	Description
Maximum Limit	Specifies the maximum number of translations that can run simultaneously. The default is **3**, the minimum value is **1**.

CALM integration settings

In this step, you specify settings for the Capital Asset Lifecycle Management (CALM) integration.

Value	Description
Client ID	Specifies the iModel agent client public ID.
Client Secret	Specifies the iModel agent client private secret.
Client Scope	Specifies the scope value of the iModel agent.

Active Workspace 4GD translator settings

In this step, you specify settings for the Active Workspace 4GD translator.

Value	Description
Maximum Limit	Specifies the maximum limit of the number of tasks the translator can handle.

Custom routes to Active Workspace Gateway

In this step, you optionally enter additional routes to the Active Workspace Gateway.

- To add a path to the table, click **Add**, and then add a path and URL.
- To remove a path from the list, select the path and then click **Remove**.

Active Workspace indexer advanced settings

In this step, you specify advanced settings for the Active Workspace indexer.

Value	Description
Maximum Teamcenter Connections	Specifies the maximum number of connection between the Teamcenter server and the indexer to be open at a given time. This value should be less than the number

Value	Description
	of warmed up Teamcenter servers available in the server manager. The default value is **3**. The minimum value allowed is **1**.
Teamcenter Retry Count	Specifies the number of tries to connect to the Teamcenter server. The default value is **3**. The minimum value allowed is **1**.

Active Workspace indexer settings

In this step, you specify parameters for the Active Workspace indexer.

Value	Description
Teamcenter Web Tier URL	Specifies the URL for the deployed Java EE Teamcenter web application. The URL should be of this form: **http://***host***:***port***/***war-file-name* Replace *host* with the host running the web application server on which the Teamcenter web application is deployed. Replace *port* with the port used by the web application server. Replace *war-file-name* with the name of the Teamcenter web application **.war** file. (The default name is **tc**.)
Maximum Teamcenter Connections	Specifies the maximum number of connection between the Teamcenter server and the indexer to be open at a given time. This value should be less than the number of warmed up Teamcenter servers available in the server manager. The default value is **3**. The minimum value allowed is **1**.
Teamcenter Retry Count	Specifies the number of tries to connect to the Teamcenter server. The default value is **5**. The minimum value allowed is **1**.
Install Indexer as a Service	Specifies you want to install the indexer as a service.
Indexing Service Name	Specifies the name of the synchronization indexer service.
Service Interval (seconds)	Specifies the interval of the synchronization indexer service.

Value	Description
Start Service	Specifies you want to start the synchronization indexer service.
Builder Service Name	Specifies the name of the suggestion builder indexer service.
Service Interval (seconds)	Specifies the interval of the suggestion builder indexer service.
Start Service	Specifies the name of the suggestion builder indexer service.
Staging Directory	Specifies the staging directory used by the indexer. This directory is the location where the indexer is installed.

To specify additional connection settings for the Active Workspace indexer, click **Advanced.**

Indexing Engine configuration

In this step, you specify values for Indexing Engine.

Value	Description
SOLR schema files location	Specifies the location of the Solr schema files. Enter the path that contains the Solr schema files. This allows the Solr and Teamcenter schemas to be automatically merged during installation of the Indexing Engine. If you leave this box blank, the schemas are not automatically merged; you must manually merge them after installing the Indexing Engine. The Solr schema files are created on the corporate server when installing the Server Extensions. Two schema files are located in *TC_DATA***ftsi\solr_schema_files**: • **TC_ACE_SOLR_SCHEMA.xml** • **TC_SOLR_SCHEMA.xml** If you did not install the Server Extensions on the corporate server, you can complete the installation of the Indexing Engine, but the schemas are not automatically

Value	Description
	merged. You must manually merge them after installing the Indexing Engine and the Server Extensions.
JRE Location	Specifies the location of the Java Runtime Environment (JRE) on the Indexing Engine host.
Install indexing engine as a service	Specifies you want to install the Indexing Engine as a service. If you leave this check box cleared, you must start the Indexing Engine manually.

Active Workspace indexer type selection

In this step, you specify the types of indexers to use for Active Workspace.

Select the indexers you want to use according to the Teamcenter features you use.

If you use Dispatcher-based indexing, select the same indexer types for this and for the **TcFtsIndexerTrans** translator.

Indexing Engine user

In this step, you enter credentials for the Solr administrator. These credentials must match for the Indexing Engine, the Indexer, Server Extensions, and the TcFTS Indexer Translator (if used).

Value	Description
User	Specifies the user name of the Solr administrator.
Password	Specifies the password for the Solr administrator account.

Microservice Framework requirement

The Active Workspace Gateway requires Microservice Framework.

Make sure you install the Microservice Framework before you install the Active Workspace Gateway.

Gateway Service settings

In this step, you specify settings for the Gateway Service used by the Gateway Client.

This panel is displayed only on Windows hosts.

Value	Description
Gateway Service Port	Specifies the port on which the Gateway Service runs. Default port is 3000.
Active Workspace URL	Specifies the URL to the Active Workspace server.
Use system version of Node.js instead of bundled version	Specifies you want to use an existing version of **Node.js** on the Gateway Service host. Select this option if you want to use your own installed version of **Node.js** *instead* of the version packaged with Active Workspace. If you select this option, enter the path to the preferred **Node.js** in the **Node.js Path** box.

Gateway security settings

In this step, you configure settings for the Active Workspace Gateway.

Value	Description
Keystore Zip File	Specifies the location of the keystore zip file (**keys.zip**) generated when you installed the microservice master node. The keystore file is generated in the **jwt_config_tool** directory under *TC_ROOT* on the microservice node host. For security, copy the **keys.zip** file to a directory on the Active Workspace Gateway host and specify that location here.
Enable TcSS Support	Values for configuring Security Services.
Enable TcSS Support	Specifies you want to enable Security Services support in Active Workspace.
TcSS Application ID	Specifies the Security Services application ID.
TcSS Login URL	Specifies the logon URL for the Security Services application. For details about configuring Security Services, see *Security Services Configuration* in Teamcenter documentation. When you configure Active Workspace for Security Services, be sure to only install the language packs for the Security Services that Active Workspace supports. If Active Workspace is deployed on a different URL, you must configure Security Services with multiple application IDs.
Security Key Settings	Security key values for Teamcenter.
Security Certificate	Specifies the path to the security certificate.
Security Key	Specifies the path to the security key file.

MATLAB client information

In this step, you specify settings for the MATLAB integration for the MBSE Integration Gateway.

Value	Description
MATLAB Installation Directory	Specifies the location where MATLAB is installed. This must be the directory containing the **bin** directory. This becomes the MATLAB root directory.
Staging Directory	Specifies the location where models downloaded from Teamcenter are stored, for example, **C:\StagingDir\MATLAB**.

Configure the Classification AI microservice

In this step, you configure the Classification AI microservice.

Classification artificial intelligence (AI) provides assistance in classifying new objects in Active Workspace. This can save time, for example, in workflows with frequently-used classes.

The classification AI engine must be trained on the data in your database, creating a model that is then validated on a new dataset to verify whether the trained model is correct. Each iteration of this process further refines the model. The training outputs a data model (a set of files) that is used to deliver suggested classes.

Value	Description
Classification AI Model Location	Specifies the path in which to place the classification AI model. The default path is *TC_ROOT***ms_node_config\ai_model**.

Required microservices

This panel notifies you that some features you selected for installation require the specific microservices listed in the panel. Use the **Back** buttons to return to the **Features** panel and select the required microservices.

Configuring the Requirements Management microservice

In this step, you supply required values for the Requirements Management microservice.

Value	Description
FSC URL	Specifies the URL to the FMS server cache (FSC).

Configuring the Requirements Management microservice

In this step, you supply required values for the Requirements Management microservice.

Value	Description
Teamcenter Web Tier URL	Specifies the URL to the Teamcenter web tier. Enter a value of the following form: **http://***host***:***port***/tc** For example: **http://myHost:7001/tc**

Configure the GraphQL microservice

In this step, you enter values needed by the GraphQL microservice.

The GraphQL microservice allows the Active Workspace client to query and fetch data from multiple data sources simultaneously, without needing to know which data comes from which source.

Value	Description
Teamcenter Web Tier URL	Specifies the URL to the Teamcenter web tier. Enter a value of the following form: **http://***host***:***port***/tc** For example: **http://myHost:7001/tc**

Advanced settings for Active Workspace object data indexer

In this step, you specify advanced settings for the Active Workspace object data indexer.

Value	Description
Maximum Query Timespan	Specifies the maximum span of a Teamcenter query in minutes (maximum=50000, minimum=5000, default=20000).
Export Batch Size	Specifies the maximum number of Teamcenter objects handled in one thread (maximum=1000, minimum=1, default=1000).

Active Workspace object data indexer settings

In this step, you specify data extraction times for the Active Workspace object data indexer.

Value	Description
Start Time	Specifies the start date and time for extracting data. All data modified after this date and time is extracted for indexing. Data older than the specified date and time is not extracted. These values are only used during first-time indexing or re-indexing. Type a **Date** value of the form *dd-MMM-yyyy*, for example, **01-JAN-2022**. Type a **Time** value of the form *HH:mm* in 24-hour format, for example, **23:59**.
No End Time	Specifies end date is the current time.
End Time	Specifies the end date and time for extracting data. All data modified before this date and time is extracted for indexing. These values are only used during first-time indexing or re-indexing. Type a **Date** value of the form *dd-MMM-yyyy*, for example, **01-JAN-2012**. Type a **Time** value of the form *HH:mm* in 24-hour format, for example, **23:59**.

Active Workspace object data translator settings

In this step, you specify settings for the Active Workspace object data translator.

TEM displays this panel only if you selected the **Active Workspace Object Data Translator**.

Value	Description
Maximum Limit	Specifies the maximum limit of the number of tasks the translator can handle. The default is **3**, the minimum value is **1**.

Configuring the predictive UI microservice

In this step, you choose whether to create a new database for the predictive UI microservice, or use an existing database.

The database for the predictive UI microservice stores command histories and other data for the Active Workspace Assistant.

- **Create user and database**

  Choose this option to create a new database user and database. You must be prepared to enter database system credentials when TEM prompts you.

- **Use existing user and database**

  Choose this option if you want to use an existing database user and database. You database administrator must create the database user and database before you proceed.

Connection settings for the predictive UI microservice

In this step, you specify Oracle connection settings for the predictive UI microservice.

Value	Description
Port	Specifies the number of the port on which the Oracle server listens. The port number was determined when the Oracle server was installed.
Enable TCPS	If you want to use secured communication with the database using secure TCP (TCPS), select the **Enable TCPS** check box, and then enter the following values. If you do not select this check box, Teamcenter uses TCP by default.
Wallet Location	Specifies the location of the secure wallet that stores CA certificates.

Value	Description
	This is the Oracle **auto_login** wallet configured on the file system. The user under which the deployer is triggered should have read access to this folder.
SSL Version	Specifies the installed TLS version.

Configure a database for the predictive UI microservice

In this step, you configure a database for the predictive UI microservice.

The database for the predictive UI microservice stores command histories and other data for the Active Workspace Assistant.

In the **Database Server** box, select your database vendor (**Oracle** or **Microsoft SQL Server**).

Enter the following database configuration values, depending on the database vendor you select.

Oracle database server values

Value	Description
Host	Specifies the name of the host on which the Oracle server runs. This host must exist, and the Oracle server must be installed.
Service	Specifies the name of the service for the Oracle instance. The service name was determined when the Oracle server was installed.
Port	Specifies the number of the port on which the Oracle server listens. The port number was determined when the Oracle server was installed.
User	Specifies a database user name: • To connect to an existing database configured for use with Teamcenter, enter the name defined for a database user when the database was configured. • To create and configure a database for use with Teamcenter, enter the name of the database user you want to create.
Password	Specifies a database password:

Value	Description
	• To connect to an existing database configured for use with Teamcenter, enter the password defined for the database user when the database was configured. • To configure a new database for use with Teamcenter, enter a password for the database user you are creating.

If you chose to create a new database instead of using an existing database, provide the following values:

System User

Specifies a user name of the Oracle system administrator account. The default value is **system**.

Password

Specifies a password for the Oracle system administrator account.

> Caution:
>
> The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab.
>
> In addition, the password must not contain any of the following characters:
>
> **! # @ $ % = & ' " ^ : ; . _ < > ( ) { }**

Database Path

Specifies the location of the tablespaces for the Teamcenter database on the Oracle server. This is typically *ORACLE_HOME***oradata***Oracle_SID* (on Windows systems) or *ORACLE_HOME*/**oradata**/*Oracle_SID* (on Linux systems).

> Note:
>
> The **Database Path** must exist and you must have write permission to the directory.

Data Directory

Specifies the path to the Teamcenter data (*TC_DATA*) directory.

This value is stored in the **TC_DATA** variable in your Teamcenter configuration. TEM creates shared data subdirectories and files in this location. Each data directory is associated with a single database user within a database instance.

> Note:
>
> Do not create a **TC_DATA** variable in the system environment. TEM sets this variable as required in Teamcenter scripts. Setting

Value	Description
	this variable in the operating system causes conflicts if you install more than one configuration.
Share Name	Specifies a name for the Teamcenter network share. Enter a name or accept the default value. During Teamcenter installation, TEM creates the network share to the configuration directory (accessible as *****server-name******share-name*) where client workstations can access configuration information. Because this shared directory is accessed using the UNC path, the server must be connected to the network during the installation.

Microsoft SQL Server values

Value	Description
Instance	If you connect to Microsoft SQL Server using a named instance, select this option and enter the instance name you defined when you installed MS SQL Server.
Port	If you connect to Microsoft SQL Server using a specific port, select this option and enter the port number you specified when you installed MS SQL Server.
Login Name	Specifies a database user name: • To connect to an existing database configured for use with Teamcenter, enter the name defined for a database user when the database was configured. • To create and configure a new database for use with Teamcenter, enter the name of the database user you want to create.
Login Password	Specifies the password for the database user: • To connect to an existing database configured for use with Teamcenter, enter the password defined for the database user when the database was configured. • To configure a new database for use with Teamcenter, enter a password for the database user you are creating.
Database Name	Specifies the name of the MS SQL Server database. The database name was determined when database was created.

Value	Description
If you chose to create a new database instead of using an existing database, provide the following values:	
System User	Specifies the user name of the SQL Server system administrator account. The default value is **sa**.
Password	Specifies the password for the SQL Server system administrator account. Caution: The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab. In addition, the password must not contain any of the following characters: **! # @ $ % = & ' " ^ : ; . _ < > ( ) { }**
Database Path	Specifies the directory in which to create the Teamcenter database on the SQL Server server.
Collation	Specifies the collation used by the Teamcenter database on the Microsoft SQL Server server. *Collation* defines the alphabet or language whose rules are applied when data is sorted or compared.
Enable UTF-8	Specifies whether to enable support for UTF-8 encoding in the Teamcenter database. Microsoft SQL Server does not provide native support for UTF-8. The **Enable UTF-8** option enables the Teamcenter server to convert character encoding to and from UTF-8 when interacting with the database. For information about configuring your Teamcenter host to support UTF-8, see the Teamcenter installation guides for Windows and Linux.
Data Directory	Specifies the path to the Teamcenter data (*TC_DATA*) directory. This value is stored in the **TC_DATA** variable in your Teamcenter configuration. TEM creates shared data subdirectories and files in this location. Each data directory is associated with a single database user within a database instance. Note: Do not create a **TC_DATA** variable in the system environment. TEM sets this variable as required in Teamcenter scripts. Setting this

Value	Description
	variable in the operating system causes conflicts if you install more than one configuration.

Database system credentials for the Command Prediction Service

In this step, you specify database system settings for the Command Prediction Service.

Value	Description
User	Type the database system user name for the database instance that contains Command Prediction Service database.
Password	Type the system user password for the database instance. Command Prediction Service database.

Command Prediction Service database settings

In this step, you specify database settings for the Command Prediction Service.

Value	Description
User	Type the user name for the Command Prediction Service database.
Password	Type the password for the Command Prediction Service database. Type the password a second time in the **Confirm** box to confirm.

Configuring the Command Prediction Service database

In this step, you choose whether to keep the Command Prediction Service database.

- **Keep Command Prediction Service database**

  Choose this option to keep the current database for the Command Prediction Service.

- **Drop Command Prediction Service database**

  Choose this option to delete the current database for the Command Prediction Service.

FTS indexer translators

In this step, you select indexer translators to install.

FTS indexer translator settings

In this step, you specify settings for FTS indexer translators.

Value	Description
Teamcenter 4-tier URL	Specifies the URL to the Teamcenter web server. The format is: **http://***host***:***port***/***web-app-name* Replace *host* with the host name of the machine the runs the web application server on which the Teamcenter web application is deployed. Replace *port* with the port used by the web application server. Replace *web-app-name* with name of the Teamcenter web application. The default is **tc**.
Teamcenter Retry Count	Specifies the number of attempts to connect to the Teamcenter server.

Visualization Data Server configuration

In this step, you specify settings for the Visualization Data Server.

Value	Description
Server Port	Specifies the port number on which the Visualization Data Server listens.
Teamcenter Web Tier URL	Specifies the URL of the Teamcenter web tier application. The URL must be similar to the following form: **http://***host***:***port***/***tc-web-app* *host* is the machine running the web application server on which the Teamcenter web application is deployed.

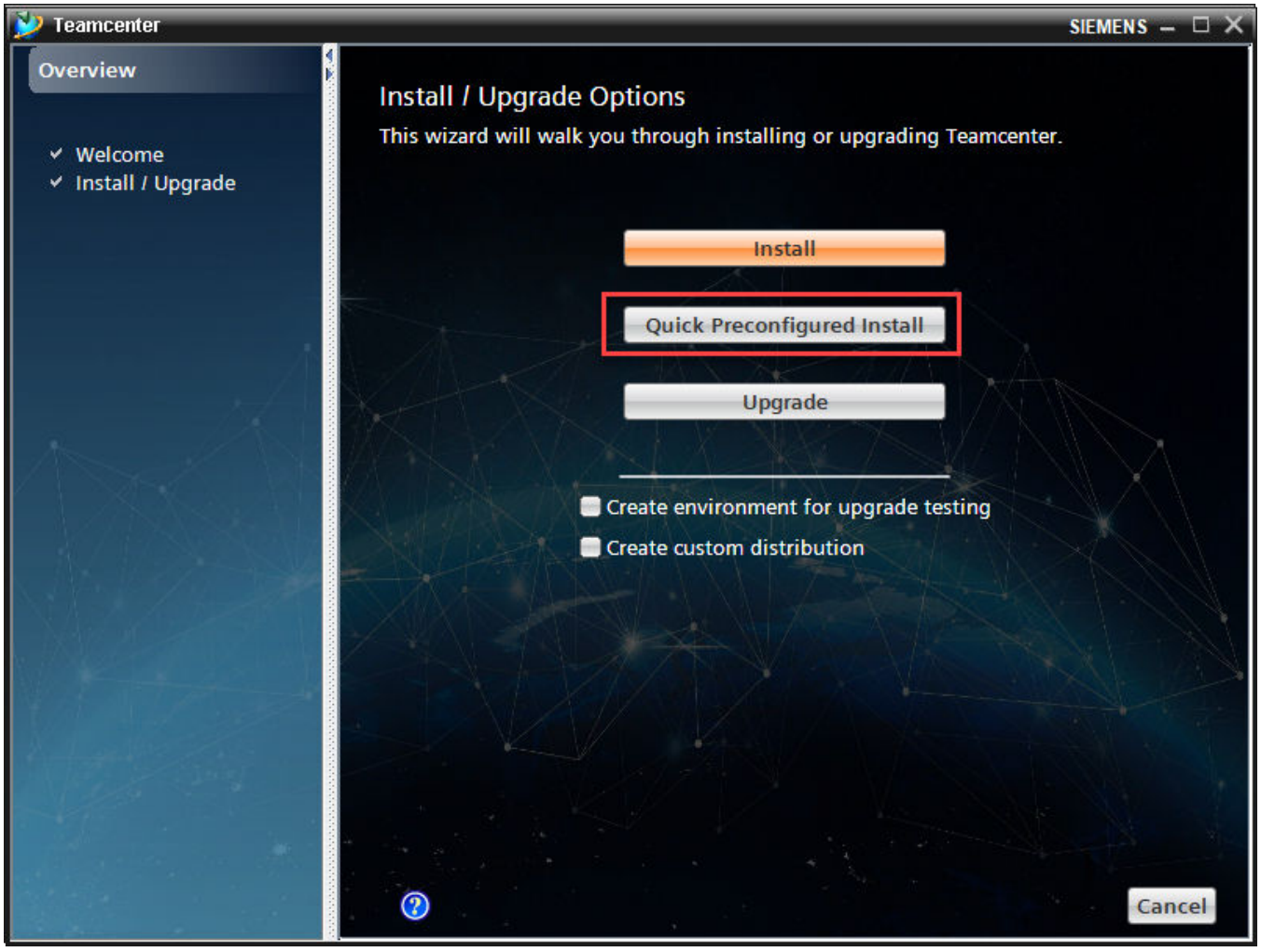
Value	Description
	port is the port value used by the web application server. *tc-web-app* is the name of the Teamcenter web application. The default is **tc**.

7. Quick preconfigured installation

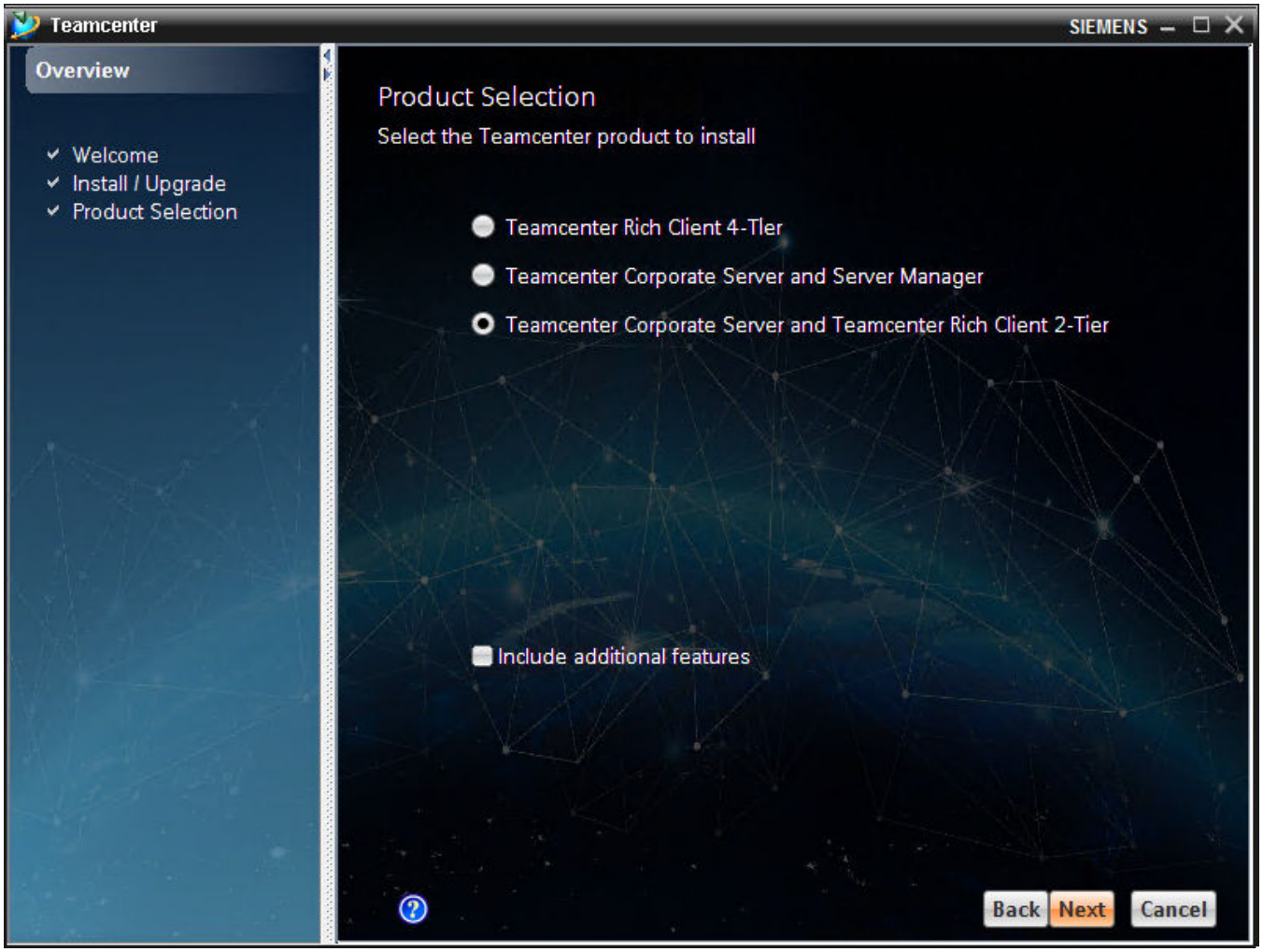
About quick preconfigured installation in TEM

The following TEM help topics describe panels for creating a quick preconfigured installation of Teamcenter.

TEM provides a set of predefined common Teamcenter configurations that require minimal user input to install. To create one of these installations, click **Quick Preconfigured Install** in the **Install/Upgrade Options** panel:



This allows you to choose one of three common Teamcenter configurations:



Quick preconfigured installations provide in as few as four TEM panels Teamcenter configurations that otherwise require as many as 18 panels. These simplified Teamcenter installations are designed to require minimal documentation outside the installation wizard. Help for each panel in the quick preconfigured installation process is provided from the help button .

If you want to add additional Teamcenter features during quick preconfigured installation, select the **Include additional features** check box. Later in the installation, TEM displays the **Features** panel, in which you can select features to add.

You can also add Teamcenter features *after* you complete a quick preconfigured installation using TEM in *maintenance mode*.

For advanced details about Teamcenter installation, see the Teamcenter server installation guides (for Windows and Linux) and the client installation guides (for Windows and Linux).

Choose a Teamcenter configuration to install

In this step, you choose which quick preconfigured Teamcenter configuration to install.

Option	Description
Teamcenter Rich Client 4–Tier	Installs a Teamcenter four-tier rich client to connect to an existing Teamcenter web tier.
Teamcenter Corporate Server and Server Manager	Installs a Teamcenter corporate server and a server manager to which Teamcenter clients can connect.
Teamcenter Corporate Server and Teamcenter Rich Client 2–Tier	Installs a Teamcenter corporate server with a two-tier rich client.

If you want to add additional Teamcenter features during quick preconfigured installation, select the **Include additional features** check box. Later in the installation, TEM displays the **Features** panel, in which you can select features to add.

Alternatively, you can add Teamcenter features *after* quick preconfigured installation using TEM in *maintenance mode*. After you complete quick preconfigured installation, you can launch TEM from the Windows start menu or from the **install** directory under the Teamcenter home directory. This launches TEM in maintenance mode, allowing you to add Teamcenter features and change configuration values as needed.

Teamcenter four-tier rich client

In this step, you provide information to install a four-tier rich client that connects to an existing Teamcenter middle tier and corporate server.

Value	Description
4 Tier Server URI	Specifies the URI to the rich client middle tier. Type a URI of the following form: **http://***host***:***port***/tc**
FCC Parent	Specifies the URI to the FMS server cache (FSC) used by the local FMS client cache (FCC) in your four-tier rich client configuration. Type a URI of the following form: **http://***host***:***port*

Value	Description
	For more information about configuring File Management System, see the *Teamcenter Administration* guide.
Installation Directory	Specifies the directory in which you want to install Teamcenter. Enter a directory that does *not* exist. TEM creates the directory you specify.

Note:

If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

Teamcenter corporate server and two-tier rich client

In this step, you provide information to create the Teamcenter corporate server and install a two-tier rich client.

This option also installs the Teamcenter Business Modeler IDE client to use to administer the Teamcenter corporate server.

Before you proceed, make sure you have the following values for your database server:

- Database type (Oracle or Microsoft SQL Server)
- Database name and port
- Database system user name and password

If you do not know these values, contact your database administrator.

For information about installing a database server and configuring databases for use with Teamcenter, see *Teamcenter Installation on Windows Using TEM* and the *Teamcenter Installation on Linux Using TEM* in the Teamcenter documentation.

Value	Description
OS User Password	Specifies the password for the operating system user account under which you logged on before you launched TEM. Teamcenter services run under this account. If you want to install Teamcenter under a different account, cancel this installation and restart TEM using the account you want to use.
Use License File	Specifies the location of the Teamcenter license file (**tc.lic**). If you set the **SPLM_LICENSE_SERVER** environment variable, this box contains the value specified in that variable.

Value	Description
Database Type	Specifies the database vendor for your database. Select **Oracle** or **Microsoft SQL Server**.
Host	Specifies the name of the host on which the database server runs.
Database Name/Service	Specifies the name of the database to be used by Teamcenter. For Microsoft SQL Server databases, this box is labeled **Database Name**. For Oracle databases, it is labeled **Service**. Type the name of the database or Oracle service to be used by Teamcenter. This name was defined when the database server was created.
Port	Specifies the port number used by the database server. The port number was determined when the database server was installed.
Database System User	Specifies the user name of the database system administrator account. The default value is one of the following: • Oracle databases: **system** • Microsoft SQL Server databases: **sa**
Database System Password	Specifies the password for the database system administrator account. Caution: The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab. Make sure the password does not contain space characters or any of the following characters: **! @ $ % ' " : ; . < > ( ) { }**
Database Directory	Specifies the directory in which to create the Teamcenter database on the database server. Type an appropriate location. If necessary, consult your database administrator. For Oracle servers, the database path is typically *ORACLE_HOME***oradata***Oracle_SID* (on Windows systems) or *ORACLE_HOME*/**oradata**/*Oracle_SID* (on Linux systems).

Value	Description
Character Encoding Type	Specifies by canonical name of the character encoding set Teamcenter clients use to access the database. Caution: To prevent data corruption, this character encoding set must match the encoding set used by the Teamcenter database. For more information about character encoding sets, see *Teamcenter Localization*.
Volume Directory	Specifies the path to the Teamcenter volume. A Teamcenter *volume* is a directory that stores files managed by Teamcenter. It is controlled by one, and only one, database. In this quick preconfigured installation, TEM creates the Teamcenter database and volume, and also an FMS server cache (FSC) that creates and serves default volumes. The volume can be created while installing a Teamcenter corporate server or a volume server. After installation, you can optionally create additional volumes for a database using TEM or the rich client Organization application. Note: If the specified volume directory does not have sufficient space, TEM prompts you to specify a different location.
Installation Directory	Specifies the directory in which you want to install Teamcenter. Enter a directory that does *not* exist. TEM creates the directory you specify.

Teamcenter corporate server and server manager

In this step, you provide information to create the Teamcenter corporate server and configure the server manager to which Teamcenter four-tier rich clients can connect.

This option also installs the Teamcenter two-tier rich client and the Business Modeler IDE client to use to administer the Teamcenter corporate server.

Before you proceed, make sure you have the following values for your database server:

- Database type (Oracle or Microsoft SQL Server)

- Database name and port
- Database system user name and password

If you do not know these values, contact your database administrator before you proceed.

For information about installing a database server and configuring databases for use with Teamcenter, see *Teamcenter Installation on Windows Using TEM* and the *Teamcenter Installation on Linux Using TEM* in the Teamcenter documentation.

Value	Description
OS User Password	Specifies the password for the operating system user account under which you logged on before you launched TEM. Teamcenter services run under this account. If you want to install Teamcenter under a different account, cancel this installation and restart TEM using the account you want to use.
Use License File	Specifies the location of the Teamcenter license file (**tc.lic**). If you set the **SPLM_LICENSE_SERVER** environment variable, this box contains the value specified in that variable.
Database Type	Specifies the database vendor for your database. Select **Oracle** or **Microsoft SQL Server**.
Host	Specifies the name of the host on which the database server runs.
Database Name/Service	Specifies the name of the database to be used by Teamcenter. For Microsoft SQL Server databases, this box is labeled **Database Name**. For Oracle databases, it is labeled **Service**. Type the name of the database or Oracle service to be used by Teamcenter. This name was defined when the database server was created.
Port	Specifies the port number used by the database server. The port number was determined when the database server was installed.
Database System User	Specifies the user name of the database system administrator account. The default value is one of the following: • Oracle databases: **system** • Microsoft SQL Server databases: **sa**
Database System Password	Specifies the password for the database system administrator account.

Value	Description
	Caution: The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab. Make sure the password does not contain space characters or any of the following characters: **! @ $ % ' " : ; . < > ( ) { }**
Database Directory	Specifies the directory in which to create the Teamcenter database on the database server. Type an appropriate location. If necessary, consult your database administrator. For Oracle servers, the database path is typically *ORACLE_HOME***oradata***Oracle_SID* (on Windows systems) or *ORACLE_HOME*/**oradata**/*Oracle_SID* (on Linux systems).
Character Encoding Type	Specifies by canonical name of the character encoding set Teamcenter clients use to access the database. Caution: To prevent data corruption, this character encoding set must match the encoding set used by the Teamcenter database. For more information about character encoding sets, see *Teamcenter Localization*.
Volume Directory	Specifies the path to the Teamcenter volume. A Teamcenter *volume* is a directory that stores files managed by Teamcenter. It is controlled by one, and only one, database. In this quick preconfigured installation, TEM creates the Teamcenter database and volume, and also an FMS server cache (FSC) that creates and serves default volumes. The volume can be created while installing a Teamcenter corporate server or a volume server. After installation, you can optionally create additional volumes for a database using TEM or the rich client Organization application.

Value	Description
	Note: If the specified volume directory does not have sufficient space, TEM prompts you to specify a different location.
Installation Directory	Specifies the directory in which you want to install Teamcenter. Enter a directory that does *not* exist. TEM creates the directory you specify.

8. Business Modeler IDE

Business Modeler IDE templates

In this step, you select templates to apply to your Business Modeler IDE environment. Business Modeler *templates* contain the data model for Teamcenter components. The **Teamcenter Foundation** template contains the data model used for core Teamcenter functions. Other templates extend this template.

Select the **Teamcenter Foundation** template and any other templates you want to apply.

Additional templates, such as custom templates you built, are also available to select if you placed them in the *TC_ROOT***install\software** directory before you launched TEM.

> Note:
>
> If you have custom templates that are not displayed, place those templates in the *TC_ROOT***install\software** directory. Then, click **Browse** to locate those templates and add them to the table of available templates, or re-launch TEM to load those templates automatically.

Database Configuration Change

This panel contains important information about steps you must perform to complete the Business Modeler IDE installation. Select the check box to indicate you have read this information, then click **Next** to continue.

Business Modeler IDE templates

In this step, you add templates to apply to your Business Modeler IDE environment. The *templates* contain the data model for Teamcenter solutions.

This panel shows two lists. The **Installed Templates** list displays the list of templates already installed and available for use within the Business Modeler IDE client. The **Candidate Templates** list displays the list of new templates you select to update or install.

Custom templates you built are available to select if you placed them in the *TC_ROOT***install\software** directory before you launched TEM.

> Note:
>
> If you have custom templates that are not displayed, place those templates in the *TC_ROOT***install\software** directory. Then, click **Browse** to locate those templates and add them to the table of available templates, or re-launch TEM to load those templates automatically.

Value	Description
Installed Templates	The templates installed to the server.
Candidate Templates	Templates that can be installed to the server, obtained by clicking the **Browse** button and locating the templates. Select the templates you want to install to the Business Modeler IDE.
Browse	Click this button to locate templates to install to the Business Modeler IDE. Default Teamcenter templates are located on the installation source in the **tc** directory.

Business Modeler IDE client

In this step, you select templates to install in the Business Modeler IDE.

Templates contain the data model for Teamcenter components. The **Teamcenter Foundation** template is installed by default. The Foundation template contains the data model used for core Teamcenter functions. All custom templates must extend the Foundation template.

Click **Add** to select the templates to install. Click **Remove** to remove templates from the list.

If you have custom templates or templates from a third-party to install, click **Browse** and browse to the directory where the templates are located.

To view the contents of a template, click **View**.

Note:

- Select the same templates that were installed on the server so that the Business Modeler IDE contains the same data model definitions as the server.
- If TEM displays a message that it could not find all the required templates, click **Update** to locate the missing templates.

Database Template Summary

This panel is for information only. It displays a list of templates to be applied when TEM populates the database during installation. Click **Next** to accept and continue.

Database configuration

In this step, you verify the list of templates to be applied to the database according to the features in your configuration.

If a template is shown without an associated feature, click **Browse** to locate the missing feature XML file.

Updating a database

This panel allows you to apply updated database templates when performing maintenance on your Teamcenter configuration.

The database update mode depends on the option you select under **Teamcenter Foundation** in the **Feature Maintenance** panel:

- **Update Database (Full Model)**

  Updates the database with Business Modeler IDE templates that contains all the custom data model, including schema items such as business objects and classes.

- **Update Database (Perform Live Updates)**

  Updates the database with live update templates that contain only nonschema data such as LOVs and rules.

The template list shows currently installed templates. If a template is present and is the correct version, the **Status** column displays a checkmark icon for that template.

To query the database for installed templates and refresh the list of templates, click **Refresh**.

Full model updates

To add a template to the list, or to update an existing template, click the **Browse** button to navigate to the directory where your packaged template files are located. Select the updated **feature_***template-name***.xml** file.

The **Status** column displays a refreshed status icon for templates to be refreshed.

Note:

- You can also update a template using the **tem** command line utility, for example.

  ```
  tem -update -full -templates=template-name-1,template-name-2 -path=location-of-template-files
  -pass=password
  ```

- If you are fixing a COTS template (for example, the Foundation template) using a new template file provided in a patch, you must copy the template's **feature_***template-name***.xml** and the *template-name***_install.zip** files to the same temporary directory containing the new *template-name***_template.zip** file.

For more information about packaging template files and updating database templates, see *BMIDE for Data Model Design*.

Live updates

Click the **Browse** button to navigate to the directory where your packaged template files are located. Select the updated *template-name*_**template_live_update.zip** file.

Select the template in the table to receive live updates, and then click **Next** to proceed with the update.

> Note:
>
> The system checks if the live update project is synchronized with the server. If there is data on the server that is not in the live update project, the update fails. You must synchronize the data model from the Business Modeler IDE, repackage, and attempt the update once more.
>
> If installation of the live updates fails, check the message in the TEM panel. Installation may have failed because the server you are attempting to install to does not have the **Live Update** preference set to accept live changes. In this case, you must ask the administrator of that production server to change the preference to accept the live updates.

For more information about live updates, see *BMIDE for Data Model Design*.

9. File Management System

About File Management System installation in TEM

The following TEM help topics describe panels that allow you to create and manage File Management System (FMS) volumes and services. For more information about using FMS, see the appropriate server installation guide (for Windows or) and see Teamcenter Administrationthe *Teamcenter Administration* guide.

FCC settings

In this step, you configure the installation directory for the FMS client cache (FCC) process for the locally installed rich client.

The FCC process uploads files to a file server, requests files from the file server, and caches client files.

Value	Description
Use current FCC	Select this option if you want to keep your existing FCC location.
Use new FCC	Select this option if you want to use the proposed new FCC location.

Teamcenter Environment Manager sets the **FMS_HOME** environment variable on this host to point to the selected location.

If you want to use the proposed **FMS_HOME** location but add information from the current **FMS_HOME** location on the client host, select **Merge values from existing FMS_HOME**. This results in an FCC configured to support the previous **FMS_HOME** environment as well as the one being installed.

> Note:
>
> The option to merge values from an existing **FMS_HOME** location is enabled only if your current configuration includes Teamcenter Foundation and the existing **FMS_HOME** location meets the following conditions:
>
> - Detectable
>
> The previous **FMS_HOME** location must be the current value of the **FMS_HOME** environment variable.
>
> - Accessible
>
> The installer must be able to open and read the previously installed **fcc.xml** file to extract the required information.

- Legible

  The installer must be able to parse this information using the **fccconfig.dtd** file being installed. At a minimum, it must be well-formed XML, containing no XML features absent from the installing DTD.

- Upgradable

  The existing installation must be of an equal or earlier version than that you are installing. Retrograde merges may be detected if the version attribute of the **fccconfig** element of the **fcc.xml** file is in the current **FMS_HOME** directory.

For advanced FCC configuration options, including enabling Teamcenter client communication system (TCCS), click **Advanced**.

FCC parents

In this step, you specify the FMS server caches (FSCs) used by the FMS client cache (FCC). The FCC can have multiple parent FSCs. FSCs are used in the priority you specify.

The **FSC assignment mode** box specifies how you want to assign FSCs.

To add an FSC to the list, click **Add**. TEM adds a row to the table of FSC values. Double-click the **Protocol**, **Host**, **Port**, or **Priority** boxes to enter values.

To modify a value in the table, double-click the box and enter the new value.

To remove an FSC from the table, select the row and click **Delete**.

Installing FMS server cache

In this step, you install and configure an *FMS server cache* (FSC) process that acts as either a volume server for file management or a server-level performance cache server for shared data access between multiple users:

- When you install Teamcenter on a host that physically contains or directly mounts a Teamcenter volume, you install an FSC to act as a volume server, uploading files to a Teamcenter volume and downloading files from the volume.

- When you install Teamcenter on a host where a volume is not located or directly mounted, you install an FSC to act as a performance cache server, managing two segment file caches, one for downloading files and one for uploading files.

- You also either install an FMS master configuration file on this host or identify a host in the FMS network that has an installation of this file (the master host).

The FMS master configuration file describes the FMS network and provides default configuration values for FMS server caches and client caches. When you install multiple volumes on different hosts for the same database, the multiple FSCs are linked through a common FMS master host.

References:

- For an overview of installing FMS and Teamcenter volumes, see *Teamcenter Installation on Linux Using TEM* and *Teamcenter Installation on Windows Using TEM* in the Teamcenter help library.
- For detailed descriptions of the FMS deployment options and configuration choices, see the *Teamcenter Administration* guide in the Teamcenter online documentation.

Value	Description
FSC ID	Specifies the identifier that FMS uses to identify this FSC server within the FMS network; it must be unique within the network.
Port	The port address dedicated to the FSC process. The default value is **4544**.
Enable configuration master	Specifies that you want to install the FMS master configuration file (**fmsmaster.xml**) on the local host. Tip: If you are installing only one FSC server in the network, you must select this option. Each Teamcenter network must have at least one master configuration file and one FSC designated to read this file.
FSC Parent URL	Specifies the URL to the parent FSC if the current FSC is not a master.

For advanced FSC configuration options, click **Advanced**.

FSC cache settings

In this step, you specify settings for the FSC cache.

Value	Description
Read Cache	
Directory	Specifies the path to the file system location on the local host for the read cache required when the FSC server acts as a cache server. The directory must not exist; it is created by Teamcenter Environment Manager. The default **$HOME** setting creates the read cache in the **$HOMEPATH** directory for Windows systems and in the **/tmp** directory for Linux systems.

Value	Description
	Tip: For FMS to operate correctly, the location you specify must be on the local host.
Max. Size (MB)	Specifies the size in megabytes for the read cache required when the FSC server acts as a cache server. Tip: If you are installing a volume on this host, FMS does not use the read cache; Siemens Digital Industries Software recommends accepting the default cache size (10 megabytes). Do not specify 0; specifying 0 creates a file cache with a default size larger than 10 megabytes. If you are not installing a volume on this host, FMS acts as a cache server. In this case, Siemens Digital Industries Software recommends increasing the value to 1000 megabytes.
Write Cache	
Directory	Specifies the path to the file system location on the local host for the write cache required when the FSC server acts as a cache server. The directory must not exist; it is created by Teamcenter Environment Manager. The default **$HOME** setting creates the write cache in the **Documents and Settings** directory for Windows systems and in the **/tmp** directory for Linux systems. Tip: For FMS to operate correctly, the location you specify must be on the local host.
Max. Size (MB)	Specifies the size in megabytes for the write cache required when the FSC server acts as a cache server. Tip: • If you are installing a volume on this host, FMS does not use the write cache; Siemens Digital Industries Software

Value	Description
	recommends accepting the default cache size (10 megabytes). Do not specify 0; specifying 0 creates a file cache with a default size larger than 10 megabytes. • If you are not installing a volume on this host, FMS acts as a cache server. In this case, Siemens Digital Industries Software recommends increasing the value to 512 megabytes or more.

FSC proxy settings

In this step, you specify proxy settings for the FMS server cache (FSC).

Value	Description
Enable HTTP Proxy	Specifies that this FSC server contacts other FSC servers through a proxy server in HTTP mode. Tip: Select this option only when installing other FSC processes that can be contacted only through a firewall.
Host	Specifies the name of the host running the HTTP proxy server.
Port	Specifies the number of the port the HTTP proxy server listens on.
Enable HTTPS Proxy	Specifies that this FSC server communicates with other FSC servers through a proxy server in HTTPS mode. Tip: Select this option only when installing other FSC processes that can be contacted only through a firewall.
Host	Specifies the name of the host running the HTTPS proxy server.
Port	Specifies the number of the port the HTTPS proxy server listens on.

FSC service – FCC defaults

In this step, you enter default settings FMS clients use to connect to the FSC service.

Value	Description
Windows Cache Directory	Specifies the default file system location for the FMS client cache (FCC) on all Windows-based rich client hosts. This default setting can be overridden by the FCC configuration file. Tip: Select a location that can be created locally on all Windows-based rich client hosts. The value you enter must include a reference to **$HOME** or **$USER**.
Linux Cache Directory	Specifies the default file system location for the FMS client cache (FCC) on all Linux-based rich client hosts. This default setting can be overridden by the FCC configuration file. Tip: Select a location that can be created locally on all Linux-based rich client hosts.
Max. Read Cache Size (MB)	Specifies the default maximum size in megabytes of whole files downloaded from the volume to rich client hosts. This default setting can be overridden by the FMS client cache configuration file. Tip: Select a size large enough to accommodate the largest whole file that users download from the volume.
Max. Write Cache Size (MB)	Specifies the default maximum size in megabytes of whole files uploaded to a volume from rich client hosts. This default setting can be overridden by the FMS client cache configuration file. Tip: Select a size large enough to accommodate the largest whole file that users upload to the volume.
Max. Partial Cache Size (MB)	Specifies the default maximum size in megabytes of the segment file cache used by Teamcenter lifecycle visualization and Engineering Process Management Visualization on rich client hosts.

Value	Description
	This default setting can be overridden by the FMS client cache configuration file. Tip: • If no or few rich client users in the network deploy Lifecycle Visualization, Siemens Digital Industries Software recommends setting this cache size to 10 megabytes. Do not specify 0; specifying 0 creates a file cache with a default size larger than 10 megabytes. • If rich client users in the network deploy Lifecycle Visualization, Siemens Digital Industries Software recommends setting this cache size in the range of 2000 megabytes to 4000 megabytes. The cache size is initially small, expanding to the maximum size only if a user launches Lifecycle Visualization to view a file of that size. The initial size of the cache is proportional to the value specify.

Parent FSCs are listed in the **Client Accessible External Sites** table. To add a parent FSC to the list, click **Add**. To edit or remove an existing site in the table, click **Edit** or **Remove**.

For more information about configuring File Management System, see the *Teamcenter Administration* guide.

Selecting the FSC deployment model

In this step, you choose the FMS server and volume model deployment model you want to use. Select a model from the list. Teamcenter Environment Manager displays a description of the selected model.

FSC service additional sites

In this step, you can enter information about additional sites to which the FMS server cache (FSC) service can connect.

To add a site to the list, click **Add**.

To edit or remove an existing site, click **Edit** or **Remove**.

When you run TEM in maintenance mode, you can click **Scan** to locate existing FSCs in your Teamcenter configuration.

Note:

If you have multiple FSCs, it may be useful to group them. You can add FSC groups when you run TEM in maintenance mode.

Adding an external site

In this step, you enter settings for an additional external site.

Value	Description
Site ID	Specifies the site ID for the external site.
Assignment Mode	Specifies an FSC assignment mode. The options are **clientmap** and **parentfsc**. Select **parentfsc** only if recommended by your system administrator. The default value is **clientmap**.

You can also specify an FSC assignment mode in **FSC assignment mode**. The options are **clientmap** and **parentfsc**. Select **parentfsc** only if recommended by your system administrator. The default value is **clientmap**.

To add a site to the list of external FSCs accessible from this host, click **Add**. To enter or change any value in the table of sites, double-click the box containing that value, and then type the new value.

Value	Description
Protocol	Specifies the protocol used by the FSC. The default value is **http**.
Host	Specifies the host name of the FSC.
Port	Specifies the port used by the FSC. The default value is **4544**.
Path	Specifies the path to the FSC.
Priority	Specifies the assignment priority for the FSC. The default value is **0**.
Transport	Specifies the transport mode used by the FSC. The default value is **lan**.

To remove a site from the list, click **Remove**.

For more information about configuring File Management System, see the *Teamcenter Administration* guide.

Create/Edit remote site

In this step, enter the connection information for the remote site.

Value	Description
Site ID	Provide an ID for the remote site.
FSC ID	Enter the ID of the FSC you want to assign to the remote site.
Protocol	Select the transport method to use to connect to the remote site, either **http** or **https** (HTTP secure).
Host	Enter the name of the remote site host machine.
Port	Enter the port address dedicated to the FSC process. The default is **4544**.
Priority	Enter a number to designate the priority this remote site has for processing. The default is **0**, meaning that it has the highest priority. Next would be priority **1**, followed by priority **2**, and so on.

FSC service connections

In this step, you specify ports on which the FMS server cache (FSC) service listens.

The FSC service can listen on multiple ports.

To add a port to the list, click **Add**. TEM adds a row to the table of port values. Double-click the **Port** or **Protocol** boxes to enter values.

To modify a value in the table, double-click the box and enter the new value.

To remove a port from the table, select the row and click **Delete**.

Rich client FCC parent settings

In this step, you specify settings for accessing the parent hosts of the FMS file server cache (FSC).

You can specify a FSC assignment mode in **FSC assignment mode**. The options are **clientmap** and **parentfsc**. Choose **parentfsc** only if recommended by your system administrator. The default value is **clientmap**.

Parent hosts are listed in the **FCC Parents** field. To add a parent host to the list, perform the following steps:

1. Click **Add**.

2. Double-click the **Host** box, then type the host name of the FSC.

3. Double-click the **Port** box, then type the port used by the FSC. The default value is **4444**.

4. In the **Protocol** box, type the appropriate protocol used by the FSC.

5. In the **Transport** box, type the appropriate transport mode used by the FSC. The default value is **lan**.

If you want to add access to additional hosts, repeat steps 1 through 5 to add access information for each FSC parent host.

After you add an FSC host, you can remove hosts from the list or edit settings using the **Remove** and **Edit** buttons. You can also change the priority the rich client uses in accessing FSC parent hosts by selecting a host in the table and clicking the **Up** or **Down** buttons.

For more information about configuring File Management System, see the *Teamcenter Administration* guide.

FSC service additional group sites

In this step, you can enter information about additional FMS server cache (FSC) group sites to which the FSC service can connect.

If you have multiple FSCs, it may be useful to group them. Create FSC groups from this panel when you run TEM in maintenance mode.

To add an FSC group to the list, click **Add**. TEM adds a row to the table of remote sites. Double-click the **FSC Group**, **Site ID**, **FSC ID**, **FSC Server**, or **Priority** boxes to enter values.

To modify a value in the table, double-click the box and enter the new value.

To remove a site from the table, select the row and click **Delete**.

When you run TEM in maintenance mode, you can click **Scan** to locate existing FSCs in your Teamcenter configuration.

Verifying the FSC service

In this step, the installer checks if an FSC (FMS server cache) is installed and whether it is configured as a master. If both are true, click **NEXT** to continue this maintenance activity.

FSC client map

In this step, click the **Add** button to add a new DNS (domain name system) mapping to the FMS master. When you click the **Add** button, enter values in the **Create/Edit FSC Client Map** dialog box:

Value	Description
FSC Group	Select an FSC group to assign the DNS. An FSC group is a group of server caches defined in the FMS master configuration file.
DNS Mapping	Select the type of DNS-based client map you want the FSC to use.
FSC ID	Select the FSC to which you want to map the FSC.
FSC Transport	Select **lan** (local area network) or **wan** (wide area network) as the kind of network to transport the FSC data.
Priority	Enter the priority you want to assign this DNS on the server, for example, 0,1, 2, 3, and so on.
FSC Connection	Select the type of connection to make with the FSC.

FSC groups

In this step, click the **Add** button to add FSC groups. An FSC (FMS Server Cache) group is a group of server caches defined in the File Management System (FMS) master configuration file.

FSC nonmaster settings

In this step, you enter the host, port, protocol, and priority values for the FSC master service.

FSC servers

In this step, enter the FSC servers that are accessible from this FMS master.

Value	Description
Server ID	Enter the ID you want to assign to the FSC.
Address	Specified the address of the FSC.
FSC Group	Select the FSC group that this new FSC will belong to. An FSC can only belong to one group.
Server Type	Select the type of FSC server you are creating: • **Master FSC Server**

Value	Description
	The main FSC server. • **Non-Master FSC Server** A secondary FSC server. • **External Load Balancer** A server that helps route FMS messages.
External Load Balancer	Select the external load balancer to use with this FSC server. External load balancers are external network hardware devices not supplied by Siemens Digital Industries Software, but are capable of forwarding FMS messages through network channels to other FSCs.

Specify the user account for the FSC service

In this step, you specify the user account under which the FMS server cache (FSC) service runs.

Value	Description
Local System account	Specifies you want the FSC service to run under the current local system user account (the account under which you run TEM).
This account	Specifies you want the FSC service to run under a different user account. If you choose this option, type the credentials for the account.
User	Specifies user name or the domain and user name for the account, for example, **domain\user**.
Password	Specifies the password for the designated user account.

FSC service additional group sites

In this step, you can enter information about additional FMS server cache (FSC) group sites to which the FSC service can connect.

If you have multiple FSCs, it may be useful to group them. Create FSC groups from this panel when you run TEM in maintenance mode.

To add an FSC group to the list, click **Add**. TEM adds a row to the table of remote sites. Double-click the **FSC Group**, **Site ID**, **FSC ID**, **FSC Server**, or **Priority** boxes to enter values.

To modify a value in the table, double-click the box and enter the new value.

To remove a site from the table, select the row and click **Delete**.

When you run TEM in maintenance mode, you can click **Scan** to locate existing FSCs in your Teamcenter configuration.

FSC service additional sites

In this step, you can enter information about additional sites to which the FMS server cache (FSC) service can connect.

To add a site to the list, click **Add**. TEM adds a row to the table of remote sites. Double-click the **Site ID**, **FSC ID**, or **FSC Server** boxes to enter values.

To modify a value in the table, double-click the box and enter the new value.

To remove a site from the table, select the row and click **Delete**.

When you run TEM in maintenance mode, you can click **Scan** to locate existing FSCs in your Teamcenter configuration.

Note:

- You cannot specify multiple remote FSCs using TEM. You can do this only by manually updating the master configuration (**fmsmaster.xml**) file.

  If you enter multiple FSCs in TEM, only the last-created site ID is recorded in the master configuration file. TEM does not display any message that states this.

  For more information about specifying multiple remote FSCs in the **fmsmaster.xml** file, see the *Teamcenter Administration* guide.

- If you have multiple FSCs, it may be useful to group them. You can add FSC groups when you run TEM in maintenance mode.

Create/Edit FSC client map

In this step, use DNS (domain name system) names to map an FMS client cache (FCC) to the parent FMS server cache (FSC).

Value	Description
FSC Group	Select an FSC group to assign the DNS.

Value	Description
	An FSC group is a group of server caches defined in the FMS master configuration file.
IP Subnet/Mask	Enter the Internet Protocol (IP) subnet and mask address for the DNS.
CIDR	Enter the Classless Inter-Domain Routing (CIDR) value that specifies the desired subnetted IP address in the form.
DNS Zone	Enter the DNS zone if you want to use a zone instead of subnet and mask.
DNS Hostname	Enter the DNS host name if you want to use host name instead of subnet and mask.
DNS Default	Select if you want to use the system's default DNS address. Use this whenever subnet/mask, DNS zone, or DNS host name client maps fail to map an FCC. This default attribute replaces the legacy **mask=0.0.0.0** technique previously used for subnet/mask maps.
DNS Not Defined	Select if the DNS is not defined for the system. This can be used to define an FSC map whenever a requesting FCC's IP address cannot be converted to a DNS name.
FSC ID	Enter the ID you want to assign to the FSC.
Priority	Enter the priority you want to assign this DNS on the server, for example, 0,1, 2, 3, and so on.
FSC Transport	Select **lan** (local area network) or **wan** (wide area network) as the kind of network to transport the FSC data.
FSC Connection	Select the type of connection to make with the FSC.

Create/Edit file store group

In this step, you define a file store group, which specifies volumes to be load balanced across several FSCs. You can load balance FMS data by distributing the network access load.

Select the FSC (FMS server cache) group to which the file store group belongs. Then select the FSC servers and external load balancers in the table that should have access to the file store group. Also select the priority with which each server accesses the volume.

Value	Description
Name	Enter the name you want to assign to the file store group.
FSC Group	Select an FSC group to assign to the file store group. (An FSC Group is a group of server caches defined in the FMS master configuration file.)
FSC Servers and External Load Balancers	Select the FSC servers and external load balancers that should have access to the file store group, and select the priority to define its load balancing priority (for example, 0, 1, 2, 3, and so on).

Create/Edit FSC group

In this step, you provide a name for the FSC group. An FSC (FMS server cache) group is a group of server caches defined in the File Management System (FMS) master configuration file.

Create/Edit FSC server

In this step, enter the information for the FSC server or external load balancer.

FMS caching enables placing the data close to the user, while maintaining a central file volume and database store. FMS requires the installation of FMS server cache (FSC) and FMS client cache (FCC) components. The FSC component provides a server process and file caches for Teamcenter server hosts. (The FCC component provides a client process and file caches for rich clients on user workstations.)

Value	Description
FSC ID	Enter the ID you want to assign to the FSC.
FSC Group	Select the FSC group that this new FSC will belong to. An FSC can only belong to one group.
Host	Enter the name of the host machine where the FSC will reside.
Server Type	Select the type of FSC server you are creating: • **Master FSC Server** The main FSC server. • **Non-Master FSC Server** A secondary FSC server. • **External Load Balancer** A server that helps route FMS messages.

Value	Description
External Load Balancer	Select the external load balancer to use with this FSC server. External load balancers are external network hardware devices not supplied by Siemens Digital Industries Software, but are capable of forwarding FMS messages through network channels to other FSCs.
Protocol	The transport method, either **http** or **https** (http secure).
Port	The port address dedicated to the FSC process.
Add	Click to add a port for the server to use. By default the **http** protocol is assigned port **4544**, and the **https** protocol is assigned port **4545**. To change the port, click in the **port** cell.
Delete	Click to remove a protocol and port.

File store group

In this step, you assign volumes to file store groups. A file store group specifies volumes to be load balanced across several FSCs. Grouping volumes into file store groups is not required, but it is useful when creating a failover FMS master.

Value	Description
Add	Click the **Add** button and enter the name of the file store group. Then click the arrow in the **FSC Group** box to select the FSC group to which the file store belongs. Select the FSC servers and external load balancers in the table that can access to the file store group. Also select the priority with which each server accesses the volume.
Edit	Make changes to the file store group.
Delete	Remove a file store group.

Scan for sites

Select the sites to which this FSC should have access.

Value	Description
Import	Specifies whether the site is imported.
Site ID	Specifies the ID for the FSC site.
FSC ID	Specifies the ID for the FSC (FMS Server cache).

Value	Description
FSC Server	Specifies the server where the FMS process runs.
Priority	Specifies the priority that this site has for processing, for example, 0,1, 2, 3, and so on.

Assign to FSC group

In this step, you select the FSC group to assign to the servers. An FSC group is a group of server caches defined in the FMS master configuration file. All FSCs must belong to one, and only one, FSC group.

Volume query

In this step, you search for available volumes in the FMS master file. Volumes can be assigned to an FSC server, to an external load balancer, or to a file store group.

Value	Description
Assign	Click this button to assign a volume to an FSC server, to an external load balancer, or to a file store group. Choose these options on the **Assign Volume** dialog box: • **Assign to FSC Server or External Load Balancer** Select to assign the volume to an FSC server (a machine where FMS processes run) or an external load balancer (a machine designated to take some of the load of FMS processes). • **Assign to File Store Group** Select to assign the volume to a file store group, which specifies volumes to be load balanced across several FSCs.
Delete	Click this button to delete the selected volume from the table.
Scan	Click this button to query the database for a current list of volumes. Any new volumes will be added to the list, and any information on existing volumes will be updated.

FSC security

In this step, you specify whether to enable HTTPS access and also specify the HTTPS access port.

Create/edit remote group site

In this step, enter the connection information for the remote site.

Value	Description
FSC Group	Select an FSC group from the list.
Site ID	Provide an ID for the remote site.
FSC ID	Enter the ID of the FSC you want to assign to the remote site.
Protocol	Select the transport method to use to connect to the remote site, either **http** or **https** (HTTP secure).
Host	Enter the name of the remote site host machine.
Port	Enter the port address dedicated to the FSC process. The default is **4544**.
Priority	Enter a number to designate the priority this remote site has for processing. The default is **0**, meaning that it has the highest priority. Next would be priority **1**, followed by priority **2**, and so on.

Cloud DSS volume settings

In this step, you specify settings for the cloud volume.

In addition to standard network storage of volumes, File Management System (FMS) supports S3 cloud volumes through the Cloud Data Storage Service (DSS). DSS lets you create volumes that are stored on Amazon S3 cloud-based servers. Configuration and use of S3 cloud storage is currently supported with Siemens Managed Services accounts only.

Value	Description
Enable Cloud Data Storage Service (DSS)	Enables the Cloud Data Storage Service.
Keystore Password	Specifies a password to protect the keystore file containing the Cloud Data Storage Service credentials.
Account ID	Specifies the ID of the Cloud Data Storage Service account that stores Teamcenter volumes.
User ID	Specifies the user ID for the Cloud Data Storage Service account that stores Teamcenter volumes.

Value	Description
Access Key ID	Specifies the ID of the key used to access Teamcenter volumes stored in the Cloud Data Storage Service account.
Secret Access Key	Specifies the secret string of the key used to access Teamcenter volumes stored in Cloud Data Storage Service account.

10. Teamcenter client communication system

About Teamcenter client communication system configuration in TEM

The following TEM help topics describe panels for installing and configuring Teamcenter client communication system (TCCS).

For more information about installing and configuring TCCS, see the appropriate server installation guide (for Windows or Linux).

For more information about managing TCCS environments, see the *Teamcenter Administration* guide.

Teamcenter client communication system (TCCS) switch

In this step, you choose whether to enable TCCS in your Teamcenter installation. TCCS provides client support for proxy environments and centralized configuration capabilities.

Select the **Use Configurations and Environments** check box to use TCCS configurations.

For more information about managing TCCS environments, see the *Teamcenter Administration* guide.

TCCS environment settings

In this step, you specify environment settings for Teamcenter client communication system (TCCS) environments.

A single TCCS configuration can contain multiple environments, providing support for multiple versions or server databases. For example, you may want to install some TCCS environments with Security Services (SSO), some environments without SSO, some environments on one server, and other environments on another server.

If multiple environments are configured, all environments are displayed at rich client logon, allowing the user to select which TCCS environment to use.

To add an environment to the table of TCCS environments, click **Add**. This adds a row to the table. Double-click a box in the new row to type a value. For each environment, type the following values.

Value	Description
Name	Specifies a name for the TCCS environment.
URI	Specifies a URI for the TCCS environment, for example: **http://myhost:8080/tc**
Tag	(Optional) Specifies a tag for the environment that can be used to filter the list of TCCS environments during rich client logon. When installing a rich client, you can optionally provide a **Client Tag Filter** value to filter the list of environments displayed in the rich client to those environments that match the filter. Example: You create 10 environments, three on **Server1** with Security Services, three on **Server1** without Security Services, and four on **Server2**. Tag the environments **SSO**, **no SSO**, and **Server2**, respectively.
SSO App ID	Specifies a Security Services (SSO) application ID. Type an application ID if you want to add a Security Services environment to your TCCS environment.
SSO Login URL	Specifies the logon URL to the Security Services environment. Note: • You must set up the Security Services environment before you configure TCCS. For example, in the **SSO App ID** box, type the value of the **SSO_APPLICATION_ID** context parameter from the web tier installation. In the **SSO Login URL** box, type the value of the **SSO_LOGIN_SERVICE_URL** context parameter. • If you use Security Services in applet-free mode, append **/tccs** to the end of **SSO Login URL** value, for example: **http://***host***:***port***/***logon-service-name***/tccs**

To remove a configuration from the table, select the appropriate row and click **Remove**.

> Note:
>
> If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.
>
> For more information about managing TCCS environments, see the *Teamcenter Administration* guide.

TCCS forward proxy settings

In this step, you define forward proxy settings for Teamcenter client communication system (TCCS).

Value	Description
Do not use forward proxy	Specifies that you do not want to use a forward proxy.
Use web browser settings	Specifies that you want to obtain proxy settings from your web browser.
Detect settings from network	Specifies that you want to obtain proxy settings from your local network.
Retrieve settings from URL	Specifies that you want to obtain settings from a specified URL.
Proxy URL	Specifies the URL to the web server from which you want to obtain proxy settings. This value must be a valid URL for a forward proxy autoconfiguration file.
Configure settings manually	Specifies that you want to enter proxy settings manually.
All protocols host	Specifies a name of a valid proxy to use for all protocols. In the accompanying **Port** box, type the port used by the proxy host.
HTTP Host	Specifies the host of a forward proxy server for the HTTP protocol. In the accompanying **Port** box, type the port used by the proxy host.
HTTPS Host	Specifies the host of a forward proxy server for the HTTPS protocol. In the accompanying **Port** box, type the port used by the proxy host.
Exceptions	Specifies a semicolon-delimited list of host names and IP addresses to exempt. This box is optional.

For more information about managing TCCS environments, see the *Teamcenter Administration* guide.

Note:

If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

TCCS reverse proxy settings

In this step, you specify reverse proxy settings for Teamcenter client communication system (TCCS) on this client host. Teamcenter uses these settings to detect a logon web page from a reverse proxy server through which Teamcenter services are accessed.

Reverse proxy configuration is optional.

The criteria table lists the reverse proxy criteria currently defined. Each row of the table is a criteria XML element defined in the specified format. By default, the table is blank and no criteria are defined. A criterion string is of the following form:

Header_Name1, *Header_Value1*, *Header_Name2*, *Header_Value2*,...:*Form_Action*

Each criterion must contain at least one header name/header value pair or at least a single form action.

To add a criterion to the table, perform the following steps:

1. Click **Add**.
2. In the **Criteria Details** table, add or remove HTTP header names and values for the selected criterion using the **Add** and **Remove** buttons.
3. In the **Form Action** box, specify a form action.
4. Click **Apply**.

   The criterion is added to the criteria table.

TCCS validates reverse proxy criteria. If you do *not* want TCCS to perform this validation, select the **Skip reverse proxy criteria check** check box. If you select this check box, every response that has an HTTP status of **200** and a content-type of **text/html** is interpreted as a form-based authentication challenge, which triggers an interaction with Security Services. If your reverse proxy is not configured for form-based authentication challenges, do *not* select this check box.

Note:

- If you must connect to a Teamcenter environment through a reverse proxy server (such as WebSEAL or SiteMinder), you may need to configure reverse proxy settings for TCCS.

- If you use SiteMinder, you must configure TCCS to detect form-based challenges originating from the reverse proxy by adding the following criterion to the **Private Reverse Proxy Settings** table.

Header name	Header value
checkHeaders	**false**

  This setting also applies to other reverse proxy servers that do not send specific header information in the 200 form-based challenge.

- If you use WebSEAL and you deploy the TCCS configuration, add the following criterion to the **Private Reverse Proxy Settings** table.

Header name	Header value	Form action
server	**webseal**	**/pkmslogin.form**

  This is required because the settings in the deployed **reverseproxy_cfg.xml** override the default WebSEAL configuration.

  If you do *not* deploy the TCCS configuration, TCCS uses the default WebSEAL configuration, so this manual configuration is not required.

- Criteria definitions are written to the **reverseproxy_cfg.xml** file.

Configuration selection for TCCS

In this step, you choose whether to modify the shared or private Teamcenter client communication system (TCCS) configuration.

If you are a TCCS administrator, select **Shared** if you want this configuration to be used by multiple users, or select **Private** if this configuration is for your use only. By default, the shared configuration is used by the system for all users connecting using TCCS.

If you are not a TCCS administrator, you can only create a **Private** configuration for your use only.

A TCCS administrator can create both shared and private configurations. A non-TCCS administrator can only create a private configuration. If both private and shared configurations exist for a user (designated as **existing** in the configuration panel in TEM), the private configuration takes precedence.

For more information about managing TCCS environments, see the *Teamcenter Administration* guide.

Configuring multiple TCCS environments

In this step, you specify environment settings for Teamcenter client communication system (TCCS) environments.

A single TCCS configuration can contain multiple environments, providing support for multiple versions or server databases. For example, you may want to install some TCCS environments with Security Services (SSO), some environments without SSO, some environments on one server, and other environments on another server.

If multiple environments are configured, all environments are displayed at rich client logon, allowing the user to select which TCCS environment to use.

To add an environment to the table of TCCS environments, click **Add**. This adds a row to the table. Double-click a box in the new row to type a value. For each environment, type the following values.

Value	Description
Name	Specifies a name for the TCCS environment.
URI/TC_DATA	Specifies a location for the TCCS environment. • For four-tier connections: Enter a URI for the TCCS environment, for example: **http://myhost:8080/tc** • For two-tier connections: Enter the path to the data directory (**TC_DATA**) where you want TEM to create shared data subdirectories and files.[1]
Tag	(Optional) Specifies a tag for the environment that can be used to filter the list of TCCS environments during rich client logon. When installing a rich client, you can optionally provide a **Client Tag Filter** value to filter the list of environments displayed in the rich client to those environments that match the filter.

1 This can be the network path to the **TC_DATA** directory on your corporate server.

Value	Description
	Example: You create 10 environments, three on **Server1** with Security Services, three on **Server1** without Security Services, and four on **Server2**. Tag the environments **SSO**, **no SSO**, and **Server2**, respectively.
SSO App ID	Specifies a Security Services (SSO) application ID. Type an application ID if you want to add a Security Services environment to your TCCS environment.
SSO Login URL	Specifies the logon URL to the Security Services environment. Note: You must set up the Security Services environment before you configure TCCS. For example, in the **SSO App ID** box, type the value of the **SSO_APPLICATION_ID** context parameter from the web tier installation. In the **SSO Login URL** box, type the value of the **SSO_LOGIN_SERVICE_URL** context parameter.
Single Server	Specifies whether to force all client sessions for the given user to use the same **tcserver** process. If set to **true**, all client sessions use the same **tcserver**. Setting it to **false** allows clients to control sharing of **tcserver** processes.

To remove a configuration from the table, select the appropriate row and click **Remove**.

Note:

If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

For more information about managing TCCS environments, see the *Teamcenter Administration* guide.

TCCS settings for two-tier rich client

In this step, you specify environment settings for Teamcenter client communication system (TCCS) environments for the two-tier rich client.

A single TCCS configuration can contain multiple environments, providing support for multiple versions or server databases. For example, you may want to install some TCCS environments with Security Services (SSO), some environments without SSO, some environments on one server, and other environments on another server.

If multiple environments are configured, all environments are displayed at rich client logon, allowing the user to select which TCCS environment to use.

To add an environment to the table of TCCS environments, click **Add**, then type the following values for the environment.

Value	Description
Name	Specifies a name for the TCCS environment.
TC_DATA	Enter the path to the data directory (**TC_DATA**) where you want Teamcenter Environment Manager to create shared data subdirectories and files.[2]
Tag	(Optional) Specifies a tag for the environment that can be used to filter the list of TCCS environments during rich client logon. In the **Client Tag Filter** panel during rich client installation, you can optionally provide a pattern to filter the list of environments displayed in the rich client to those environments that match the pattern. Example: You create 10 environments, three on **Server1** with Security Services, three on **Server1** without Security Services, and four on **Server2**. Tag the environments **SSO**, **no SSO**, and **Server2**, respectively.
SSO App ID	Specifies a Security Services (SSO) application ID. Type an application ID if you want to add a Security Services environment to your TCCS environment.

2 This can be the network path to the **TC_DATA** directory on your corporate server.

Value	Description
SSO Login URL	Specifies the logon URL to the Security Services environment. Note: You must set up the Security Services environment before you configure TCCS. For example, in the **SSO App ID** box, type the value of the **SSO_APPLICATION_ID** context parameter from the web tier installation. In the **SSO Login URL** box, type the value of the **SSO_LOGIN_SERVICE_URL** context parameter.
TcServer Character Encoding Canonical Name	Specifies the canonical name of the character encoding set Teamcenter clients use to access the database. Caution: To prevent data corruption, this character encoding set must match the encoding set used by the Teamcenter database.
Single Server	Specifies whether to force all client sessions for the given user to use the same **tcserver** process. If set to **true**, all client sessions use the same **tcserver**. Setting it to **false** allows clients to control sharing of **tcserver** processes.

To remove a configuration from the table, select the appropriate row and click **Remove**.

Note:

If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

For more information about managing TCCS environments, see the *Teamcenter Administration* guide.

Forward proxy settings for TCCS

In this step, you define forward proxy settings for Teamcenter client communication system (TCCS).

Value	Description
Do not use forward proxy	Specifies that you do not use a forward proxy.
Use web browser settings	Specifies that you want to obtain proxy settings from your web browser. Select this option if your users are required to use their web browser settings to point to the proxy server. Selecting this option automatically retrieves the proxy settings from the client's web browser.
Detect settings from network	Specifies that you want to obtain proxy settings from your local network. Select this option if you use a web proxy auto-discovery protocol (WPAD) to point to the proxy server. With WPAD, clients automatically locate a URL of a configuration file using the dynamic host configuration protocol (DHCP) or the domain name system (DNS).
Retrieve settings from URL	Specifies that you want to obtain settings from a specified URL. Select this option if you use a proxy autoconfiguration (PAC) file to point to the proxy server.
Proxy URL	Specifies the URL to the forward proxy autoconfiguration (PAC) file from which you obtain proxy settings.
Configure settings manually	Specifies you do not use automatic methods to point to the proxy server and want to configure proxy server settings manually.
All protocols host	Specifies you use the same proxy server all forward and reverse proxy requests. Type the host name or IP address of the server in the **All Protocols Host** box, and type the server port number in the **Port** box.
HTTP Protocols	Specifies you have separate proxy servers dedicated to HTTP and HTTPS requests.
HTTP Host	Specifies you have an HTTP proxy server to use. Select this check box, and then type the host name in the **HTTP Host** box and the HTTP proxy host port number in the **Port** box.

Value	Description
HTTPS Host	Specifies you have an HTTPS proxy server to use. Select this check box, and then type the host name in the **HTTPS Host** box and the HTTPS proxy host port number in the **Port** box.
Exceptions	Specifies a semicolon-delimited list of host names and IP addresses that are not proxied. For example, **localhost; my_tc; 182** exempts **http://localhost:8017/tc**, **https://my_tc:14327/tc**, and **http://182.0.0.27:8080/tc**. This box is optional.

For more information about managing TCCS environments, see the *Teamcenter Administration* guide.

> Note:
>
> If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

TCCS client tag filter

In this step, you optionally specify a pattern on which to filter Teamcenter client communication system (TCCS) environments available to the rich client.

In the **Client Tag Filter** box, type a pattern to apply when filtering TCCS environments. Wildcard characters (*****) are allowed.

The **Client Tag Filter** pattern is compared to the **Tag** parameters on defined TCCS environments. Environments that do not fit the pattern are not available to the rich client. For example, If the rich client **Client Tag Filter** value is **9.***, all TCCS environments with **Tag** values beginning with **9.** are available to the rich client. Environments with**Tag** values beginning with **10** are not available.

For more information about managing TCCS environments, see the *Teamcenter Administration* guide.

TCCS configuration selection

In this step, you choose whether to modify the shared or private Teamcenter client communication system (TCCS) configuration.

If both the shared and the private TCCS configurations exist, the private configuration takes precedence. If both shared and private TCCS configurations exist, modifying the shared configuration may have no effect on clients because the private configuration takes precedence. Shared configurations may be edited only by administrators.

For more information about managing TCCS environments, see the *Teamcenter Administration* guide.

Removing a TCCS configuration

In this step, you can remove Teamcenter client communication system (TCCS) configurations.

A TCCS configuration contains information on how TCCS connects to the server. A TCCS configuration can be either shared or private. Whether a TCCS configuration is shared or private is determined at installation time. Shared configurations can be created only by administrators.

Select the **Shared** or **Private** check boxes to remove shared or private TCCS configurations.

> Note:
>
> A shared TCCS configuration is located in the **%ALLUSERSPROFILE%/Siemens/cfg** directory (Windows systems) or the **/etc/Siemens/cfg** (Linux systems). A private TCCS configuration is located in the **%USERHOME%** directory.

Kerberos authentication settings

In this step, you specify settings for Kerberos authentication in Teamcenter.

Kerberos is a network authentication protocol that uses a system of *tickets* to allow nodes communicating over nonsecure networks to securely verify identities of each side. Using a client-server model, it provides mutual authentication: the user and the server verify each other's identities.

Value	Description
Support Kerberos authentication	Specifies you want to use Kerberos authentication for Teamcenter logon.
Always prompt for user ID	Specifies you want to always prompt for a Kerberos user name. If you want to enable zero sign-on functionality on Windows hosts, clear this check box. *Zero sign-on* allows Windows users to launch a Teamcenter client without being prompted to log on to Teamcenter. Note: Zero sign-on functionality requires you configure Security Services in applet-free mode in the **Security Services** panel.

Value	Description
	For more information about configuring Security Services, see *Security Services Configuration*.

Single sign-on functionality requires you configure Security Services in the **Security Services** panel.

For more information about configuring Security Services, see *Security Services Configuration*.

Secure socket layer (SSL) settings

In this step, you specify settings for secure socket layer (SSL) authentication in Teamcenter.

Value	Description
Use Microsoft Windows Certificate Store (Recommended)	Specifies you want to use certificates stored in Microsoft Windows. This option is available only on Windows hosts.
Disable SSL	Specifies you want to disable SSL authentication.
Configure Certificate Store Manually	Specifies you want to manually configure the certificate store for Teamcenter.
Configure trust store	Contains options for manually configuring the certificate store for Teamcenter.
Use trust store	Specifies you want to use a trust store. If you select this option, enter the path to file that contains the trust store you want to use.
Accept untrusted certificates	Specifies you want to accept untrusted certificates.
Configure key store	Contains options for configuring the keystore for Teamcenter.
Use key store	Specifies you want to use a keystore. If you select this option, enter the path to the keystore. Also, specify the file type. The default file type is **JKS**.

For more information about configuring SSL for Teamcenter, see *Security Services Configuration*.

11. Web tier

About web tier installation in TEM

The following TEM help topics describe panels that install the server manager and enable the web tier to communicate with the Teamcenter server.

For more information about using installing the Teamcenter web tier, see the appropriate server installation guide (for Windows or Linux).

Java EE web tier

Setting default web server preferences

In this step, you optionally define a web tier application server that enables rich client users to generate and view bookmark files that interact with Teamcenter lifecycle visualization.

Requirements:

A Teamcenter web tier application must be generated and deployed.

References:

For information about configuring the web tier application, see *Teamcenter Installation on Windows Using TEM* and *Teamcenter Installation on Linux Using TEM* in the Teamcenter help library.

Value	Description
Set the preferences	Specifies whether to set the specified preferences in the Teamcenter configuration.
Host	Specifies the name of the server where the web tier application is deployed. The host name can be a physical host name, alias, fully-qualified domain name (FQDN), or IP address.
Port	Specifies the number of the port for the web tier application.
Application Name	Specifies the name of the web tier application. The default name of the web tier application is **tc**.

Note:

- If you use SSL, make sure you include the fully qualified domain name of the host in the URL to the web application.
- If your network uses IPv6 (128-bit) addresses, use the host name in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

.NET web tier

Internet Information Services (IIS) settings

In this step, you provide Internet Information Services (IIS) settings for Teamcenter web tier deployment.

Value	Description
IIS Web Site Configuration	
Use Existing Web Site	Specifies that you want to use an existing web site. You must select the existing web site from the list. Teamcenter creates the virtual directory for the Teamcenter application in the specified web site in IIS. The Teamcenter application is thus hosted in the specified web site. This option is selected by default.
Create New Web Site	(Optional) Specifies that you want to create a new web site for the Teamcenter web tier deployment. You must specify values for **Web Site Name**, **Web Site Port**, and **Web Site Root Path**.
Web Site Name	(Optional) Specifies the name of the new web site in IIS. This value is required only if you select the **Create New Web Site** option.
Web Site Port	(Optional) Specifies the port number of the new web Site in IIS. This port must be available and unassigned. This value is required only if you select the **Create New Web Site** option.
Web Site Root Path	(Optional) Specifies the root of web content subdirectories for the new web site. This value is required only if you select the **Create New Web Site** option.
IIS Web Application Pool Configuration	
Use Existing Application Pool	Specifies whether to use an existing application pool from the list provided. An application pool is a set of one or more applications assigned to an IIS worker process. The Teamcenter .NET web tier is an ASP.NET 2.0 application, so the application pool can only host other ASP.NET 2.0 applications (not other versions of ASP.NET, such as 1.1). Keep this in mind if you intend to have this application pool host other applications.

Value	Description
	A general recommendation is to use a dedicated (stand-alone) application pool for Teamcenter web tier deployment. This option is selected by default.
Create New Application Pool	(Optional) Specifies whether to create a new application pool. You must provide a value for **Application Pool Name**.
Application Pool Name	(Optional) Specifies the name for the IIS application pool. This value is required only if you select the **Create New Application Pool** option.
IIS Virtual Directory Configuration	
Virtual Directory Name	Specifies the IIS virtual directory name for Teamcenter web tier deployment. The default value is **tc**. Web URLs for Teamcenter four-tier deployments are based on this value. For example, if you specify the default value as **tc**, the URLs are of the form: **http://***host***:***port***/tc/...**

Note:

If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

.NET web tier

In this step, you set the initial configuration values for installing the .NET web tier in a four-tier Teamcenter deployment.

Note:

This step applies only when you are deploying the four-tier architecture.

Value	Description
Web Tier Language	Specifies the same locale that is specified for Teamcenter server. This locale is used for localization of messages coming from the web tier. The default web tier language is English. Choose one of the following languages: Chinese (Simplified) Chinese (Traditional) Czech English French German Hebrew Italian

Value	Description
	Japanese Korean Polish Portuguese (Brazilian) Russian Spanish
Server Managers	Specifies each server manager host and port for your Teamcenter installation. At least one server manager must be configured for a working deployment, so you must specify at least one host and value. **Host** specifies the machine name where the server manager is running, and **Port** specifies the port on which the server manager listens. This port must match the port you specify during the corresponding server manager installation.
Pool ID	Specifies the ID of the server pool to which the given server pool is assigned.

For additional web tier configuration options, click **Advanced**.

> Note:
>
> If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

.NET web tier advanced settings

In this step, you specify advanced settings for the .NET web tier in a four-tier Teamcenter deployment.

Value	Description
Session Time Out	Specifies the web tier session time out in minutes. The default value is **20**. If a user is inactive for more than the time-out value, the user's web tier session expires. In the rich client, client credentials are cached. After a session time-out, the rich client automatically logs on silently and allows the user to continue working.
Response Compression Threshold	Specifies the threshold in number of bytes beyond which the web server should compress responses sent back to the client. Typically, compressing smaller responses does not yield significant compression, so all responses equal to or less than the value specified are sent to the client uncompressed.

Value	Description
	Note: Setting this value to **0** causes the server to compress every response sent to the client. The default value is **500** bytes.
Client Cache Time Out	Specifies the time, in minutes, to retain the client cache. Cached files are deleted after the specified interval.
TcSS Enabled	(Optional) Specifies whether to enable Security Services. If Security Services is enabled, you must provide valid values for **TcSS Application ID** and **TcSS Service URL**. The default value is **false**.
TcSS Application ID	(Optional) Specifies the application ID of your Teamcenter installation as configured in the Security Services installation.
TcSS Login Service URL	(Optional) Specifies the URL to the Security Services Login Service web application.
Critical System Events Notification	(Optional) Specifies whether to notify the administrator of critical system events. If selected, you must provide values for **Administrator Email** and **SMTP Host**. If selected, certain error level log messages are e-mailed to the specified e-mail address. These error messages usually signify a serious operational or functional problem in the deployment and typically require manual intervention to be correct. These messages are also logged on the Windows event log. If you do not specify e-mail notification, you can view messages in the Windows event log.
Administrator Email	(Optional) Specifies the administrator's e-mail address for critical system events notification.
SMTP Host	(Optional) Specifies the SMTP (Simple Mail Transfer Protocol) Host to send e-mail for critical system events notification.
Cluster Deployment	(Optional) Select this option if you have a clustered web Tier deployment using the ASP.NET state service as the out-of-process state server. If selected, you must specify values for **ASP.NET State Service Host** and **ASP.NET State Service Port**. Select this option only if you use a web farm (clustered web tier) deployment *and* you want to use the ASP.NET State Service as your out-of-process state server. If you plan to use any other out-of-process state server, such as SQL*Server, do not select this option. The Teamcenter installer supports only the ASP.NET State Service as the out-of-process state server; other state servers may be configured manually after the initial Teamcenter installation is complete.
State Server Host	(Optional) Specifies the ASP.NET state service host name for session state management.

Value	Description
State Server Port	(Optional) Specifies the ASP.NET state service port number for session state management.
Legacy URL Support	(Optional) Select this option if you want to provide basic URL redirection to support legacy URLs from earlier versions of Teamcenter. This option automatically redirects legacy URLs to current Teamcenter URLs with no informational messages.
X509Certificate	Specifies the location the X.509 certificate for the .NET web tier.

.NET web tier client integration

In this step, you set the optional configuration values for .NET web tier client integration.

Value	Description
Session Time Out	(Optional) Specifies the time, in minutes, to allow an inactive client session to remain open.
Use Hybrid Authentication	(Optional) Specified whether to use hybrid authentication for Microsoft Applications. If this is set to **false**, users must enter a name and password in Microsoft applications even if they have logged on through Teamcenter applications. Set this value to **true** to avoid the extra authentication challenges from Microsoft applications. The default value is **true**.
Use AIWS	Specifies whether to use the application interface web service (AIWS) for integration with Remote Workflow.
User Name	(Optional) Specifies the user name for logging on to Teamcenter on behalf of the remote Teamcenter application. The default value is **infodba**.
User Password	(Optional) Specifies the user password for logging on to Teamcenter on behalf of the remote Teamcenter application. This value is encrypted.

Caution:

Never use the **infodba** user to create working data or initiate workflow processes. The **infodba** user is to be used *only* for certain tasks during Teamcenter installation. Using this account to create data or initiate workflow processes can cause unexpected and undesirable behaviors.

If you require a user with high-level privileges to create data, create a new user and grant database administrator privileges to that user.

ASP .NET state service configuration

In this step, you set initial configuration values for the ASP .NET state service for the Teamcenter .NET web tier. You can use the ASP .NET state service to configure the .NET web tier in clustered mode for network load balancing.

> Note:
>
> This step applies only when you are deploying the four-tier architecture.

Value	Description
ASP .NET State Service Host	Specifies the host on which the ASP .NET state service runs.
ASP .NET State Service Port	Specifies the port used by the ASP .NET state service.

12. Security Services

Configuring Security Services

In this step, you configure Security Services for Teamcenter. These services eliminate prompts for logon credentials when users launch multiple Teamcenter products within a single user session. Authentication is performed by an external identity service provider, such as lightweight directory access protocol (LDAP), instead of the Teamcenter product.

Prerequisite:

Installation and configuration of Security Services.

For information, see *Security Services Configuration* in the Teamcenter help library.

> Note:
>
> Make sure the Security Services web applications are installed and running. TEM verifies the connection to Security Services and does not allow you to continue from this panel if the connection fails.
>
> Installation of Security Services using the Web Application Manager is described in the appropriate server installation guide (for Windows or Linux).

Value	Description
Login URL	Specifies the complete URL of the Security Services Login Service web application.
Service URL	Specifies the complete URL of the Security Services Identity Service web application.
Application ID	Specifies the application ID for this instance of Teamcenter in the Security Services application registry.
Administrative User	Specifies the user name of the Teamcenter administrative user account.
Password	Specifies the password for the Teamcenter administrative user account.
Disable database authentication	Specifies whether to disable authentication to the Teamcenter database by Security Services. By default, this checkbox is cleared. Siemens Digital Industries Software recommends selecting this checkbox because disabling database authentication prevents a malicious program from bypassing Security Services and logging into Teamcenter using a stale password in the Teamcenter database.

Value	Description
	Note: If you disable both Teamcenter database authentication *and* Security Services (SSO) variables, no users can log on. To avoid this, make sure that Security Services (SSO) variables are *not* disabled when Teamcenter database authentication is disabled.

Note:

If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

Configuring Security Services during maintenance

In this step, you configure Security Services during Teamcenter maintenance. Security Services eliminates prompts for logon credentials when users launch multiple Teamcenter products within a single user session. Authentication is performed by an external identity service provider, such as lightweight directory access protocol (LDAP), instead of the Teamcenter product.

Note:

This option applies only when you are deploying the two-tier architecture.

When you deploy the four-tier architecture, you configure Security Services in the web tier application. For information, see *Teamcenter Installation on Linux Using TEM* or *Teamcenter Installation on Windows Using TEM*.

Prerequisite:

Installation and configuration of Security Services.

For information, see *Security Services Configuration* in the Teamcenter help library.

Note:

Make sure the Security Services web applications are installed and running. TEM verifies the connection to Security Services and does not allow you to continue from this panel if the connection fails.

Installation of Security Services using the Web Application Manager is described in the appropriate server installation guide (for Windows or Linux).

Value	Description
Login URL	Specifies the complete URL of the Security Services Login Service web application.
Service URL	Specifies the complete URL of the Security Services Identity Service web application.
Application ID	Specifies the application ID for this instance of Teamcenter in the Security Services application registry.
Disable database authentication	Specifies whether to disable authentication to the Teamcenter database by Security Services. By default, this checkbox is cleared. Siemens Digital Industries Software recommends selecting this checkbox because disabling database authentication prevents a malicious program from bypassing Security Services and logging into Teamcenter using a stale password in the Teamcenter database.

Note:

If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

Configuring Security Services for rich client

In this step, you provide information required to enable Security Services in the rich client.

Note:

If you use Security Services in the Teamcenter web tier application, you must configure Security Services using the Web Application Manager as described in the appropriate server installation guide (for Windows or Linux).

Prerequisite:

Installation and configuration of Security Services.

For information, see *Security Services Configuration* in the Teamcenter help library.

Value	Description
Login URL	Specifies the complete URL of the Security Services Login Service web application.
Application ID	Specifies the application ID for this instance of the rich client in the Security Services application registry.

Value	Description
	An application is represented within Security Services as a unique text string known as an application ID. You must define an application ID for each Teamcenter application in your Security Services domain. You use these application IDs when completing the Application Registry table.

Note:

If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

Configuring Security Services for the rich client

In this step, you configure Security Services for use with Teamcenter.

Value	Description
Login URL	Specifies the complete URL of the Security Services Login Service web application. If you use Security Services in applet-free mode, type the URL using the following format: **http://***host***:***port***/***login-service-name***/tccs**
Application ID	Specifies the application ID for this instance of Teamcenter in the Security Services application registry.

For more information about configuring Security Services, see *Security Services Configuration*.

Note:

If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

Key Manager Configuration

In this step, you optionally enable Key Manager for use with Teamcenter.

Prerequisite: Install Key Manager using Deployment Center.

Teamcenter Key Manager is an optionally-installed feature that enables you to manage, edit, and share encryption keys and policies in a centralized secure manner for a distributed Teamcenter site.

The *key manager server* stores all policies and keys on a single host, accessed over secure HTTPS. A *key manager satellite* resides on each enterprise tier host, and accesses the key manager server over HTTPS.

To enable Key Manager, select the **Enable Key Manager** check box.

In the **Satellite Location** box, enter the path to a key storage location on the local host.

To proceed with Teamcenter installation without configuring Key Manager, clear the **Enable Key Manager** checkbox.

For more information about Key Manager, see the *System Administration* guide in the Teamcenter documentation.

13. Server manager

Server manager database configuration

In this step, you configure a database for the server manager cluster.

In the **Database Server** box, select your database vendor (**Oracle** or **Microsoft SQL Server**).

Enter the following database configuration values, depending on the database vendor you select.

Oracle database server values

Value	Description
Host	Specifies the name of the host on which the Oracle server runs. This host must exist, and the Oracle server must be installed.
Service	Specifies the name of the service for the Oracle instance. The service name was determined when the Oracle server was installed.
Port	Specifies the number of the port on which the Oracle server listens. The port number was determined when the Oracle server was installed.
User	Specifies a database user name: • To connect to an existing database configured for use with Teamcenter, enter the name defined for a database user when the database was configured. • To create and configure a database for use with Teamcenter, enter the name of the database user you want to create.
Password	Specifies a database password: • To connect to an existing database configured for use with Teamcenter, enter the password defined for the database user when the database was configured. • To configure a new database for use with Teamcenter, enter a password for the database user you are creating.

If you chose **Create user and database** in the **Server Manager Cluster Configuration** panel, provide the following values:

Value	Description
System User	Specifies a user name of the Oracle system administrator account. The default value is **system**.
Password	Specifies a password for the Oracle system administrator account. Caution: The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab. In addition, the password must not contain any of the following characters: **! # @ $ % = & ' " ^ : ; . _ < > ( ) { }**
Database Path	Specifies the location of the tablespaces for the Teamcenter database on the Oracle server. This is typically *ORACLE_HOME***oradata***Oracle_SID* (on Windows systems) or *ORACLE_HOME*/**oradata**/*Oracle_SID* (on Linux systems). Note: The **Database Path** must exist and you must have write permission to the directory.
Enable TCPS	If you want to use secured communication with the database using secure TCP (TCPS), select the **Enable TCPS** check box, and then enter the following values. If you do not select this check box, Teamcenter uses TCP by default.
Wallet Location	Specifies the location of the secure wallet that stores CA certificates. This is the Oracle **auto_login** wallet configured on the file system. The user under which the deployer is triggered should have read access to this folder.
SSL Version	Specifies the installed TLS version.

Microsoft SQL Server values

Value	Description
Instance	If you connect to Microsoft SQL Server using a named instance, select this option and enter the instance name you defined when you installed MS SQL Server.
Port	If you connect to Microsoft SQL Server using a specific port, select this option and enter the port number you specified when you installed MS SQL Server.
Login Name	Specifies a database user name: • To connect to an existing database configured for use with Teamcenter, enter the name defined for a database user when the database was configured. • To create and configure a new database for use with Teamcenter, enter the name of the database user you want to create.
Login Password	Specifies the password for the database user: • To connect to an existing database configured for use with Teamcenter, enter the password defined for the database user when the database was configured. • To configure a new database for use with Teamcenter, enter a password for the database user you are creating.
Database Name	Specifies the name of the MS SQL Server database. The database name was determined when database was created.

If you chose to create a new database instead of using an existing database, provide the following values:

System User	Specifies the user name of the SQL Server system administrator account. The default value is **sa**.
Password	Specifies the password for the SQL Server system administrator account.

> Caution:
>
> The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab.
>
> In addition, the password must not contain any of the following characters:

Value	Description
	! # @ $ % = & ' " ^ : ; . _ < > ( ) { }
Database Path	Specifies the directory in which to create the Teamcenter database on the SQL Server server.
Collation	Specifies the collation used by the Teamcenter database on the Microsoft SQL Server server. *Collation* defines the alphabet or language whose rules are applied when data is sorted or compared.
Enable UTF-8	Specifies whether to enable support for UTF-8 encoding in the Teamcenter database. Microsoft SQL Server does not provide native support for UTF-8. The **Enable UTF-8** option enables the Teamcenter server to convert character encoding to and from UTF-8 when interacting with the database. For information about configuring your Teamcenter host to support UTF-8, see the Teamcenter installation guides for Windows and Linux.
Data Directory	Specifies the path to the Teamcenter data (*TC_DATA*) directory. This value is stored in the **TC_DATA** variable in your Teamcenter configuration. TEM creates shared data subdirectories and files in this location. Each data directory is associated with a single database user within a database instance. Note: Do not create a **TC_DATA** variable in the system environment. TEM sets this variable as required in Teamcenter scripts. Setting this variable in the operating system causes conflicts if you install more than one configuration.

Server manager cluster configuration

In this step, you specify the user name and password for the database system user for the server manager database.

Value	Description
User	Specifies the user name for the database system user account.
Password	Specifies the password for the database system user account.

Configuring the server manager cluster

In this step, you enter settings for the server manager cluster.

In the **Cluster ID** box, type a name for the server manager cluster.

To balance the sessions load among multiple server managers, each server manager must have the same **Cluster ID** (that is, use the same server manager database). The **Cluster ID** value is stored in the **MANAGER_CLUSTER_ID** property in the *TC_ROOT***pool_manager\serverPool***database-name**.properties** file.

Choose one of the following options:

- **Create user and database**

  Choose this option to create a new database user and database for the server manager. You must be prepared to enter database system credentials when TEM prompts you.

- **Use existing user and database**

  Choose this option if you want to use an existing database user and database for the server manager. Your database administrator must create the database user and database before you proceed.

JMX configuration for Teamcenter Management Console

In this step, you add server components to view in the Teamcenter Management Console.

To add a server component, click **Add**. This adds a row to the **Server Components** table. For each component you add, enter the following values.

Value	Description
Type	Select either **Server Manager** or **Web Tier**.
ID	Type the ID of the component. For example, type **PoolA** for the default server manager pool or **Teamcenter1** for the default web tier. Tip: Obtain the server manager pool name from the **smgrPoolId** value in the *TC_ROOT***install\configuration.xml** file. Obtain the web tier ID from the Web Application Manager used to create the web tier application.

Value	Description
Host	Type the host name of the machine running the server.
JMX RMI Port	Type the JMX RMI port number for the server. For example, type **8088** for the default server manager port or **8089** for the default web tier port.

To remove a component from the **Server Components** table, select the row and click **Remove**.

> Note:
>
> If you add a **Web Tier** server component, you must configure your web application server to allow remote JMX connection with LDAP authentication. Each web application server (for example, JBoss, Tomcat, and WebSphere) require different steps to allow remote JMX connection.

For more information about installing the Teamcenter Management Console, see the *Teamcenter Administration* guide in the Teamcenter documentation.

Configure secure communication for Teamcenter Management Console

In this step, you specify communication settings for the Teamcenter Management Console.

First, specify whether you want to use SSL by checking or clearing the **Enable SSL** check box.

- SSL not enabled:

  In the **Http port** box, type the port you want the Teamcenter Management Console to use. The default port is **8083**.

- SSL enabled:

  Enter the following values:

Value	Description
Https Port	Type the port to be used for HTTPS communication.
KeyStore	Type the full path and file name to the keystore file.
KeyStore Type	Type the file extension for the keystore.
KeyStore Password	Type the password to the keystore.
KeyManager Password	Type the manager password to the keystore.

For more information about installing the Teamcenter Management Console, see the *Teamcenter Administration* guide in the Teamcenter documentation.

Teamcenter Management Console LDAP Configuration

In this step, you specify LDAP configuration settings for the Teamcenter Management Console.

Value	Description
Use Embedded LDAP	Specifies whether to use lightweight directory access protocol (LDAP) to facilitate authentication and authorization. Only one embedded LDAP comes with the Teamcenter Management Console. There is no support for multiple embedded LDAP servers. If you select this option, enter the following **Protocol** and **Port** values.
Protocol	Select the type of security protocol: **ldap** or **ldaps** (secure LDAP).
Port	Type the port used by the LDAP instance to listen for connections. The default value is **15389**.
KeyStore	Type the path to the KeyStore for the LDAP server. KeyStores store private keys for SSL secured services and also trusted certificates of certification authorities (CA).
KeyStore Password	Type the password for the KeyStore for the LDAP server.
Use External LDAP	Specifies whether to use an existing LDAP server. Multiple external LDAP servers are supported for failover purposes. To support failover, these multiple LDAP servers must have similar LDAP configurations. If you select this option, enter the following values.

Value	Description
Protocol	Select the type of security protocol: **ldap**, **ldaps** (secure ldap), or **tls** (transport layer security).
Host	Type the name where the stand-alone LDAP server resides.
Port	Type the port used by the LDAP instance to listen for connections.
Partition	Type the unique name of the LDAP partition.
Users	Type the name for the list of users to receive LDAP permission. The default value is **ou=Users**.
User Object Class	Type the class for the users to receive LDAP permission. The default value is **inetOrgPerson**.
User Attribute	Type the attribute that users must have to receive LDAP permission.
Administrator DN	Type the distinguished name (DN) of the LDAP administrator, the LDAP user who has search and read permissions in the LDAP directory service.
Administrator Password	Type the password for the LDAP administrator.
User Filter	Type the LDAP-formatted filter to narrow the pool of authorized users. Use the following format: **(***attribute1***=***value1***)** **(***attributeN***=***valueN***)**

For more information about installing the Teamcenter Management Console, see the *Teamcenter Administration* guide in the Teamcenter documentation.

LDAP configuration for server manager

In this step, you specify LDAP configuration settings for the server manager.

Value	Description
Use Embedded LDAP	Specifies whether to use lightweight directory access protocol (LDAP) to facilitate authentication and authorization. Only one embedded LDAP comes with the Teamcenter Management Console. There is no support for multiple embedded LDAP servers. If you select this option, enter the following **Protocol** and **Port** values.
Protocol	Select the type of security protocol: **ldap** or **ldaps** (secure LDAP).
Port	Type the port used by the LDAP instance to listen for connections. The default value is **15389**.
Use External LDAP	Specifies whether to use an existing LDAP server. Multiple external LDAP servers are supported for failover purposes. To support failover, these multiple LDAP servers must have similar LDAP configurations. If you select this option, enter the following values.
Protocol	Select the type of security protocol: **ldap**, **ldaps** (secure LDAP), or **tls** (transport layer security).
Host	Type the name where the stand-alone LDAP server resides.
Port	Type the port used by the LDAP instance to listen for connections.
Partition	Type the unique name of the LDAP partition.
Users	Type the name for the list of users to receive LDAP permission. The default value is **ou=Users**.
User Object Class	Type the class for the users to receive LDAP permission. The default value is **inetOrgPerson**.

Value	Description
User Attribute	Type the attribute that users must have to receive LDAP permission.
User Filter	Type the LDAP-formatted filter to narrow the pool of authorized users. Use the following format: **(***attribute1***=***value1***)** **(***attributeN***=***valueN***)**

Installing the server manager

In this step, you configure settings for the server manager, which manages a pool of Teamcenter server processes running in the enterprise tier. The server manager starts and times out the server processes.

> Note:
>
> This option applies only when you are deploying the four-tier architecture.
>
> For small deployments, install the server manager on the host running the web tier application in a Java application server.
>
> For larger deployments, you can install the server manager on multiple hosts. In this case, the pool of server processes is distributed as subpools across the hosts, with a server manager for each subpool.

References:

- For an overview of the four-tier architecture components and instructions for installing and deploying the web tier application, see the Teamcenter installation guides for Windows and Linux.
- For information about configuring and administering the server manager, see the *Teamcenter Administration* guide.

These documents are available in the Teamcenter documentation library.

> Note:
>
> Record each value you set for the server manager: for some values, you must provide the identical value when configuring the web tier application; for other values, you must coordinate the values in the web tier application.

Value	Description
Pool ID	Specifies a unique ID for this pool of server processes.
JMX RMI Port	Specifies the number of the port running the Java Management Extension (JMX) HTTP adaptor. The JMX HTTP adaptor enables viewing the status of the server pool and dynamically altering the pool configuration values. Tip: Record this port number. Administrators require the port number to access the adaptor at a URL (composed of the server manager host name and this port number).
Assignment Service Port	Specifies the port number used by the server manager assignment service.
Server Host	Specifies the logical host name of the server manager host. This value allows you to control which IP address is used when connecting to Teamcenter servers. If your server manager host has only one IP address, leave this field blank. If the server host has multiple IP addresses and you want the server manager to use a specific address when connecting to Teamcenter servers, type the address or the logical host name of the server manager host. The value you enter is written to the **SERVER_HOST** parameter in the **serverPool.properties** file.
Max Servers in Sub-Pool	Specifies the maximum number of Teamcenter server processes allowed to run in this pool (for a single-host configuration) or in this subpool (for a multihost configuration).
Min Warm Servers	Specifies the minimum number of Teamcenter server processes in this pool that are started but not logged onto. Tip: If necessary to maintain the minimum number of warm servers, while not exceeding the maximum number of server processes, the server manager times out servers in use.
Server Target	Specifies the target number of server processes to be available in this pool or subpool during specified times. Specify these values as time and integer pairs separated by commas. For example:

Value	Description
	0700 3, 1700 2 This value sets the target number of server processes as 3 between 7:00 a.m. and 5:00 p.m. and as 2 between 5:00 p.m. and 7:00 a.m. • If the number of server processes is below the specified target, warm servers are added to reach this number. In this case, the number of warm servers exceeds the minimum. • If the number of server processes exceeds the specified target, only the minimum number of warm servers is maintained and servers are terminated as they time out.
Logins per Minute	Specifies the number of logons the server manager allows per minute for this pool or subpool. Tip: Setting this value to **0** allows an unlimited number of logons.
Startup Mode	Specifies how you want to start the server manager
Service/Daemon	Specifies you want to run the server manager as a service (a system service on Windows or a daemon on Linux).
Command Line	Specifies you want to run the server manager manually from a command line.

For additional configuration options, click **Advanced**.

Note:

- The server manager log file contains status messages recorded during server manager startup. See the information in this file if you encounter web tier connection problems.
- On Linux systems, if you install the server manager using an account without root privileges, a user with root privileges must run the root postinstallation tasks script to register the server manager daemon.

  After you complete server manager installation in TEM, locate and run the following script:

  TC_ROOT/**install/root_post_tasks_***id*.**ksh**

Server manager timeout settings

In this step, you specify timeout settings for the Teamcenter server manager.

After installation, you can further configure timeout settings using the Teamcenter Management Console as described in *Teamcenter Administration*.

The **TcServer** processes can be configured for *idle timeouts*, when an assigned **TcServer** instance does not receive any requests from the client application(s). An assigned **TcServer** instance can be in one of three modes, and client applications connected to the **TcServer** instance will change the mode based on the type of work that is currently being performed. These modes should help you determine how long to set the idle timeout values:

STATELESS This is the default mode of a **TcServer** process and indicates that no persistent data is cached in memory. The only cost of timing out a **TcServer** in **STATELESS** mode is the cost of a server assignment and authentication when the client does become active again. The Active Workspace client makes up the majority of **STATELESS** sessions.

READ The **READ** mode is used when a timeout would cause a performance or functional issue but not loss of unsaved edits. The cost of timing out a **TcServer** in **READ** mode, is the time the user has to spend to get back to the state he was in before. The rich client and NX client make up the majority of **READ** sessions.

EDIT The **EDIT** mode indicates there are unsaved edits. Those changes will be lost if the **TcServer** is timed out. The rich client and NX client make up the majority of **EDIT** sessions.

The server manager allows timeouts to be configured with different values to be used when the total number of **TcServer** instances is below or above the **PROCESS_TARGET** value. The total number of **TcServer** is both the assigned **TcServer** session, and the warm **TcServer** waiting to be assigned.

The following configuration values in TEM define the idle timeout when below the **PROCESS_TARGET** value.

Value	Description
Hard Timeout Edit	Specifies the idle timeout, in seconds, when the **TcServer** is in **EDIT** mode and the number of **TcServer** instances is below the **PROCESS_TARGET** value. The client may apply this mode to the server when pending updates to server data are not yet committed to the database. If the timeout interval is reached, the changes are lost, regardless of the status of the server.
Hard Timeout Read	Specifies the idle timeout, in seconds, when the **TcServer** is in **READ** mode and the number of **TcServer** instances is below the **PROCESS_TARGET** value. The client may apply this mode to the server when the client's requests have set a temporary state in the server

Value	Description
	to be used by subsequent requests. If the timeout interval is reached, the read is cancelled, regardless of the state of the server.
Hard Timeout Stateless	Specifies the idle timeout, in seconds, when the **TcServer** is in **STATELESS** mode and the number of **TcServer** instances is below the **PROCESS_TARGET** value.. The client may apply this mode to the server when no requests depend on the state that a previous request has made to the server. If the server is lost, the next request can be executed on a new server without functional issues except for the performance of assigning a new server. This action is performed regardless of the state of the server.
Soft Timeout Edit	Specifies the idle timeout, in seconds, when the **TcServer** is in **EDIT** mode and the number of **TcServer** instances is above the **PROCESS_TARGET** value. The client may apply this mode to the server when pending updates to server data are not yet committed to the database. If the timeout interval is reached and the number of servers in a server pool exceeds the specified **PROCESS_TARGET** parameter, the changes are lost.
Soft Timeout Read	Specifies the idle timeout, in seconds, when the **TcServer** is in **READ** mode and the number of **TcServer** instances is above the **PROCESS_TARGET** value. The client may apply this mode to the server when the client's requests have set a temporary state in the server to be used by subsequent requests. If the timeout interval is reached and the number of servers in a server pool exceeds the specified **PROCESS_TARGET** parameter, the read is cancelled.
Soft Timeout Stateless	Specifies the idle timeout, in seconds, when the **TcServer** is in **STATELESS** mode and the number of **TcServer** instances is above the **PROCESS_TARGET** value. The client may apply this mode to the server when no requests depend on the state that a previous request has made to the server. If the server is lost, the next request can be executed on a new server without functional issues except for the performance of assigning a new server. This action is performed if the number of servers in a server pool exceeds the specified **PROCESS_TARGET** parameter.

The server manager will switch from hard timeouts to soft timeouts when the number of **TcServer** instances exceeds the **PROCESS_TARGET** value. The timeout values are incrementally reduced until the

total **TcServer** process count reaches 110% of the **PROCESS_TARGET** value, at which point the timeout values will be the soft values. While the server manager dynamically adjusts the timeout values based on the **TcServer** load, the timeout values will never be longer than the hard limits, so these are enforced regardless of load.

As the total count of **TcServer** instances approaches the **PROCESS_MAX** value, the timeout values are further reduced. This incremental reduction starts at 95% of the **PROCESS_MAX** value and brings the idle timeouts to 20% of the soft values.

The server manager logs messages for automated changes in idle timeout values, and when a **TcServer** times out. Each **TcServer** instance also records in the syslog changes to the idle timeouts and when the **TcServer** times out.

Uninstalling the server manager database

In this step, you choose whether to leave the server manager database on the database server when you uninstall the server manager.

Value	Description
Keep server Manager database	Specifies you want leave the server manager database on the database server.
Drop server Manager database	Specifies you want to remove the server manager database from the database server.

14. Dispatcher

About Dispatcher installation in TEM

The following TEM help topics describe panels that allow you to install and configure the optional Dispatcher feature for Teamcenter. For more information about installing Dispatcher, see Dispatcher — Deployment and Administration.

For information about translators for the Dispatcher server, see *Enable default translators*.

Installing Dispatcher

In this step, you install the optional Dispatcher feature, an integration of the Dispatcher Server and Teamcenter. Dispatcher enables Teamcenter users to translate CAD data files that are managed by Teamcenter to JT or CGM file format for viewing in either Engineering Process Management Visualization or Teamcenter lifecycle visualization.

Prerequisites:

- Install and configure the Dispatcher Server.
- Install, configure, and verify translators.

Postinstallation task:

Manually create an Access Manager rule that permits the Dispatcher proxy user to update attributes of a **TranslationRequest** object. If you fail to create this rule, the Dispatcher service reports errors.

```
Condition = Has Class
Value = DispatcherRequest
ACL Name = DispatcherRequest
ACE Type of Accessor = User
ACE ID of Accessor = DC-proxy-user-id
ACE Privilege = Write
ACE Privilege Value = Grant
ACE Privilege = Delete
ACE Privilege Value = Grant
```

References:

For information about installing Dispatcher Server, see *Dispatcher — Deployment and Administration* in the Teamcenter help library.

Value	Description
Translation Service Proxy User Name	Specifies the name of the Teamcenter user that logs in for Dispatcher services (the *ETS proxy user*). Tip: Siemens Digital Industries Software recommends that the Dispatcher proxy user not be the same as the Teamcenter user as the proxy user requires a unique access rule.
Translation Service Proxy Password	Specifies the password for the Dispatcher proxy user.
TSTK Scheduler Host	Specifies the name of the host on which the Dispatcher Server scheduler is deployed. This host name is added to the translation server URL: **rmi://***host-name***:***port-number*
TSTK Scheduler Port	Specifies the number of the port used by the Dispatcher Server scheduler. This port number is added to the translation server URL: **rmi://***host-name***:***port-number*
NX UG Manager Support	Specifies whether this installation of Dispatcher supports Teamcenter Integration for NX or NX Integration.
Service Registry Hostname	Specifies the name of the host where the Dispatcher service registry runs. When deploying the two-tier architecture, this can be the local host.
Service Registry Port	Specifies the number of the port used by the Dispatcher service registry.
Translation Service TCServer Hostname	Specifies the name of the host on which the Dispatcher service **tcserver** runs.
Extractor Port	Specifies the number of the port used by the Dispatcher extractor service. This port is used to control this Dispatcher service.
Scheduler Port	Specifies the number of the port used by the Dispatcher scheduler service. This port is used to control this Dispatcher service.
Loader Port	Specifies the number of the port used by the Dispatcher loader service. This port is used to control this Dispatcher service.
Specify Dataset Owner	Specifies the owner of the datasets submitted for translation. The default value is **CAD**.

Entering Dispatcher user credentials

In this step, you supply user credentials for the Dispatcher user account.

Value	Description
User	Specifies the user ID for the Dispatcher user account.
Password	Specifies the password for the Dispatcher user account.

Installing Dispatcher components

In this step, you specify settings for Dispatcher installation.

Value	Description
Dispatcher Root directory	Specifies the root directory of the Dispatcher installation. Siemens Digital Industries Software recommends specifying the Dispatcher root directory as close to the Teamcenter root directory as possible.
SCHEDULER	
Install Scheduler	Select this check box to install the Dispatcher scheduler.
Scheduler Port	Specifies the port for the translation scheduler.
MODULE	
Install Module	Select this check box to install the Dispatcher module.
Staging Directory	Specifies the default staging directory for translations. Note: If you are installing the module and the scheduler on the same machine, the **Module Port** box is disabled.
Module Port	Specifies the port for the translation module.
ADMIN CLIENT	
Install Admin Client	Select this option to install the Dispatcher administrative client.

Dispatcher settings

In this step, you specify installation settings for Dispatcher.

Value	Description
Enter Logging Level	Enter the level of messages you want Dispatcher to record. Select one of the following levels: • **OFF** • **FATAL** • **ERROR** • **WARN** • **INFO** • **DEBUG** • **TRACE** • **DBCHG** • **ALL** The default level is **INFO**.
Dispatcher Services Log Directory	Specifies a directory for the Dispatcher service log.
Install Documentation	Specifies whether to install documentation (JavaDoc) for the Translation Service. If you select this check box, specify a location in which to install the documentation in the **Documentation Install Directory** box.
Run Dispatcher As:	Options for how to run Dispatcher services.
Windows Service	Specifies you want to run Dispatcher services as Windows services. These services can be managed through the **Services** dialog box in the Windows Control Panel.
Console Application	Specifies you want to launch Dispatcher services in a console window.
Start Dispatcher	Select this check box to automatically start Dispatcher services.

Dispatcher translation service settings

In this step, you specify settings for the translation service.

Value	Description
Dispatcher Server Hostname	Specifies the name of the server where the translation server will be hosted.
Dispatcher Server Port	Specifies the port to be used for the translation service. The default value is **2001**. Make sure that the port you type is not used by any other process.

Value	Description
Staging Directory	Specifies the location to be used as the staging directory for the translation service.
Dispatcher Client Proxy User Name	Specifies the name of the proxy user who will use translation services.
Dispatcher Client Proxy Password	Specifies the password for the proxy user. Enter the password again in the **Translation Service Proxy Confirm Password** box.
Polling interval in seconds	Specifies the time, in seconds, that the translation service waits before querying for translation requests.
Do you want to store JT files in Source Volume?	Specifies whether to store visualization files in the associated visualization dataset. Choose **Yes** or **No**.

Dispatcher translation service (additional settings)

In this step, you specify additional settings for the translation service.

Value	Description
Enter Logging Level	Enter the level of messages you want Dispatcher to record. Select one of the following levels: • **OFF** • **FATAL** • **ERROR** • **WARN** • **INFO** • **DEBUG** • **TRACE** • **DBCHG** • **ALL** The default level is **INFO**.
Advanced Settings	
Do you want to update existing visualization data?	Specifies whether the Translation Service should update existing visualization data for subsequent translations of the same version. Choose **Yes** or **No**.
Deletion of successful translation in minutes	Specifies the number of minutes the translation service waits before querying and deleting successful translation request objects. If the this value is **0**, no translation request cleanup is done.

Value	Description
Threshold time in minutes for successful translation deletion	Specifies the number of minutes to allow after the last modification of a successful translation request before the request can be deleted.
Deletion of unsuccessful translation in minutes	Specifies the number of minutes the translation service waits before querying and deleting unsuccessful translation request objects. If the this value is **0**, no translation request cleanup is done.
Threshold time in minutes for unsuccessful translation deletion	Specifies the number of minutes to allow after the last modification of an unsuccessful translation request before the request can be deleted.

Selecting translators

In this step, you select translators to install on the Dispatcher server.

For information about translators, see *Dispatcher — Deployment and Administration*.

Translator settings

In this step, you specify settings for translators used by the Dispatcher server. The settings required vary by the applications associated with each translator. For more information about translators, see *Dispatcher Server Installation*.

15. Teamcenter Reporting and Analytics

About Reporting and Analytics installation in TEM

You install the Teamcenter integration to Teamcenter Reporting and Analytics using TEM. Reporting and Analytics requires additional steps to complete configuration.

For more information, see the appropriate server installation guide (for Windows or Linux) and also the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

Reporting and Analytics install options and general settings

In this step, you configure installation options for the Reporting and Analytics integration.

Reporting and Analytics is a stand-alone reporting application. Reporting and Analytics adds a **Reporting and Analytics Reports** folder to Report Builder, which contains reports created with Reporting and Analytics. You can view, edit, set permissions and delete Reporting and Analytics reports from Report Builder. Viewing reports launches Reporting and Analytics. Reporting and Analytics also adds menu commands to My Teamcenter to generate Reporting and Analytics reports.

Value	Description
Create license server	Specifies whether you want to install a Reporting and Analytics license server.
Create WAR file	Specifies whether to generate a WAR file for the Reporting and Analytics web application.
Create metadata	Specifies whether to populate the Reporting and Analytics metadata database. Select this only during the first installation of Reporting and Analytics. If you are upgrading from a previous version of Reporting and Analytics or adding additional hosts, do not select this option.
Secure Connection	Specifies whether to use a secure connection (HTTPS) when connecting to the Reporting and Analytics license server.

> Note:
>
> Reporting and Analytics requires additional steps to complete configuration. For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

Reporting and Analytics license server settings

In this step, you specify settings for the Reporting and Analytics license server.

Value	Description
License File Path	Specifies the location of the Reporting and Analytics license file (**license.dat**).
Keystore Settings	
Override Keystore Default Input	Specifies whether to allow the license server to use its default keystore and password.
Keystore Path	Specifies the path to the keystore for Reporting and Analytics licenses. Specifies the path to the keystore file that contains the public and private key used for encryption and decryption in HTTPS communication.
Keystore Password	Specifies the password to be used for encryption and decryption in HTTPS communication.

Note:

- For information about starting the Reporting and Analytics license server, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.
- Reporting and Analytics requires additional steps to complete configuration.

  For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

Reporting and Analytics WAR file settings

In this step, you specify the web application context, host, and port for the Reporting and Analytics integration web application.

Value	Description
Web Application Context	Specifies the application name for the Reporting and Analytics web application. The default value is **eQube**. This name is included in the URL for the web application.
Web Application Server Name	Specifies the name of the server where the Reporting and Analytics web application is deployed.
Web Application Server Port	Specifies the port number used by the Reporting and Analytics web application.

The complete URL to the Reporting and Analytics web application is of the following form:

http://*host-name***:***port***/***context-name***/***rest-of-path*

For example, a web application named **TcRA** running on a host named **MyHost** using port **7001** uses the following URL:

http://MyHost:7001/TcRA/BuildNPlay

Note:

Reporting and Analytics requires additional steps to complete configuration.

For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

Reporting and Analytics license settings

In this step, you configure the local host to provide license authorizations for the Reporting and Analytics integration.

Reporting and Analytics is a stand-alone reporting application. Reporting and Analytics adds a **TcRA Reports** folder to Report Builder, which contains reports created with Reporting and Analytics. You can view, edit, set permissions and delete Reporting and Analytics reports from Report Builder. Viewing reports launches Reporting and Analytics. Reporting and Analytics also adds menu commands to My Teamcenter to generate Reporting and Analytics reports.

Value	Description
License Server Host	Specifies the host on which the Reporting and Analytics license server runs.
License Server Port	Specifies the port used by the Reporting and Analytics license server.
License Authentication Timeout	Specifies the interval in seconds to wait for a response from the Reporting and Analytics license server.

Note:

- For information about starting the Reporting and Analytics license server, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.
- Reporting and Analytics requires additional steps to complete configuration.

  For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

Reporting and Analytics metadata settings

In this step, you specify metadata settings for the Reporting and Analytics integration.

This panel is displayed only if you select **Create metadata** in the **Reporting and Analytics install options and general settings** panel.

Value	Description
Teamcenter 4–tier URL	Specifies the URL to the Teamcenter four-tier rich client (**http://***host***:***port***/***context-root*).
Teamcenter User	Specifies the user name for the Teamcenter user who administers Reporting and Analytics.
Teamcenter Password	Specifies the password for the Teamcenter user who administers Reporting and Analytics.
Teamcenter Group Name	Specifies the group name for the Teamcenter user who administers Reporting and Analytics.
Teamcenter Role Name	Specifies the role name for the Teamcenter user who administers Reporting and Analytics.
Connection ID	Specifies a connection ID of one or more alphanumeric characters to use when connecting to the Reporting and Analytics server.
Connection Name	Specifies a name for the Reporting and Analytics, for example, **TcConnection**.
Teamcenter Version	Specifies the version of Teamcenter for which you installed Reporting and Analytics.

Note:

- Reporting and Analytics requires additional steps to complete configuration.

  For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

- If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

Reporting and Analytics database selection

In this step, you configure database settings for the Reporting and Analytics integration.

Reporting and Analytics is a stand-alone reporting application. Reporting and Analytics adds a **Reporting and Analytics Reports** folder to Report Builder, which contains reports created with Reporting and Analytics. You can view, edit, set permissions, and delete Reporting and Analytics reports from Report Builder. Viewing reports launches Reporting and Analytics. Reporting and Analytics also adds menu commands to My Teamcenter to generate Reporting and Analytics reports.

Prerequisites:

- A database server must be installed. Teamcenter supports Oracle and MS SQL Server databases.
- A database instance must exist, either a specific instance configured for Teamcenter or a multipurpose instance to be configured in this step.
- A database user for Reporting and Analytics must be configured on the database server.

References:

For information about installing a database server and configuring databases for use with Teamcenter, see *Teamcenter Installation on Linux Using TEM* and *Teamcenter Installation on Windows Using TEM* available in the Teamcenter help library.

In the **Database Engine** box, select the database engine you use (**Oracle** or **Microsoft SQL Server 2005**).

Enter the following database configuration values, depending on the database engine you select:

Oracle database server values

Value	Description
Database Server	Specifies the name of the host on which Oracle Server runs. This host must exist, and Oracle Server must be installed.
Service	Specifies the name of the service for the Oracle instance. The service name was determined when the Oracle server was installed.
Port	Specifies the number of the port on which Oracle Server listens. The port number was determined when Oracle Server was installed.
Database User	Specifies the Reporting and Analytics database user name. The database user must exist and be configured for use with Teamcenter.
Database Password	Specifies the password for Reporting and Analytics database user.

Microsoft SQL Server values

Value	Description
Database Server	Specifies the name of the host on which MS SQL Server runs. This host must exist, and MS SQL Server must be installed.

Choose one of the following methods to connect to the database:

Value	Description
Named Instance	If you connect to Microsoft SQL Server using a named instance, select this option and enter the instance name you defined when you installed MS SQL Server.
Port	If you connect to Microsoft SQL Server using a specific port, select this option and enter the port number you specified when you installed MS SQL Server.
Login Name	Specifies the Reporting and Analytics database user name. The database user must exist and be configured for use with Teamcenter.
Login Password	Specifies the password for the Reporting and Analytics database user.
Database Name	Specifies the name of the MS SQL Server database. The database name was assigned when database was created.

Note:

Reporting and Analytics requires additional steps to complete configuration.

For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

Reporting and Analytics WAR and metadata settings

In this step, you specify WAR file and metadata settings for the Reporting and Analytics integration.

Value	Description
Metadata Owner	Specifies the user name for the owner of Reporting and Analytics metadata. By default, this is the database user name you specified in the **Reporting and Analytics Database Selection** panel.
Web Application Server	Specifies the vendor of the web application server on which you deploy Reporting and Analytics.
Use localization	Select this check box to enable localization in Reporting and Analytics.
Master Locale	Specifies the master locale. This locale determines the primary language used for data input on the server.
Preferred Locales	Specifies one or more additional preferred locales.

Note:

Reporting and Analytics requires additional steps to complete configuration.

For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

Reporting and Analytics authentication settings

In this step, you specify the authentication method and related settings for the Reporting and Analytics integration.

Value	Description
Authentication Type	
eQube Authentication	Specifies eQube authentication.
SSO Authentication	Specifies Teamcenter Security Services authentication.
Windows (NTLM) Authentication	Specifies Windows NT LAN Manager (NTLM) authentication.
Network Properties	
Domain Name	Specifies the name of the NTLM domain.
Computer Account Name	Specifies the account name of the NTLM domain controller.
Computer Account Password	Specifies the password of the NTLM domain controller.

Note:

- Selecting **SSO Authentication** requires that you install Teamcenter with Security Services enabled and configure the LDAP server before you install Reporting and Analytics.

  For information about installing Security Services, see *Security Services Configuration*.

- Reporting and Analytics requires additional steps to complete configuration.

  For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

Reporting and Analytics WAR SMTP settings

In this step, you specify SMTP settings to enable users to receive e-mail generated by Reporting and Analytics.

Value	Description
SMTP Host	Specifies the host name of the SMTP server host.
Authenticate	Specifies whether to require authentication on the SMTP server.
User Name	Specifies the user name of the Reporting and Analytics e-mail account.
Password	Specifies the password for the Reporting and Analytics e-mail account.
Include Administrator(s) Email	Specifies you want to send notifications to the Reporting and Analytics administrator.
Administrator(s) Email ID	Specifies the email account ID of the Reporting and Analytics administrator.

Note:

Reporting and Analytics requires additional steps to complete configuration.

For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

Reporting and Analytics metadata SSO settings

In this step, you specify metadata settings for Security Services with the Reporting and Analytics integration.

Value	Description
Teamcenter Application Identifier	Specifies the identifier of the Teamcenter web tier application. Security Services uses this identifier for logon authorizations in Reporting and Analytics.

Note:

Reporting and Analytics requires additional steps to complete configuration.

For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

Reporting and Analytics WAR SSO settings

In this step, you specify WAR file settings for Reporting and Analytics with Security Services.

Value	Description
TcRA Application Identifier	Specifies the application identifier for the Reporting and Analytics web application.
SSO Scheduler Application Identifier	Specifies the ID of scheduler application.
Mediator Password	For information about mediating applications, see *Security Services Configuration* in the Teamcenter documentation. Specifies the Security Services mediator password.
Identity Service URL	Specifies URL to the Security Services Identity Service.
Login Service URL	Specifies the URL to the Security Services Login Service.

Note:

- Reporting and Analytics requires additional steps to complete configuration.

  For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

- If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

Reporting and Analytics Security Services configuration

In this step, you specify configuration settings for Reporting and Analytics with Security Services.

Value	Description
Teamcenter Application Identifier	Specifies the application identifier for the Teamcenter web application.
TcRA Application Identifier	Specifies the application identifier for the Reporting and Analytics web application.
SSO Scheduler Application Identifier	Specifies the ID of scheduler application.
Mediator Password	For information about mediating applications, see *Security Services Configuration* in the Teamcenter documentation. Specifies the Security Services mediator password.
Identity Service URL	Specifies URL to the Security Services Identity Service.
Login Service URL	Specifies the URL to the Security Services Login Service.

Note:

- Reporting and Analytics requires additional steps to complete configuration.

  For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

- If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

Reporting and Analytics web parts and services

In this step, you optionally enable web services and integration with SharePoint and Teamcenter community collaboration with Reporting and Analytics.

Value	Description
Enable SOA	Enable the Teamcenter service-oriented architecture (SOA) connector with Reporting and Analytics.
Enable Sharepoint/Tc Community Integration	Select this check box to enable Reporting and Analytics integration with Microsoft SharePoint services and Teamcenter community collaboration.

Note:

Reporting and Analytics requires additional steps to complete configuration.

For more information, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

Reporting and Analytics snapshot migration

In this step, you specify how you want to migrate Reporting and Analytics snapshots during upgrade.

Value	Description
Do not run snapshot migration through installer	Specifies you do not want to migrate Reporting and Analytics snapshots during upgrade.
Run snapshot migration through installer	Specifies you want to migrate Reporting and Analytics snapshots during upgrade.
Snapshot Migration Scheme	Options to specify how to migrate snapshots.

Value	Description
Sequential	Specifies sequential migration. If you select this option, select **Normal** or **Batch Execution**, and type a batch size in the **Batch Size** box.
Parallel	Specifies parallel migration. Type a thread count in the **Thread Count** box.

Note:

For more information about these options, see the *Teamcenter Reporting and Analytics Deployment Guide* in the Reporting and Analytics software kit.

Upgrading a copied test environment

In this step, you provide information required to upgrade a copied test environment for Teamcenter Reporting and Analytics.

16. Repeatable Digital Validation

Configuring an RDV database

In this step, you configure a separate database for use with Repeatable Digital Validation.

> Note:
>
> QPL and a separate RDV database are not required if you use cacheless search.

A separate RDV database also allows you to tune the RDV database without interfering with the Teamcenter database.

Prerequisites:

- An Oracle database server must be installed.
- A database instance must exist, either a specific instance configured for Teamcenter or a multipurpose instance to be configured in this step.

References:

For information about installing a database server and configuring databases for use with Teamcenter, see *Teamcenter Installation on Linux Using TEM* and *Teamcenter Installation on Windows Using TEM* in the Teamcenter help library.

Value	Description
Database Server	
Database Engine	Specifies the type of database server you are connecting to, in this case, Oracle Server.
Host	Specifies the name of the host on which Oracle Server runs. This host must exist, and Oracle Server must be installed.
Port	Specifies the number of the port on which Oracle Server listens. The port number was determined when Oracle Server was installed.
Instance (SID)	Specifies the name of the service for the Oracle instance. The service name was determined when the Oracle server was installed.
Database User	Specifies a database user name. For the RDV database, if you use QPL, the user name must be **qpl**.

Value	Description
	• To connect to a database configured for use with Teamcenter, enter the name defined for a database user when the database was configured. • To configure a database for use with Teamcenter, enter the name of the database user you want to create. You must also complete the fields in the **Database Creation** section.
Database Password	Specifies a database password: • To connect to a database configured for use with Teamcenter, enter the password defined for the database user when the database was configured. • To configure a database for use with Teamcenter, enter a password for the database user you are creating. To configure a database, you must also complete the fields in the **Database Creation** section. Caution: The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab. Make sure the password does not contain space characters or any of the following characters: `!@$%'":;.<>(){}`
Database Creation	
Create Tablespaces and User	Specifies that you want to configure a database. The **Database User** and **Database Password** fields in the **Database Server** section must identify the user name and password for the database you are configuring.
Database System User	Specifies the user name for the Oracle system user account.
Database System Password	Specifies the password for the Oracle system user account.
Tablespace Directory on Server	Specifies the full path to the tablespace directory on the Oracle server host where the database tablespace files can be created.

Value	Description
	Enter this path in the format valid for the operating system on which Oracle Server runs, rather than of the corporate server you are installing. For example, if the corporate server is a Linux system, but the Oracle Server host is a Windows system, enter the path in Windows format.
Tablespace Sizes (MB)	Specifies the size for each tablespace in megabytes.
IDATA Size **TEMP Size**	The size of the tablespace depends on the amount of data harvested from the Teamcenter database. The RDV database is heavily used for data warehousing (it experiences large uploads and simple queries but few updates).

Configuring Repeatable Digital Validation

In this step, you install and configure files used in conjunction with the rich client Design Context application.

For QPL-based Design Context, installing Repeatable Digital Validation (RDV) services is required. For Appearance-based Design Context, installing RDV services is not required.

Value	Description
Settings	
QPL Port	Specifies the number of the port the QPL server listens to for requests. The default value is **14730**.
Search Engine	
JT search engine	Specifies a search engine that is not specific to NX. Tip: Use this value when files used with RDV are tessellated files originally created using any software (including NX).
UG search engine	Specifies an NX-based search engine. Tip: Use this value when all files used with RDV are created in NX.
NX Application Location	Specifies the path to the location of an installed NX application.

Database engine selection for Repeatable Digital Validation

In this step, you provide information required to create the database for Repeatable Digital Validation (RDV).

> Note:
>
> QPL and a separate RDV database are not required if you use cacheless search.

Prerequisites:

- A database server must be installed, either Oracle Server or MS SQL Server.
- A database instance must exist, either a specific instance configured for Teamcenter or a multipurpose instance to be configured in this step.

References:

For information about installing a database server and configuring databases for use with Teamcenter, see *Teamcenter Installation on Linux Using TEM* and *Teamcenter Installation on Windows Using TEM* available in the Teamcenter help library.

In the **Database Engine** box, select the database engine you use (**Oracle** or **Microsoft SQL Server 2005**).

Enter the following database configuration values, depending on the database engine you select:

Oracle database server values

Value	Description
Database Server	Specifies the name of the host on which Oracle Server runs. This host must exist, and Oracle Server must be installed.
Service	Specifies the name of the service for the Oracle instance. The service name was determined when the Oracle server was installed.
Port	Specifies the number of the port on which Oracle Server listens. The port number was determined when Oracle Server was installed.
Database User	Specifies a database user name. For the RDV database, if you use QPL, the user name must be **qpl**. • To connect to an existing database configured for use with Teamcenter, enter the name defined for a database user when the database was configured.

Value	Description
	• To create and configure a database for use with Teamcenter, enter the name of the database user you want to create.
Database Password	Specifies a database password: • To connect to an existing database configured for use with Teamcenter, enter the password defined for the database user when the database was configured. • To configure a new database for use with Teamcenter, enter a password for the database user you are creating. Caution: The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab. Make sure the password does not contain space characters or any of the following characters: **! @ $ % ' " : ; . < > ( ) { }**

Microsoft SQL Server values

Value	Description
Database Server	Specifies the name of the host on which MS SQL Server runs. This host must exist, and MS SQL Server must be installed.
Choose one of the following methods to connect to the database:	
Named Instance	If you connect to Microsoft SQL Server using a named instance, select this option and enter the instance name you defined when you installed MS SQL Server.
Port	If you connect to Microsoft SQL Server using a specific port, select this option and enter the port number you specified when you installed MS SQL Server.
Database User	Specifies a database user name: • To connect to an existing database configured for use with Teamcenter, enter the name defined for a database user when the database was configured.

Value	Description
	• To create and configure a new database for use with Teamcenter, enter the name of the database user you want to create.
Database Password	Specifies the password for the database user: • To connect to an existing database configured for use with Teamcenter, enter the password defined for the database user when the database was configured. • To configure a new database for use with Teamcenter, enter a password for the database user you are creating.
Database Name	Specifies the name of the MS SQL Server database. The database name was determined when database was created.

17. Rich client

About rich client installation in TEM

The Teamcenter rich client is a gateway to your company's product information. The rich client framework allows you to integrate and run Product Data Management applications along with various other applications, all from a common platform. These applications can be Microsoft Office applications, custom applications, Java Plug-ins, or CAD/CAM/CAE applications such as NX.

The following TEM help topics describe panels that allow you to install Teamcenter rich clients and add-on features. For more information about using FMS, see the appropriate client installation guide (for Windows or Linux) and the Teamcenter Administration.

Setting two-tier transport mode

If you want to allow multiple concurrent user sessions of your two-tier rich client, set the transport mode for the two-tier rich client. In the **Activation Mode** box, select **PER_CLIENT**. (The default value, **NORMAL**, does not allow multiple concurrent user sessions.)

- The number of user sessions allowed in **PER_CLIENT** mode is limited by the capabilities of your operating system.
- For information about enabling multiple rich client support, see *Enabling multiple client sessions* in the appropriate client installation guide (for Windows or Linux).

Two-tier Teamcenter server settings

In this step, you specify values required for the rich client to access your Teamcenter server.

Value	Description
Connection Port	Specifies the port number on which the TAO implementation repository service is to run on the client workstation. Make sure this value reflects the port used by your Teamcenter corporate server.
2–tier Servers	Specifies the servers that provide database access for your rich client. To add a database, perform the following steps: 1. Click **Add**. 2. Enter the path to the data directory (**TC_DATA**) where you want Teamcenter Environment Manager to create shared data

Value	Description
	subdirectories and files. This can be the network path to the **TC_DATA** directory on your corporate server. 3. Enter a unique name for the connection. 4. Click **OK**. 5. If you want to add access to additional databases, repeat steps 1 through 4 to add access information for each database. After you add a database, you can remove databases from the list or edit settings using the **Remove** and **Edit** buttons. You can also change the priority the rich client uses in database access by selecting a database in the table and clicking the **Up** or **Down** buttons.

Supplying middle-tier server settings

In this step, you supply connection settings for the four-tier rich client.

The **4-tier Servers** table lists web servers to which the four-tier rich client connects.

To add a server to the table, click **Add**. Double-click the box in the **URI** or **Connection Name** columns to type values for the additional server.

Use the **Up** and **Down** buttons to assign server priority.

To remove a server from the table, select the appropriate row and click **Remove**.

The **Compress (gzip) the responses from the Web application servers** check box is selected by default. This option provides faster connection performance from the server.

Two-tier rich client uses TCCS instead of IIOP

The Teamcenter two-tier rich client now uses TCCS (Teamcenter client communication system) instead of IIOP (Internet Inter-ORB Protocol) to communicate with the corporate server.

IIOP protocol is no longer supported in Teamcenter. During upgrade, TEM converts existing two-tier rich clients to use TCCS.

Rich client run-time home

In this step, you enter a location in which you want to place rich client files during run time for the shared rich client installation. In the **Runtime Home Location** box, enter a local path.

For more information about installing a shared rich client, see the appropriate client installation guide (for Windows or Linux).

Rich client two-tier settings

In this step, you enter settings for the two-tier rich client.

In the **Rich client Web Server** box, enter the URL to the presentation tier web application. Teamcenter uses this value to construct URLs within the two-tier rich client. Optionally, you can leave this field blank, making URLs within the rich client nonfunctional.

> Note:
>
> - If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.
> - If you use SSL, make sure you include the fully qualified host name in the URL to the web application.

Rich client settings

In this step, you configure access to the Teamcenter documentation.

Value	Description
Enable online help	Specifies that you want to access the Teamcenter documentation from your rich client configuration. Select this check box to enable documentation access.
Documentation server URL	Specifies the URL to the Teamcenter documentation. Type the appropriate online help URL: **https://***domain***/en-US/doc/282219420/PL20240523460057788.xid1899404/html/xid1899405** Replace *domain* with the source from which you access online help: • Support Center (Internet): **docs.sw.siemens.com** • Siemens Documentation Server (local network): *doc-server-host*:*doc-server-port*

Value	Description
	If you use the Siemens Documentation Server, you must install the server and documentation before you configure documentation access from Teamcenter clients. For information about installing documentation and the Documentation Server, see the appropriate client installation guide (for Windows or Linux).

For advanced configuration options, click **Advanced**.

> Note:
>
> If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

Rich client run-time folder

In this step, you enter a location in which you want to place rich client temporary files during run time. In the **Runtime Temp Folder** box, enter a local path.

18. Lifecycle Visualization

About Lifecycle Visualization installation in TEM

Teamcenter provides an embedded viewer and the **Lifecycle Visualization** perspective for the rich client, as well as the stand-alone Teamcenter lifecycle visualization application which can be launched from the rich client. The embedded viewer allows you to visualize 3D models in the Lifecycle Viewer application and within other Teamcenter client applications such as Structure Manager.

If you want to use the enhanced Lifecycle Visualization capabilities of these Lifecycle Visualization viewers, you must purchase the necessary Lifecycle Visualization licenses and download Lifecycle Visualization software. For more information about using Lifecycle Visualization, see *Visualization on Rich Client — Getting Started*.

The following TEM help topics describe panels that allow you to configure Lifecycle Visualization. These panels are displayed if you select one of the following features:

- **Teamcenter Visualization (Embedded) for Rich Client**
- **Teamcenter Visualization (Stand-alone) for Rich Client**

On Windows systems, these features are *not* required if you install Lifecycle Visualization before you install the rich client. However, if your versions of Lifecycle Visualization and Teamcenter differ (for example, if you do not install Lifecycle Visualization 2412 with Teamcenter 2412), the rich client may display an error when you open the viewer. If this happens, see the troubleshooting topics in *Teamcenter Rich Client Installation on Windows*.

On Linux systems, these features are required to enable Lifecycle Visualization viewers in the rich client.

Installing the embedded viewer for rich client

In this step, you provide information required to install the Lifecycle Visualization embedded viewer for rich client.

Prerequisites:

- A Lifecycle Visualization software kit must be available in a location accessible to this host, or Lifecycle Visualization must be installed on a host accessible to this host.

If Lifecycle Visualization (embedded viewer or standalone application viewer) is already installed:

1. In the **Teamcenter Visualization Location** box, enter the location in which Lifecycle Visualization software is installed.

2. Select **Connect to existing Teamcenter Visualization application at the above location**.

If no Lifecycle Visualization software is installed:

1. In the **Teamcenter Visualization Location** box, enter the location in which you want to install Lifecycle Visualization software.

2. Select **Install Teamcenter Visualization (Embedded) to the above location from the following image**.

3. In the **Teamcenter Visualization Install Image** box, enter the full path to the **Teamcenter_Visualization_***version***.msi** file in the Lifecycle Visualization software kit. Include the **.msi** file name in the path.

Installing the standalone application viewer for rich client

In this step, you provide information required to support the Lifecycle Visualization standalone application viewer for rich client.

Prerequisites:

- Lifecycle Visualization must be installed on the current host.

References:

For information about Lifecycle Visualization licensing and functionality, see *Visualization on Rich Client — Getting Started* guide and the Teamcenter 2412 help library.

In the **Existing Install Location** box, enter the location in which Lifecycle Visualization software is installed. This feature configures the rich client to launch the installed standalone application viewer.

Configuring Lifecycle Visualization for Teamcenter

In this step, you enter Lifecycle Visualization settings for Teamcenter.

Value	Description
Protocol	Specifies the protocol to use for Lifecycle Visualization requests.
Host	Specifies the host on which to install Lifecycle Visualization.
Port	Specifies the port you want Lifecycle Visualization to use.
Domain	Specifies the domain under which Lifecycle Visualization runs.

19. Teamcenter integrations

Team Collaboration Integration settings

In this step, you enter settings for the Team Collaboration Integration, which provides the capability to post to social applications such as Slack and Microsoft Teams using the Teamcenter Social Integration.

Value	Description
Service Access Key ID	Specifies the account access key ID for the Team Collaboration Integration. This value is required.
Service Secret Key	Specifies the secret key for the Team Collaboration Integration. This value is required.

Configuring ERP Connect Toolkit

In this step, you install the generic ERP Connect Toolkit interface.

> Note:
>
> The ERP Connect Toolkit is intended for sites currently using ERP Connect. Sites setting up new integrations should use the appropriate Teamcenter Gateway product.

Configuring ERP Connect Toolkit is required only if your site needs to integrate Teamcenter with other Enterprise Resource Planning (ERP)-supported applications, such as BAAN.

Postinstallation:

Complete the software configuration following the instructions in the *Teamcenter Environment Variables*.

Value	Description
ERP Data Directory Location	Specifies installation of the ERP Connect Toolkit interface.
Share Name	Specifies a name for the Teamcenter network share. Enter a name or accept the default value.

Teamcenter Integration for NX for rich client

In this step, you specify the location of your NX installation in the **NX Install Location** field.

Note:

When you upgrade to a new version of NX, uninstall the **NX Rich Client Integration** feature in TEM, and then reinstall this feature, specifying the path to the new NX installation in the **NX Install Location** box in TEM.

Verifying requirements for Teamcenter Excel import

In this step, TEM verifies that the required software for the Teamcenter Excel import feature are present on your system. If the required software is not present, you must install it before you can continue with installation.

Read the messages on this panel and perform the recommended actions before you continue.

iWay integration settings

In this step, you specify settings for the iWay integration to Teamcenter.

In the **iWay Installation Location** box, enter the path to the iWay software.

Microsoft Office support for rich client

In this step, you type the URI to the Teamcenter Client for Microsoft Office application.

Note:

If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

Google Online microservice settings

In this step, you specify settings for the Google Online microservice.

For more information about the Google Online server, see *Deploying Document Management* in the Teamcenter documentation.

Value	Description
Google Online Server Settings	Settings for the Google Online server.
Google Authorized Redirect URIs	Specifies authorized redirect URIs for the Google server. Enter fully qualified domain names.
Google Application Name	Specifies the name of your Google web application.

Value	Description
Google Client ID	Specifies the client ID of your Google web application.
Google Client Secret	Specifies the client secret password of your Google web application.
Sponsor User Information	Credentials for the *Sponsored Authentication* user. You create these when you create a user profile.
Sponsor User ID	Specifies the user ID of the sponsored user.
Sponsor User Password	Specifies the password of the sponsored user. Enter the password again in the **Confirm Password** box to confirm.
Google Online Server Connection Settings	Settings for the Google Online server connection.
Teamcenter Gateway URL	Specifies the URL to the Active Workspace Gateway. The URL should be of this form: **http://***host***:***port* Replace *host* and *port* with the host and port on which the Gateway runs. For example: **http://localhost:3000**
Teamcenter SSO	Specifies whether to use Security Services when connecting to the Google Online server.

Teamcenter Client for Microsoft Office installation

This panel verifies whether the current host meets the system requirements for Teamcenter Client for Microsoft Office. This includes the required versions of the Microsoft .NET framework and other libraries and also a supported version of Microsoft Office.

Choose how you want to enable access to Client for Office:

Install Teamcenter Client for Microsoft Office for all users on this system	Specifies that Client for Office will be available for all users on the current machine.

Install Teamcenter Client for Microsoft Office for me only	Specifies that Client for Office will be available for the current user only.

For more information about installing Teamcenter Client for Microsoft Office, see *Teamcenter Rich Client Installation on Windows*.

Teamcenter Extensions for Microsoft Office

This panel verifies whether the current host meets the system requirements for Teamcenter Extensions for Microsoft Office. This includes the required versions of the Microsoft .NET framework and other libraries and also a supported version of Microsoft Office.

For more information about installing Teamcenter Extensions for Microsoft Office, see *Teamcenter Rich Client Installation on Windows*.

Teamcenter Office Online server settings

In this step you specify settings for the Teamcenter Office Online server.

You must install the Teamcenter Office Online web service on a separate machine and not on the same machine that has Microsoft Office Online Server. Ensure that both are Windows hosts with machines with Microsoft Internet Information Server (IIS) installed.

Value	Description
Microsoft Office Online Server Settings	Settings for accessing the Microsoft Office Online server.
MS Office Online Server Discovery URL	Specifies the reference URL of the deployed Microsoft Office Online Server. For example: **http://OfficeOnline/hosting/discovery**
Sponsor User Information	Sponsored authentication settings. Sponsored authentication allows an application integrated with Teamcenter to log onto Teamcenter using sponsored mode.
User ID	Specifies the user ID of the sponsored authentication user.
Password	Specifies the password for the sponsored authentication user. Type the password again in **Confirm Password** to confirm.

Value	Description
Office Online Server Connection Settings	Connection settings for the Teamcenter Office Online server.
Teamcenter 4-tier URL	Specifies the URL to the Teamcenter web tier.
FSC Connection URL	Specifies the connection URL to the Teamcenter FMS server cache (FSC).

Office Online Server IIS settings

In this step, you specify settings for the Microsoft Internet Information Server (IIS) that hosts the Web Application Open Platform Interface (WOPI) server for Office Online.

> Note:
>
> Teamcenter Office Online web service is only supported on an IIS web server. You must first enable IIS and ASP.NET on the machine on which you plan to install Teamcenter Office Online web service. You must use the same script that you used to install Microsoft Office Online Server. To do so, refer to the scripts specified in **Office Online Server**.

Value	Description
IIS Web Site Configuration	
Use Existing Web Site	Specifies that you want to use an existing web site. You must select the existing web site from the list. Teamcenter creates the virtual directory for the Office Online application in the specified web site in IIS. The Office Online application is hosted in the specified web site. This option is selected by default.
Create New Web Site	(Optional) Specifies that you want to create a new web site for the Office Online deployment. You must specify values for **Web Site Name**, **Web Site Port**, and **Web Site Root Path**.
Web Site Name	(Optional) Specifies the name of the new web site in IIS. This value is required only if you select the **Create New Web Site** option.
Web Site Port	(Optional) Specifies the port number of the new web site in IIS. This port must be available and unassigned. This value is required only if you select the **Create New Web Site** option.
Web Site Root Path	(Optional) Specifies the root of web content subdirectories for the new web site. This value is required only if you select the **Create New Web Site** option.
IIS Web Application Pool Configuration	

Value	Description
Use Existing Application Pool	Specifies whether to use an existing application pool from the list provided. An application pool is a set of one or more applications assigned to an IIS worker process. The Teamcenter .NET web tier is an ASP.NET application. Keep this in mind if you intend to have this application pool host other applications. This option is selected by default.
Create New Application Pool	(Optional) Specifies whether to create a new application pool. You must provide a value for **Application Pool Name**.
Application Pool Name	(Optional) Specifies the name for the IIS application pool. This value is required only if you select the **Create New Application Pool** option.
IIS Virtual Directory Configuration	
Virtual Directory Name	Specifies the IIS virtual directory name for Office Online application deployment. Web URLs for four-tier deployments are based on this value. The URLs are of the form: **http://***host***:***port***/***application***/...**
Log File Path	Specifies the path in which to place log files for the Office Online web server.

Teamcenter Office Online WOPI host settings

In this step, you supply settings for Teamcenter Office Online to access the Web Application Open Platform Interface (WOPI) server.

Value	Description
Host Name	Specifies the host name Teamcenter Office Online web service, also known as the WOPI host.
Port	Specifies the port used by the WOPI server.

Teamcenter Client for Microsoft Office configuration

In this step, you enter Teamcenter server settings for Teamcenter Client for Microsoft Office.

Value	Description
Install Teamcenter Single Sign-on support for Office Client	Select this check box if you want to use Security Services with Client for Office.
SSO Application ID	Specifies the application ID of your Teamcenter installation as configured in the Security Services installation.

Value	Description
Protocol	Specifies the protocol used to access the Security Services application (**http** or **https**).
SSO Server Host	Specifies the server host for the Security Services application.
SSO Server Port	Specifies the port used by the Security Services application.
SSO Application Name	Specifies the application name of the Security Services application.

Configuring the Office Online microservice

In this step, you specify settings for the Teamcenter Office Online microservice.

Value	Description
Microsoft Office Online Server Settings	Settings for the Office Online server.
MS Office Online Server Discovery URL	Enter the reference URL of the deployed Microsoft Office Online Server. For example: **http://host_office_online_server/hosting/discovery**
Sponsor User Information	Credentials for the Teamcenter *Sponsored Authentication* user. For information about sponsored authentication, see the *Security Administration* guide.
Use Sponsored Authentication	Specifies you want to use sponsored authentication.
User ID	Specifies the user ID of the sponsored authentication user.
Password	Specifies the password of the sponsored authentication user. Confirm the password by typing it again the **Confirm Password** box.
Protocol Selection	
Use HTTPS Protocol	Specifies you want to use HTTP protocol to access the Office Online server.
Certificate Path	Specifies the path to the certificate. Click the browse button (**...**) to browse to the certificate location.

Value	Description
Password	Specifies the certificate password. Confirm the password by typing it again the **Confirm Password** box.
Office Online Server Connection Settings	Connection settings for the Office Online server.
Active Workspace Gateway URL	Specifies the URL to the Active Workspace Gateway. The URL should be of this form: **http://***host***:***port* Replace *host* and *port* with the host and port on which the Gateway runs. For example: **http://localhost:3000**
Teamcenter SSO	Specifies whether to use Security Services when connecting to the Office Online server.

Workflow to Scheduling Integration settings

In this step, you specify settings for the Workflow to Schedule Integration.

The Workflow to Scheduling Integration allows workflow to send updates to related tasks in a schedule.

Prerequisite:

You must create the proxy user account (**projproxy**) before you install the Workflow to Scheduling Integration.

Value	Description
Proxy User Name	Specifies the proxy user name for the Teamcenter server.
Proxy User Group	Specifies the proxy user group for the Teamcenter server.
Proxy User Password	Specifies the password for the proxy user.

Configuring SCM ClearCase Integration

In this step, you configure the SCM ClearCase Integration by specifying the location of a ClearCase server on the local host.

Note:

An existing installation of a ClearCase server is required.

20. Multi-Site Collaboration

Installing Multi-Site Collaboration

This panel presents steps to perform before you proceed with upgrading Multi-Site Collaboration

Enabling the Teamcenter Enterprise integration for Teamcenter Integration Framework

In this step, you enable the Teamcenter Enterprise integration for Teamcenter Integration Framework.

In the **Enterprise Connector** box, browse to the location of the Teamcenter Enterprise connector files (**mti.jar** and **mtiems.jar**).

TEM must be able to access these files to enable the Teamcenter Enterprise integration.

For more information on Teamcenter Integration Framework, see the Teamcenter Integration Framework documentation available on Support Center.

Teamcenter Integration Framework settings

In this step, you have the option to change the default port settings for Teamcenter Integration Framework.

If you want to change the values of **Web Server Port**, **LDAP Server Port**, **Security Port**, **Web UI Port**, or **Active MQ Port**, click **Advanced**, and then type new port values.

For more information on Teamcenter Integration Framework, see the Teamcenter Integration Framework documentation on Support Center.

Teamcenter Integration Framework disk image

In this step, you specify settings for creating a disk image file.

Value	Description
JDK Location	Enter the location of a supported Java development kit (JDK). Teamcenter Integration Framework requires the JDK to create the disk image.
Installation Location on Targeted Machine	Enter the path in which you intend to deploy the disk image on the target host.
Disk Image File Directory	Enter the path on the current host in which to save the disk image file.

When TEM creates the disk image file, it zips all the files under the *TC_ROOT***tcif** folder into a ZIP file called **diskimage.zip**, and then places the ZIP file into the **Disk Image File Directory**. The root folder within this ZIP file is **tcif**. After it is complete, TEM copies the TEM installer, configuration files, and installation log files to the same location. TEM also creates a silent installation file that can be used by TEM to silently install the disk image file.

If you are upgrading from a supported version of Teamcenter Integration Framework, you are prompted for your administrator user credentials. For more information about upgrading Teamcenter Integration Framework, see *Upgrading Teamcenter Integration Framework* in the Teamcenter Integration Framework documentation on Support Center.

Event notification system configuration

In this step, you specify settings for the event notification system.

Value	Description
Database Name	Specifies the name of the event notification system database.
Database User	Specifies the database user of the event notification system database.
Database Password	Specifies the password for the event notification system database.
Username	Specifies the user name for logging on to the Apache ActiveMQ messaging server.
Password	Specifies the password for logging on to the Apache ActiveMQ messaging server.

Multi-Site IDSM settings

In this step, you enter settings for the Multi-Site Distributed Services Manager (IDSM) service.

Value	Description
Service ID	Specifies an ID for the IDSM service.
Service Name	Specifies a name for the IDSM service.
Port	Specifies the port used by the IDSM service.
RPC Number	Specifies the remote procedure call (RPC) program number for the IDSM service. By default, the Multi-Site RPC server uses random TCP ports over a range of ports. The range varies depending on your platform. If your enterprise security requires servers to communicate on static port numbers, you can customize the Multi-Site configuration to run the ODS and IDSM servers on specified port numbers.
Staging Area	Specifies the temporary directory for storing data.
Staging Area Size	Specifies the size in bytes for the temporary directory.

Multi-Site ODS settings

In this step, you enter settings for the Multi-Site Object Directory Services (ODS) service.

Value	Description
Service ID	Specifies an ID for the ODS service.
Service Name	Specifies a name for the ODS service.
Port	Specifies the port used by the ODS service.
RPC Number	Specifies the remote procedure call (RPC) program number for the ODS service. By default, the Multi-Site RPC server uses random TCP ports over a range of ports. The range varies depending on your platform. If your enterprise security requires servers to communicate on static port numbers, you can customize the Multi-Site configuration to run the ODS and IDSM servers on specified port numbers.

21. Archive and Restore

Archive: Create Connection

In this step, you select the type of connection you want to create to the Teamcenter database that will be designated as an archive database. You can connect to a new or existing database. Choose the appropriate option:

- **Connect to existing database**: Connects your configuration to an existing archive database at another site.
- **Populate archive database**: Connects to and populates a new database at another site, designating that database as the archive. Optionally choose to create a database on the other site if one does not already exist.

For more information about archiving and restoring, see Multi-Site Collaboration in the Teamcenter documentation.

Archive: Foundation Database

In this step, you provide the information that Teamcenter requires to connect to the Teamcenter database that will be designated as an archive database. The archive database must be the same as the Teamcenter database.

Prerequisites:

- You must install a database server. Teamcenter supports Oracle or Microsoft SQL Server databases.
- If you use Oracle, you must create a database instance, either a specific instance configured for Teamcenter or a multipurpose instance to be configured in this step.

References:

For more information about archiving and restoring, see Multi-Site Collaboration in the Teamcenter documentation.

In the **Data Directory** box, enter a location for the Teamcenter data directory (*TC_DATA*).
The directory must exist. TEM creates shared data subdirectories and files in this location.

In the **Database Server** box, select your database vendor (**Oracle** or **Microsoft SQL Server**).

Enter the following database configuration values, depending on the database vendor you select.

Oracle database server values

Value	Description
Host	Specifies the name of the host on which the Oracle server runs. This host must exist, and the Oracle server must be installed.
Service	Specifies the name of the service for the Oracle instance. The service name was determined when the Oracle server was installed.
Port	Specifies the number of the port on which the Oracle server listens. The port number was determined when the Oracle server was installed.
User	Specifies a database user name: • To connect to an existing database configured for use with Teamcenter, enter the name defined for a database user when the database was configured. • To create and configure a database for use with Teamcenter, enter the name of the database user you want to create.
Password	Specifies a database password: • To connect to an existing database configured for use with Teamcenter, enter the password defined for the database user when the database was configured. • To configure a new database for use with Teamcenter, enter a password for the database user you are creating.

If you chose to create a new database instead of using an existing database, provide the following values:

System User	Specifies a user name of the Oracle system administrator account. The default value is **system**.
Password	Specifies a password for the Oracle system administrator account.

Caution:

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

Make sure the password does not contain space characters or any of the following characters:

Value	Description
	! @ $ % ' " : ; . < > ( ) { }
Database Path	Specifies the location of the tablespaces for the Teamcenter database on the Oracle server. This is typically *ORACLE_HOME***oradata***Oracle_SID* (on Windows systems) or *ORACLE_HOME*/**oradata**/*Oracle_SID* (on Linux systems).
Data Directory	Specifies the path to the Teamcenter data (*TC_DATA*) directory. This value is stored in the **TC_DATA** variable in your Teamcenter configuration. TEM creates shared data subdirectories and files in this location. Each data directory is associated with a single database user within a database instance. Note: Do not create a **TC_DATA** variable in the system environment. TEM sets this variable as required in Teamcenter scripts. Setting this variable in the operating system causes conflicts if you install more than one configuration.
Share Name	Specifies a name for the Teamcenter network share. Enter a name or accept the default value. During Teamcenter installation, TEM creates the network share to the configuration directory (accessible as *****server-name***share-name*) where client workstations can access configuration information. Because this shared directory is accessed using the UNC path, the server must be connected to the network during the installation.

Microsoft SQL Server values

Value	Description
Instance	If you connect to Microsoft SQL Server using a named instance, select this option and enter the instance name you defined when you installed MS SQL Server.
Port	If you connect to Microsoft SQL Server using a specific port, select this option and enter the port number you specified when you installed MS SQL Server.
Login Name	Specifies a database user name: • To connect to an existing database configured for use with Teamcenter, enter the name defined for a database user when the database was configured.

Value	Description
	• To create and configure a new database for use with Teamcenter, enter the name of the database user you want to create.
Login Password	Specifies the password for the database user: • To connect to an existing database configured for use with Teamcenter, enter the password defined for the database user when the database was configured. • To configure a new database for use with Teamcenter, enter a password for the database user you are creating.
Database Name	Specifies the name of the MS SQL Server database. The database name was determined when database was created.

If you chose to create a new database instead of using an existing database, provide the following values:

System User	Specifies the user name of the SQL Server system administrator account. The default value is **sa**.
Password	Specifies the password for the SQL Server system administrator account.

> Caution:
>
> The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab.
>
> Make sure the password does not contain space characters or any of the following characters:
>
> **! @ $ % ' " : ; . < > ( ) { }**

Database Path	Specifies the directory in which to create the Teamcenter database on the SQL Server server.
Collation	Specifies the collation used by the Teamcenter database on the Microsoft SQL Server server. *Collation* defines the alphabet or language whose rules are applied when data is sorted or compared.
Enable UTF-8	Specifies whether to enable support for UTF-8 encoding in the Teamcenter database. Microsoft SQL Server does not provide native support for UTF-8. The **Enable UTF-8** option enables the Teamcenter server to convert character encoding to and from UTF-8 when interacting with the database.

Value	Description
	For information about configuring your Teamcenter host to support UTF-8, see the Teamcenter installation guides for Windows and Linux.
Data Directory	Specifies the path to the Teamcenter data (*TC_DATA*) directory. This value is stored in the **TC_DATA** variable in your Teamcenter configuration. TEM creates shared data subdirectories and files in this location. Each data directory is associated with a single database user within a database instance. Note: Do not create a **TC_DATA** variable in the system environment. TEM sets this variable as required in Teamcenter scripts. Setting this variable in the operating system causes conflicts if you install more than one configuration.

PostgreSQL database server values

Value	Description
Host	Specifies the name of the host on which the PostgreSQL server runs. This host must exist, and the PostgreSQL server must be installed.
Port	Specifies the number of the port on which the PostgreSQL server listens. The port number was determined when the PostgreSQL server was installed.
Login Name	Specifies a database user name: • To connect to an existing database configured for use with Teamcenter, enter the name defined for a database user when the database was configured. • To create and configure a database for use with Teamcenter, enter the name of the database user you want to create.
Login Password	Specifies a database password: • To connect to an existing database configured for use with Teamcenter, enter the password defined for the database user when the database was configured. • To configure a new database for use with Teamcenter, enter a password for the database user you are creating.

Value	Description
Database Name	Specifies the name of the PostgreSQL database. The database name was determined when database was created.

If you chose to create a new database instead of using an existing database, provide the following values:

System User	Specifies a user name of the PostgreSQL system administrator account. The default value is **postgres**.
Password	Specifies a password for the PostgreSQL system administrator account.

> Caution:
>
> The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab.
>
> Make sure the password does not contain space characters or any of the following characters:
>
> **! @ $ % ' " : ; . < > ( ) { }**

Database Path	Specifies the location of the tablespaces for the Teamcenter database on the PostgreSQL server.
Data Directory	Specifies the path to the Teamcenter data (*TC_DATA*) directory. This value is stored in the **TC_DATA** variable in your Teamcenter configuration. TEM creates shared data subdirectories and files in this location. Each data directory is associated with a single database user within a database instance.

> Note:
>
> Do not create a **TC_DATA** variable in the system environment. TEM sets this variable as required in Teamcenter scripts. Setting this variable in the operating system causes conflicts if you install more than one configuration.

Archive: Multisite Configuration

In this step, you install the components that replicate data between multiple Teamcenter sites, enabling the exchange of data objects with other Teamcenter databases over a wide area network (WAN).

You must install at least one of the services that Multi-Site Collaboration uses to manage the replication process for this database:

- The object directory service (ODS) provides location and access information for Teamcenter objects distributed to various sites in a distributed Teamcenter environment.
- One or more Teamcenter Distributed Services Manager (IDSM) processes manage the replication of objects from one Multi-Site Collaboration site to another.

Value	Description
Distributed Services Manager (IDSM)	Specifies that you want to install the distributed services manager service on this host. You can choose to install both the IDSM service and the ODS service. You must install one of the two services. If you choose both, this system becomes both an IDSM and an ODS server for the same database.
Object Directory Services (ODS)	Specifies that you want to install the object directory services on this host. You can choose to install both the IDSM service and the ODS service. You must install one of the two services. If you choose both, this system becomes both an IDSM and an ODS server for the same database.

For more information about archiving and restoring, see Multi-Site Collaboration in the Teamcenter documentation.

Archive: Multi-Site ODS settings

In this step, you enter settings for the Multi-Site Object Directory Services (ODS) service.

Value	Description
Service ID	Specifies an ID for the ODS service.
Service Name	Specifies a name for the ODS service.
Port	Specifies the port used by the ODS service.
RPC Number	Specifies the remote procedure call (RPC) program number for the ODS service. By default, the Multi-Site RPC server uses random TCP ports over a range of ports. The range varies depending on your platform. If your enterprise security requires servers to communicate on static port numbers, you can customize the Multi-Site configuration to run the ODS and IDSM servers on specified port numbers.

For more information about archiving and restoring, see Multi-Site Collaboration in the Teamcenter documentation.

Archive: Multi-Site IDSM settings

In this step, you enter settings for the Multi-Site Distributed Services Manager (IDSM) service.

Value	Description
Service ID	Specifies an ID for the IDSM service.
Service Name	Specifies a name for the IDSM service.
Port	Specifies the port used by the IDSM service.
RPC Number	Specifies the remote procedure call (RPC) program number for the IDSM service. By default, the Multi-Site RPC server uses random TCP ports over a range of ports. The range varies depending on your platform. If your enterprise security requires servers to communicate on static port numbers, you can customize the Multi-Site configuration to run the ODS and IDSM servers on specified port numbers.
Staging Area	Specifies the temporary directory for storing data.
Staging Area Size	Specifies the size in bytes for the temporary directory.

For more information about archiving and restoring, see Multi-Site Collaboration in the Teamcenter documentation.

Archive: Database synchronization check

In this step, you verify the data models of the main Teamcenter database and the archive database.

TEM scans the main database and the archive database to verify their data models are synchronized. In some cases, TEM automatically installs missing data model to align the archive and main databases.

For more information about archiving and restoring, see Multi-Site Collaboration in the Teamcenter documentation.

22. Additional features

Configure documentation access

In this step, you configure access to Teamcenter documentation in the rich client.

Value	Description
Enable Online Help	Specifies that you want to access Teamcenter documentation from Teamcenter rich clients. Select this check box to enable documentation access.
Documentation Server URL	Specifies the URL to the Teamcenter documentation. Teamcenter rich clients can access documentation from one of two sources: • Internet: Access documentation from Support Center. • Local: Access documentation from the Siemens Documentation Server installed on your local host or network. If you use the Siemens Documentation Server, you must install the server and documentation content before you configure documentation access from Teamcenter clients. For information about the documentation URL to enter, see the appropriate client installation guide (for Windows or Linux).

> Note:
>
> For more information about configuring client access to online help, see the Teamcenter client installation guides for Windows and Linux.

Installing CAD-BOM alignment

In this step, you configure a set of parameters to be used as database preferences to allow the Teamcenter installation to interact and share visual data with Teamcenter product master management. Configuring this feature allows designs managed by this installation of Teamcenter to be related to parts in products that are managed by Product Master Management.

Value	Description
PDM System Namespace	Specifies a unique cluster of Teamcenter installations. This value must correspond to a valid value defined in the Product Master Management database. Contact your Product Master Management administrator for an appropriate valid value. This value is used to populate a **UsageWC_MathSystemNamespace** database preference.

Value	Description
	Note: The PDM system namespace is also referred to as a *math system namespace*.
PDM System Name	Specifies a unique name for your Teamcenter installation within the scope of the PDM system namespace. This name is used to identify the originating system of related design components aligned or published to the Product Master Management database. This value should be unique within the scope of the PDM system namespace. The recommended value is the site ID of your installation. This value is used to populate a **UsageWC_MathSystemName** database preference. Note: • The PDM system name is automatically registered with Product Master Management at run time. • The PDM system name is also referred to as a *math system name*.
Item ID Namespace	Specifies the scope of uniqueness for item ID values of designs that are aligned with or published to Product Master Management. This value must correspond to a valid value defined in the Product Master Management database. Contact the Product Master Management administrator for an appropriate valid value. This value is used to populate a **UsageWC_MathNumberNamespace** database preference. Note: The PDM system namespace is also referred to as a *math number namespace*.

Product Master Management URL and Security Services

In this step, you configure access to the Product Master Management application.

Value	Description
Teamcenter PMM URL	Specifies the locale and endpoint URL of the Product Master Management web services. Click **Add** to add a URL to the list.
Enable SSO	Specifies whether to enable Security Services for single sign-on with Product Master Management.
Application ID	Specifies the application ID of your Product Master Management installation as configured in the Security Services installation.
Perpetual Release Mode	Specifies that you want Product Master Management to use perpetual release mode. Perpetual release mode uses date-based part effectivity to configure the product. Product Master Management does not support perpetual releasing without part effectivity.
Present Time Mode	Specifies that you want Product Master Management to use present time release mode.

Note:

- If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.
- The release mode cannot be changed after installation completes. To change the release mode, you must reinstall the Usage Server.

Product Master Management

In this step, you configure Teamcenter alignment with Product Master Management.

Value	Description
Teamcenter BOM Web Service End-Point	Specifies the endpoint URL of the Product Master Management web services, for example: **http://***host***:***port***/tc/tcbompost/tcbompostwebservice** This value is used to populate a **UsageWC_Endpoint** database preference.
PDM System Namespace	Specifies a unique cluster of Teamcenter installations. This value must correspond to a valid value defined in the Product Master Management database. Contact

Value	Description
	your Product Master Management administrator for an appropriate valid value. This value is used to populate a **UsageWC_MathSystemNamespace** database preference. Note: The PDM system namespace is also referred to as a *math system namespace*.
PDM System Name	Specifies a unique name for your Teamcenter installation within the scope of the PDM system namespace. This name is used to identify the originating system of related design components aligned or published to the Teamcenter BOM database. This value should be unique within the scope of the PDM system namespace. The recommended value is the site ID of your installation. This value is used to populate a **UsageWC_MathSystemName** database preference. Note: • The PDM system name is automatically registered with Product Master Management at run time. • The PDM system name is also referred to as a *math system name*.
Item ID Namespace	Specifies the scope of uniqueness for item ID values of designs that are aligned with or published to Product Master Management. This value must correspond to a valid value defined in the Product Master Management database. Contact the Product Master Management administrator for an appropriate valid value. This value is used to populate a **UsageWC_MathNumberNamespace** database preference. Note: The PDM system namespace is also referred to as a *math number namespace*.

Also, select a release mode for Product Master Management, either **Perpetual Release Mode** or **Present Time Mode**.

Note:

If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

Configuring Teamcenter Automotive Edition-GM Overlay

In this step, you configure Teamcenter Automotive Edition-GM Overlay.

Value	Description
GMO Prefix ID	Specifies three uppercase alphabetical characters to prefix GMO item IDs. The prefix ID you enter must be 3 characters and contain only uppercase letters. A GMO item ID has 8 characters, the first 3 are the alphabetical characters you specify as the prefix; the following 5 characters are numeric. For example, if you specify an item ID prefix of ABC, items are created with item IDs starting from ABC00001 to ABC99999.

Note:

For postinstallation tasks for Teamcenter Automotive Edition-GM Overlay, refer to the *Teamcenter Rich Client Installation on Windows* and the *Teamcenter Rich Client Installation on Linux*.

Embedded Software Solutions for Foundation

In this step, you select settings for Embedded Software Solutions:

Install default software types

Select this option if you want to install the default Teamcenter item types that represent recognized embedded software parts and types.

Install default processor types

Select this option if you want to install the default Teamcenter item types that represent recognized processors.

For more information about configuring and using Embedded Software Solutions, see *Embedded Software Solutions*.

Hierarchical storage management (HSM) settings

In this step, you specify settings for third-party hierarchical storage management (HSM) software.

Value	Description
HSM Primary Hosts	Specify hosts on which third-party HSM software is installed. To add a host to the table, click **Add**. To remove a host from the table, select the host and click **Delete**.
Read Thru Supported by 3rd Party HSM Software	Specifies whether third-party HSM provides read-through capability.
HSM Secondary Tier Capacity (GB)	Specifies the capacity, in gigabytes, of the HSM storage volume.

Manufacturing Process Management options

In this step, you select Manufacturing Process Management types to include in your installation.

MATLAB client information

In this step, you specify settings for the MATLAB integration for the MBSE Integration Gateway.

Value	Description
MATLAB Installation Directory	Specifies the location where MATLAB is installed. This must be the directory containing the **bin** directory. This becomes the MATLAB root directory.
Staging Directory	Specifies the location where models downloaded from Teamcenter are stored, for example, **C:\StagingDir\MATLAB**.

NX Graphics Builder installation

In this step, you enter the location of the NX installation.

Value	Description
NX Install Location	Specifies the path to the NX installation.
Graphics Builder Base Port	Specifies the port used for the HTTP graphics builder server. Any free port is valid.

Value	Description
Number of Ports	Specifies the maximum number of graphics builder instances to be started.
Teamcenter 4-tier URL	Specifies the Teamcenter server URL.

OData microservice settings

In this step, you specify parameters to configure the open data (OData) microservice.

Value	Description
Teamcenter Web Tier URL	Specifies the URL to the Teamcenter web tier. Enter a value of the following form: **http://***host***:***port***/tc** For example: **http://myHost:7001/tc**
Teamcenter FMS URL	Specifies the URL to the File Management System (FMS) master.

Configuring Content Management for rich client

In this step, you identify Content Management web servers you want to access from this rich client host. Click **Add** or **Remove** to add or remove server URLs from the table.

> Note:
>
> If your network uses IPv6 (128-bit) addresses, use the hostname in URIs and do not use the literal addresses, so the domain name system (DNS) can determine which IP address should be used.

iModel (CALM) bank microservice settings

In this step, you specify settings for the iModel bank microservice.

In the **Teamcenter Web Tier URL** box, type the URL to the Teamcenter web tier, using the form:

http://*host***:***port***/tc**

For example:

http://myHost:7001/tc

CALM utility settings

In this step, you specify settings for the Capital Asset Lifecycle Management (CALM) utilities.

For more information about the CALM solution, see the Active Workspace documentation.

Value	Description
COMOS Base URL	Specifies the URL to the COMOS server, using the form: **http://***host*.*network*:*port*
Teamcenter Web Tier URL	Specifies the URL to the Teamcenter web tier. Enter a value of the following form: **http://***host*:*port***/tc** For example: **http://myHost:7001/tc**
FSC URL	Specifies the URL to the FMS server cache (FSC).

SCM ClearCase for rich client

This panel verifies the required version of the ClearCase client is installed on this rich client host.

Java EE-based lifecycle interoperability web services

In this step, you specify the four-tier server URL and the lifecycle interoperability web services (LIS) core service port.

Value	Description
4-Tier Server URL	Specifies the URL to the Teamcenter four-tier server.
LIS Core Service Port	Specifies the number of the port on which the LIS core service listens.
Is SSO Enabled	Specifies whether to enable Security Services for LIS web services.

Value	Description
SSO Login Service URL	Specifies the URL to the Security Services login service.
SSO Application ID	Specifies the application ID of the Security Services login service.

23. Updates Manager

About Updates Manager actions in TEM

The following TEM help topics describe panels displayed by Updates Manager, a TEM feature that applies downloaded patches to Teamcenter.

For more information about applying patches using Updates Manager, see the appropriate server installation guide (for Windows or Linux).

Media verification

In this step, you verify locations of Teamcenter software.

TEM displays this panel if a problem is found with one of the media locations provided. If the Teamcenter software files are corrupt or not found, or if an update is missing from one of the specified locations, you must correct the locations or replace the files in the specified location.

Value	Description
Update Location	Specifies locations of software kits for Teamcenter product updates (minor releases and patches). If the **Exists** column indicates a problem with an update location (**X**), click **Browse** and then re-enter the location. If the location is correct but the **Exists** column still indicates a problem, re-expand the given software kit to replace the files in the location.

> Note:
>
> TEM applies updates in the order you specify. If updates contain different versions of the same software component, the update closest to the bottom of the list takes precedence.

Configuration enhancements

In this step, you review configuration enhancements provided in the Teamcenter product update (minor release or patch).

For some Teamcenter features in your installation, template updates are required. To view information about configuration enhancements that affect your installation, click **View Enhancement Info** for each feature.

Select the **Accept Data Model Updates** check box to verify you understand and accept the data model updates included in the enhancements.

> Warning:
>
> Features containing data model objects may be updated. That is, database model changes may occur. Siemens Digital Industries Software recommends you back up your database before continuing.

Updates Manager

In this step, you choose whether to download or apply updates.

Updates Manager is the TEM function that applies downloaded patches to Teamcenter.

Removing backup files

In this step, you may choose to remove backups of files replaced by patches you applied previously.

Choosing a patch to apply

In this step, you choose a patch to apply to your Teamcenter installation.

Prerequisites:

- Download patch files from Support Center.

In the **Download Directory** box, enter the path to the directory in which you downloaded Teamcenter patches. In the **File** box, enter the name of the update file that contains the patch you want to apply.

Choosing an update to apply

In this step, you choose an update to apply to your Teamcenter installation.

Prerequisites:

- Download update files from Support Center.

In the **Download Directory** box, enter the path to the directory that contains the update file you downloaded. In the **Update List** box, select one or more updates to apply.

To view the readme file for the update, click **View README**.

Supplying information about the updates server

In this step, you provide FTP access information for the server on which you post downloaded Teamcenter updates.

Value	Description
Host	Specifies the host name of the updates server.
Port	Specifies the port used by the updates server.
User	Specifies the user name to use when accessing the updates server.
Password	Specifies the password to use when accessing the updates server.
Directory on FTP where updates are located	Specifies the FTP path on the updates server for transferring updates.
Path can be browsed	Specifies whether the FTP directory on the updates server can be browsed.

Applying updates

In this step, you specify the locations TEM requires to apply updates.

Value	Description
Update kit location	Specifies the directory that contains the downloaded Teamcenter update files you want to apply to your Teamcenter installation.
Backup directory	Specifies the directory you want to contain backups of files replaced during the update process.
Base Media Location	Specifies the the location of the Teamcenter release software kit.
Install Directory	Specifies the Teamcenter application root directory (*TC_ROOT*).

For more information about applying Teamcenter updates, see the appropriate Teamcenter server installation guide (for Windows or Linux).

Cache regeneration settings

In this step, you specify whether to regenerate server-side caches during patching. If you want to regenerate server caches during patching, select the **Regenerate Client Cache** check box.

Enable database changes

In this step, you supply database credentials to allow changes to the database that are required to complete the patch.

Value	Description
Database User	Specifies the user ID of the Teamcenter database user.
Database User Password	Specifies the password of the Teamcenter database user account.
Use database system user	If TEM does not already have the database system user credentials, select this check box and enter the credentials in the following boxes. Database system user credentials are required because the database changes require **CREATE SEQUENCE** and **CREATE TRIGGER** permissions.
System User	Specifies the user ID of the database system user.
System User Password	Specifies the password for the database system user account.

Enable new capabilities

In this step, you confirm whether to enable new capabilities added by the current Teamcenter software update kit.

To enable the new capabilities listed, click **Next**. Otherwise, click **Back** to choose a different maintenance option, or click **Cancel** to cancel installation of the update.

For information about the new capabilities listed, see the *What's New* section of the release **README** file.

24. Upgrade

Prerequisite diagnostics

This panel performs a series of diagnostics on your existing Teamcenter installation to assess readiness for update.

In the **Enter a working directory where logs can be created** box, enter a location where TEM can create log files for prerequisite diagnostics.

Click **Run** to begin diagnostics.

> Note:
>
> No Teamcenter data is modified in this step. No installation or update processes are initiated.

When the diagnostics are complete, this panel displays the results of the diagnostics. To view a detailed log of these results, click **Review**.

If any diagnostics fail, you must resolve those issues before you can proceed.

Warnings from diagnostic tests

This panel is displayed because one or more warnings occurred during pre-upgrade diagnostics. Review the warnings and any recommended actions, and acknowledge each warning by selecting each check box before you continue.

Custom database template

In this step, you enter a template file name. Any items found in the database which are not part of the default templates will be written out into this custom template file.

Value	Description
Template	Type a name for a new custom template that will be used to store the extra items.

Type collision verification

In this step, you specify your current version of Teamcenter for the type collision verification analysis performed during pre-upgrade diagnostics.

Type collisions occur when two or more types (business objects) have the same name. This duplication causes a conflict (collision), requiring that one of the identical names be changed. If your database has defined custom type names that are the same as any type that will be added by Teamcenter during this upgrade, your database cannot be upgraded.

In the **Current Release** box, select your current Teamcenter version, and then click the **OK** button to return to the **Pre-Upgrade Diagnostics** panel.

> Warning:
>
> It is very important that you select the exact version and patch level of your database. Do not guess or select a release that is close to the release. Doing so can cause an incorrect analysis.

TEM performs the type analysis during pre-upgrade diagnostics. If TEM detects a type collision, the upgrade is blocked from proceeding. The results of the type collision analysis are placed in the log directory.

> Note:
>
> If you do not see your Teamcenter version listed in the **Current Release** box, contact your Siemens Digital Industries Software customer support representative.

Upgrading workflow objects

In this step, you specify how to handle workflow objects during Teamcenter upgrade:

- **Upgrade all workflow jobs**

  Select this option if you want to convert all file-based workflow templates to database workflow template objects, convert any transient objects associated with the workflow templates to persistent objects, and update the referencing workflow processes.

- **Upgrade in-process jobs only**

  Select this option if you want to convert only those workflow objects that are in process.

For more information about configuring and using workflows, see the *Teamcenter Administration* guide.

Identify the Teamcenter configuration

In this step, you type a unique ID and optional description for the Teamcenter configuration.

Additional upgrade options

In this step, you specify additional Teamcenter upgrade options.

If you want to generate a client cache, select the **Generate client cache** check box.

This specifies that you want to generate a cache of data that rich clients can download once at initial logon and then reuse on the client host. This option reduces server demand, reduces startup time, and improves overall performance. When this option is selected, TEM generates the client cache at the end of the install, upgrade, or update action. If you clear this option, but a client cache already exists, the old client cache is deleted.

Database daemons port check

This panel verifies the port specified for database daemons is available.

Reporting and Analytics upgrade

In this step, you choose how you want to upgrade your Reporting and Analytics installation.

- **Upgrade metadata**

  Upgrade metadata from previous installation.

- **Upgrade WAR**

  Upgrade the Reporting and Analytics WAR file from the previous installation.

- **Upgrade WAR and metadata**

  Upgrade the WAR file and metadata from the previous installation.

- **Upgrade metadata and create new WAR**

  Upgrade the metadata and create a new Reporting and Analytics WAR file.

Repeatable Digital Validation database user

In this step, you provide information needed to access the Repeatable Digital Validation (RDV) database.

Value	Description
User	Specifies the user name of the RDV database user.
Password	Specifies the password for the RDV database user.

Selecting a Teamcenter configuration to upgrade

In this step, you select the Teamcenter configuration to upgrade, or accept the default selection if a single configuration is available.

New application root directory

In this step, you specify the root directory for your upgraded Teamcenter installation. In the **New Application Root Directory**, enter the root directory for the upgraded Teamcenter installation.

This panel contains a table of all features found in the existing installation, with the current status of each. Click **Browse** to add any custom templates missing from the table.

Old application root

In this step, you specify the location of your previous Teamcenter installation.

Test environment location

In this step, you specify a location in which to create the copy of your production environment.

> Note:
>
> TEM does not prompt you to select features when creating a copy of an environment for testing. The features installed in the test environment are based on the feature data models that are installed in the database. You can add additional features after the copy process is complete.

Verifying templates and features for the test environment

In this step, you locate features associated with templates applied to the database in a copy of a production environment you create for upgrade testing.

TEM displays this panel if you select **Create environment for upgrade testing** in the **Install/Upgrade Options** panel.

The table shows features being applied to the database for the copy of the production environment. If a feature is not shown for a given template, click **Browse** to locate the associated feature XML file.

> Caution:
>
> This panel does not verify template versions. Make sure the template and feature versions are correct before you continue.

Upgrade information

In this step, you enter information to upgrade your existing installation. When you click the **Next** button, TEM attempts to connect to the database and get all volume information from it. TEM also verifies you have write permission on each local volume folder. This can take up to several minutes.

Value	Description
Old TC_DATA Location	Enter the path of the *TC_DATA* location on the server to be upgraded.
New TC_DATA Location	Enter the new path you want to use for the upgraded *TC_DATA* location on the server.
Database User	Enter the user name of a user with DBA privileges on the server.
Database Password	Enter the password for the user. Caution: The password must not be empty nor contain any whitespace characters such as space, tab, newline, carriage return, form feed, or vertical tab. Make sure the password does not contain space characters or any of the following characters: **! @ $ % ' " : ; . < > ( ) { }**

Upgrade database features

In this step, you provide paths to templates that need to be upgraded.

This panel provides a list of templates provided by Siemens Digital Industries Software and our partners. Any template showing **Upgrade** in the status column has been detected in this database and must be upgraded. If a template was detected and the path to the template is missing, use the **Browse** button to find the missing template package. After all matched template packages are found, the **Next** button is enabled.

Warning:

Failure to find all missing template packages results in migration issues with your custom data model to the Business Modeler IDE, possible corruption of data, and issues with using TEM.

Value	Description
Browse	Click this button to locate paths to the packaged template ZIP files.

Volume Migration

In this step, you determine where to create the volumes associated with the database for the test environment.

Ownership of all volumes is transferred to the target system as part of the copy process. By default, TEM creates volumes in the path specified in the **Default volume directory path**.

If you want to specify a location for a given volume, enter the path in the **Copied Volume Path** box for the volume. The **Copied Volume Path** value for a volume must be unique. (No other volume may use this location.) The **Copied Volume Path** value can point to a volume directory, a partial volume directory, or an empty directory. TEM creates whatever subdirectories are missing. The originating host name of the volume is used in the default volume location. This is done in the case two volumes originating from different servers use the same path.