



# **PTC Windchill® Basic Administration Guide**

**PTC Windchill 11.0 F000**

---

**Copyright © 2015 PTC Inc. and/or Its Subsidiary Companies. All Rights Reserved.**

User and training guides and related documentation from PTC Inc. and its subsidiary companies (collectively "PTC") are subject to the copyright laws of the United States and other countries and are provided under a license agreement that restricts copying, disclosure, and use of such documentation. PTC hereby grants to the licensed software user the right to make copies in printed form of this documentation if provided on software media, but only for internal/personal use and in accordance with the license agreement under which the applicable software is licensed. Any copy made shall include the PTC copyright notice and any other proprietary notice provided by PTC. Training materials may not be copied without the express written consent of PTC. This documentation may not be disclosed, transferred, modified, or reduced to any form, including electronic media, or transmitted or made publicly available by any means without the prior written consent of PTC and no authorization is granted to make copies for such purposes.

Information described herein is furnished for general information only, is subject to change without notice, and should not be construed as a warranty or commitment by PTC. PTC assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

The software described in this document is provided under written license agreement, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. It may not be copied or distributed in any form or medium, disclosed to third parties, or used in any manner not provided for in the software licenses agreement except with written prior approval from PTC.

UNAUTHORIZED USE OF SOFTWARE OR ITS DOCUMENTATION CAN RESULT IN CIVIL DAMAGES AND CRIMINAL PROSECUTION. PTC regards software piracy as the crime it is, and we view offenders accordingly. We do not tolerate the piracy of PTC software products, and we pursue (both civilly and criminally) those who do so using all legal means available, including public and private surveillance resources. As part of these efforts, PTC uses data monitoring and scouring technologies to obtain and transmit data on users of illegal copies of our software. This data collection is not performed on users of legally licensed software from PTC and its authorized distributors. If you are using an illegal copy of our software and do not consent to the collection and transmission of such data (including to the United States), cease using the illegal version, and contact PTC to obtain a legally licensed copy.

**Important Copyright, Trademark, Patent, and Licensing Information:** See the About Box, or copyright notice, of your PTC software.

**UNITED STATES GOVERNMENT RESTRICTED RIGHTS LEGEND**

This document and the software described herein are Commercial Computer Documentation and Software, pursuant to FAR 12.212(a)-(b) (OCT'95) or DFARS 227.7202-1(a) and 227.7202-3(a) (JUN'95), and are provided to the US Government under a limited commercial license only. For procurements predating the above clauses, use, duplication, or disclosure by the Government is subject to the restrictions set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software Clause at DFARS 252.227-7013 (OCT'88) or Commercial Computer Software-Restricted Rights at FAR 52.227-19(c)(1)-(2) (JUN'87), as applicable. 01012015

**PTC Inc., 140 Kendrick Street, Needham, MA 02494 USA**

# Contents

About This Guide .....	7
Getting Started with Windchill Administration.....	11
Administering Windchill Solutions—an Introduction .....	12
Logging On as the Administrator .....	15
Working With the Initial Organization Context.....	19
Establishing Administrators .....	20
Establishing End Users .....	25
The Next Steps.....	27
Administration Overview .....	29
Your Installed Windchill Architecture.....	30
Your Installed Windchill Environment.....	30
Managing Your System .....	32
Managing User Access to Data.....	34
Managing Users .....	45
Managing Data.....	47
Managing Windchill Processes .....	52
Managing User Collaboration .....	57
Additional Administrative Groups .....	57
Post-Installation Activities.....	58
Contexts – Distributed and Hierarchical Administration.....	59
Contexts—An Administrative Overview .....	60
Context Administrative Items .....	61
Creating the Contexts from which Users Work .....	84
Administering Domains and Policies.....	86
Administering the Numbering of Parts, Documents, CAD Documents, Managed Baselines, and Change Objects.....	104
Administering the Versioning of Parts, Documents, and CAD Documents.....	105
Administering Preferences .....	107
Best Practices for Monitoring and Maintenance .....	111
Understanding the Site .....	113
Site Administration Overview .....	114
Typical Duties of Site Administrators .....	114
Out-of-the-Box Site Configuration .....	131
Site Administration Best Practices.....	131
Understanding Organizations.....	137
Organization Administration Overview.....	138
Typical Duties of Organization Administrators .....	139
Out-of-the-box Organization Templates .....	147

---

Creating an Organization Context .....	155
Owning Organization Participants .....	158
Using the Organization Utilities Page .....	161
Changing an Established Internet Domain .....	162
Using the OrganizationSync Utility for User Organization Changes .....	162
Best Practices .....	164
Understanding Products and Libraries .....	171
Overview .....	172
Typical Duties of Product and Library Administrators .....	172
Creating a Product .....	179
Creating a Library .....	179
Administering Teams .....	180
Using the Product and Library Utilities Page .....	182
Out-of-the-box Product and Library Context Templates .....	182
Configuring Products or Libraries for Dynamic Documents .....	224
Configuring Part and Document Relationships .....	225
Best Practices for Object Initialization Rules .....	231
Understanding Projects and Programs .....	233
Project and Program Administration Overview .....	234
Typical Duties of Project and Program Managers .....	235
Out-of-the-box Project and Program Templates .....	241
Configuring Part and Document Relationships .....	244
Understanding Participants (Users, Groups, and Organizations) .....	251
Overview of Windchill Participants .....	252
Working with LDAP Directory Services .....	255
Using the Participant Administration Utility .....	265
Windchill Participant Status .....	282
Participant (Users, Groups, and Organizations) Identification .....	285
Best Practices for Assigning Domains to Participants .....	285
Receiving Administrative Notifications .....	287
Managing the Participant Cache .....	287
Maintaining the Connections between Participant Objects and their Directory Server Entries .....	289
Registering a non-Windchill User .....	290
Profile Management .....	291
Teams and Team Template Administration .....	297
Overview .....	298
Context Teams .....	298
Shared Teams .....	298
Understanding Life Cycles .....	299
The Life Cycle Model .....	300
Basic and Advanced Life Cycles .....	301
Managing Life Cycle Processes .....	303
Accessing the Life Cycle Template Administration Utility .....	305
Out-of-the-box Life Cycle Templates .....	306

---

Working with Life Cycle Templates .....	310
Promotion Process .....	326
Overriding and Reassigning Life Cycle and Team Templates.....	329
Defining Additional Life Cycle States .....	330
Access Control for Life Cycle Administration .....	330
Best Practices .....	330
Understanding Workflow .....	337
Overview.....	338
Managing Workflow Security .....	340
Workflow Version Control .....	343
Using the Workflow Template Editor.....	344
Exporting and Importing Workflow Templates Across Releases.....	354
Process Manager Toolbar Access Control .....	355
Using PDF Forms as Task Templates .....	356
Viewing Workflow History .....	356
Workflow Instance States .....	363
Out-of-the-Box Workflow Templates .....	364
Workflow Template Execution Flags .....	375
Electronic Signatures .....	384
Best Practices .....	387
Understanding Context Templates .....	393
Out-of-the-box Context Templates.....	394
Methods of Creating Additional Context Templates.....	394
Creating Business XML Files for Context Templates.....	396
Required Contents of Files Used to Create a Context Template.....	396
ZIP File Contents of an Exported Context Template.....	398
Required Contents of ZIP File Used for Importing a Context Template .....	399
Managing Context Templates .....	401



## About This Guide

The *PTC Windchill Basic Administration Guide* is a collection of administrative reference topics from the **Basic Administration** section of the PTC Windchill Help Center and serves as a reference guide for Windchill business and application administrators. This guide can be used with all PTC Windchill solutions.

The following table illustrates the responsibilities and skills of administrators:

	<b>Administrator</b>
Responsibilities	Configuring the system (see <i>PTC Windchill Administration - Configuring Your PTC Windchill Environment</i> ) Maintaining a running system (see <i>PTC Windchill Specialized Administration Guide</i> ) Interfacing with other systems (see <i>PTC Windchill Enterprise Administration Guide</i> ) Administering PTC Windchill applications (see this guide)
Skills	Understanding PTC Windchill server and client, HTML, HTTP, and database.

## Related Documentation

Many of the sections in this guide have additional help topics available in the PTC Windchill Help Center.

Documentation from the following areas is available only from the PTC Windchill Help Center:

- Administering Views
- Managing Data Security

- 
- Calendar
  - Team Template Administration
  - PTC Windchill License Groups

The following guides are also available and may be helpful:

- *PTC Windchill Specialized Administration Guide*
- *PTC Windchill Enterprise Administration Guide*
- *PTC Windchill Administration - Configuring Your PTC Windchill Environment*

## Technical Support

Contact PTC Technical Support through the PTC website, or by phone, email, or fax if you encounter problems using this product or the product documentation. The PTC eSupport portal provides the resources and tools to support your PTC Windchill implementation:

<https://support.ptc.com/appserver/cs/portal/>


For complete details, see the *PTC Customer Support Guide*:

<http://support.ptc.com/appserver/support/csguide/csguide.jsp>

You must have a Service Contract Number (SCN) before you can receive technical support. If you do not know your SCN, see “Preparing to contact TS” on the **Processes** tab of the *PTC Customer Support Guide* for information about how to locate it.

## Documentation for PTC Products

You can access PTC documentation using the following resources:

- **PTC Windchill Help Center**—The PTC Windchill Help Center includes all PTC Windchill documentation. You can browse the entire documentation set, or use the search capability to perform a keyword search. To access the PTC Windchill Help Center, you can:
  - Click any help icon  in PTC Windchill
  - Select **Help** ► **Windchill Help Center** from the **Quick Links** menu at the top right of any PTC Windchill page
  - Use the following link to access all PTC help centers:  
<https://support.ptc.com/appserver/cs/help/help.jsp>
- **Reference Documents** website—The Reference Documents website is a library of all PTC guides:  
<http://support.ptc.com/appserver/cs/doc/refdoc.jsp>



---


A Service Contract Number (SCN) is required to access the PTC documentation from the Reference Documents website. If you do not know your SCN, see “Preparing to contact TS” on the **Processes** tab of the *PTC Customer Support Guide* for information about how to locate it:

<http://support.ptc.com/appserver/support/csguide/csguide.jsp>

When you enter a keyword in the **Search Our Knowledge** field on the PTC eSupport portal, your search results include both knowledge base articles and PDF guides.

## Comments

PTC welcomes your suggestions and comments on its documentation. To submit your feedback, you can:

- Send an email to [documentation@ptc.com](mailto:documentation@ptc.com). To help us more quickly address your concern, include the name of the PTC product and its release number with your comments. If your comments are about a specific help topic or book, include the title.
- Click the feedback icon  in the PTC Windchill Help Center toolbar and complete the feedback form. The title of the help topic you were viewing when you clicked the icon is automatically included with your feedback.



# 1

## Getting Started with Windchill Administration

Administering Windchill Solutions—an Introduction .....	12
Logging On as the Administrator.....	15
Working With the Initial Organization Context .....	19
Establishing Administrators .....	20
Establishing End Users .....	25
The Next Steps .....	27

This section provides a road map for getting your Windchill solution set up so that it is usable as a test system. The section also provides some basic information about Windchill administrators and your Windchill environment.

PTC strongly recommends that all administrators read this section as well as the following sections in their entirety:

- [Administration Overview on page 29](#)
- [Contexts – Distributed and Hierarchical Administration on page 59](#)

Later sections assume that you are familiar with this information.

---

# Administering Windchill Solutions—an Introduction

This topic collection provides business administration information for the following Windchill solutions:

[Windchill PDMLink](#)

[Windchill ProjectLink](#)

[Pro/INTRALINK](#)

[Arbortext Content Manager](#)

[PTC Windchill PDM Essentials](#)

[Global Product Development Package I](#)

After a Windchill solution installation is complete, the following basic activities have been accomplished:

- A Web server and servlet engine are installed and configured.
- The Windchill database is installed and configured.
- Any administrative and enterprise directory services that are going to be used are configured.
- The Windchill solution and Windchill Help Center are installed and have been started.

If you want more information about these activities, see the *PTC Windchill Installation and Configuration Guide*.

Before you can get started with administrative activities in your Windchill solution, you must log on as the administrator (defined during the installation). Additionally, you may also need to create a context for the installed default organization and establish additional administrators.

The next topics in this section describe how to log on, work with the initial organization context, and establish additional administrators. The last topic provides a guide to which additional sections you may want to read next.

## Regarding Arbortext Content Manager

The general information and information specific to Windchill PDMLink (products and libraries) is relevant to Arbortext Content Manager administrators.

As parts and CAD documents are not supported in Arbortext Content Manager, disregard references to those objects. References to "Arbortext" or "Arbortext products" refer to the Arbortext Editor and Arbortext Publishing Engine, not the Arbortext Content Manager solution.

---

## Regarding Pro/INTRALINK

Pro/INTRALINK 11.0 is a powerful enhancement to the robust PDM functionality of Pro/INTRALINK 3.4. Additionally, Pro/INTRALINK 11.0 uses PDM capabilities to manage CAD documents and documents and includes many of the functions and features of Windchill PDMLink. However, Pro/INTRALINK 11.0 does not support parts (WTParts), change objects, and dynamic documents.

The general information and information specific to Windchill PDMLink (products and libraries) is relevant to Pro/INTRALINK administrators. However, as parts, change objects, and dynamic documents are not supported in Pro/INTRALINK, disregard references to those objects.

## Regarding PTC Windchill PDM Essentials

The general information and information specific to Windchill PDMLink (products and libraries) is relevant to PTC Windchill PDM Essentials administrators.

As parts (WTParts) and dynamic documents are not supported in PTC Windchill PDM Essentials, disregard references to those objects.

### Overview

PTC Windchill PDM Essentials is a preconfigured, packaged solution designed for rapid, small deployments by customers with basic MCAD data management needs. The package contains everything needed for basic CAD data management except the operating system (OS).

### Summary

- Microsoft SQL Server 2014 is bundled with PTC Windchill PDM Essentials and is automatically installed and configured. This bundled SQL server version is licensed with, and can be used only with PTC Windchill PDM Essentials.
- The following Windchill capabilities are included and preconfigured in PTC Windchill PDM Essentials:
  - Support for managing Creo Parametric CAD documents
  - Support for managing documents (PDF, Word, Excel, PowerPoint, TXT)
  - Server-side representation publishing and client-side viewing
    - ◆ Creo View Lite is included for client 3-D viewing and markup.
    - ◆ Creo Parametric CAD worker, publishing adapter, and the associated license are included and automatically configured for publishing
  - Windchill Directory Server (for managing users)
  - The following Windchill Workgroup Manager products are bundled and installed on the server and available for client deployment.

- 
- ◆ Windchill Workgroup Manager for Creo Illustrate
  - ◆ Windchill Workgroup Manager for Creo Schematics
  - ◆ Windchill Workgroup Manager for Creo Elements/Direct Drafting
  - ◆ Windchill Workgroup Manager for Creo Elements/Direct Modeling
  - ◆ Windchill Workgroup Manager for AutoCAD
  - ◆ Windchill Workgroup Manager for Autodesk Inventor
  - ◆ Windchill Workgroup Manager for SolidWorks
  - ◆ Windchill Workgroup Manager for Mathcad
  - ◆ Windchill Workgroup Manager for Arbortext IsoDraw
- The following Windchill capabilities are excluded:
    - No support for parts (WTParts), part configurations, or advanced configuration options (only CAD documents and documents, such as Microsoft Word or text documents, are supported).

---

 **Note**

WTParts are Windchill parts. CAD data for Creo Parametric parts and SolidWorks parts is managed in Windchill as CAD documents.

---

- No support for content replication
- No support for change objects
- No support for indexed content search (Windchill Solr is not installed)

---

 **Note**

Attribute search is supported.

---

## Regarding Global Product Development Package I

The general information and information specific to Windchill PDMLink (products and libraries) is relevant to PTC Windchill PDM Essentials administrators.

As parts (WTParts) and dynamic documents are not supported in Global Product Development Package I, disregard references to those objects.

---

## Overview

PTC Global Product Development Package I is a foundational solution for PDM and MCAD data management. The package contains everything needed for Multi-MCAD data management, document management, publishing, and visualization. It includes the following features:

- Replication to provide high-performance design collaboration among distributed global teams
- Support for integrations with all Creo Parametric applications, Mathcad, AutoCAD, Autodesk Inventor, SolidWorks, and NX
- Visualization, validation, and review capabilities with Creo View Lite and all the Creo View adapters for publishing formats from Creo Parametric applications, SolidWorks, Autodesk Inventor, AutoCAD, and NX

PTC Global Product Development Package I does not include support for parts, changes, packages, or security labels and agreements but is extensible in that Windchill modules that do not require parts, such as ProjectLink and additional MCAD workgroup managers, can be added.

## Logging On as the Administrator

You can access your Windchill solution using a URL from a Web browser.

---

### Note

The server manager, method server, and web server must be running before Windchill can be accessed.

---

The URL string is formatted as follows:

```
http://<hostname>:<port>/<webapp>
```

The required parameters were defined when your Windchill solution was installed. You only need to include the port number when the Web server being used is using a port number other than 80 (default).

If the web server is using the default port, then you can enter `http://<hostname>/<webapp>` in your web browser's **Address** (or **Location**) text box. For example, if you specified Windchill for the `<webapp>` parameter, then the following URL entered in the Web browser **Address** text box opens the Windchill home page:

```
http://<hostname>/Windchill
```

---

 **Tip**

If you are logging on using the same system where your solution is installed, you can use `localhost` as `<hostname>`.

---

 **Note**

If your system was configured with SSL, then the URL used to access Windchill uses the `https` prefix, rather than `http`.

---

Use the administrative user defined during the installation to log on. This user is a member of the Administrators group and has out-of-the box privileges that give you full control over all Windchill objects.

After you log on, you are initially presented with a welcome page that highlights the main features of Windchill. This welcome page displays each time you log on, unless you select the **Do not show this page upon startup** checkbox. You can view the welcome page at any time by selecting **Quick Links** ► **Help** ► **Welcome to Windchill**.

---

 **Best Practice**




If you want to use a site administrator to manage Windchill, you should create a second site administrator for these tasks to improve Windchill performance. For more information, see [Establishing Site Administrators on page 132](#).

---







---


## Home Page

Click the home  icon in the upper left corner to view your **Home**  page. The **Home**  page is where users manage their daily work.

---

### Note

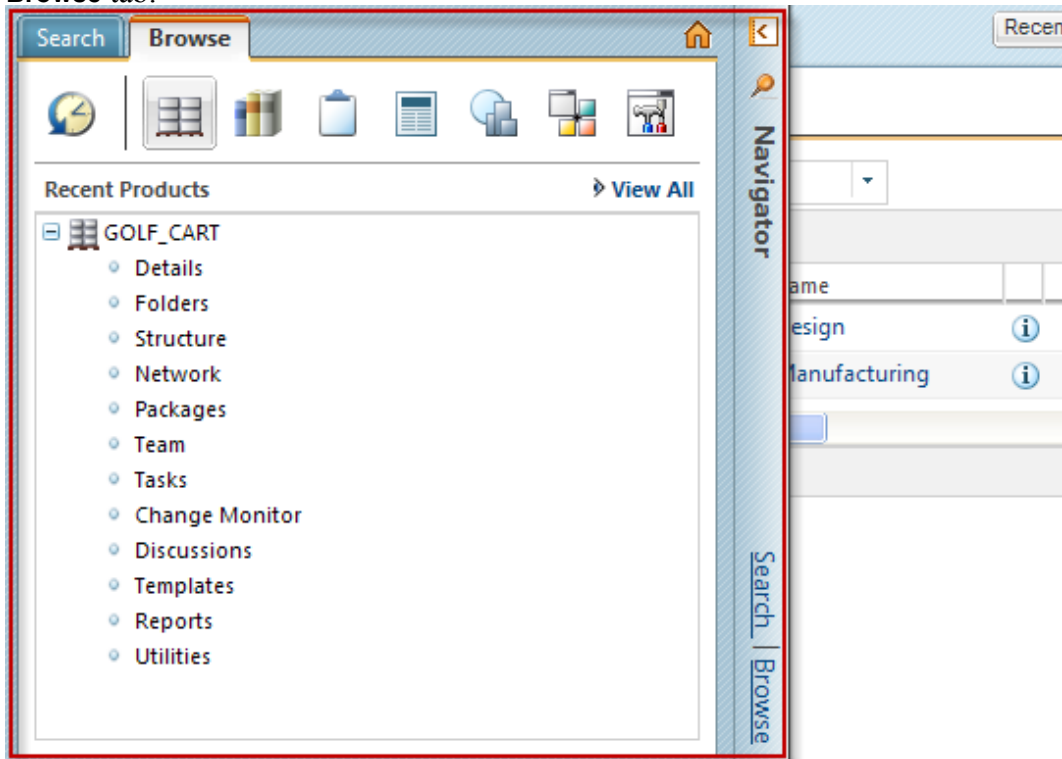
While individual users can each have their own customized **Home**  page, all site administrators share a single customized **Home**  page. The site administrator's **Home**  page is displayed for all users who have not yet customized their individual **Home**  page.

For information on customizing the **Home**  page, see the Setting Up Your Environment topics in the Windchill Help Center.

---

## Navigator












The **Navigator** on the left side of the page contains two tabs: the **Search** tab and the **Browse** tab.



The **Search** tab allows you to search for objects in Windchill by entering your own advanced search parameters or by using a saved or historic search. For more information on searching in Windchill, see the Searching for Information topics in the Windchill Help Center.

---

The **Browse** tab allows you to navigate to various contexts for which you have access, such as projects, products, or organizations. The contexts available in the **Browse** tab depend on which products you have installed at your site, and include the following:

- **Site** —Provides site administrators access to configure and manage the Windchill system as a whole. **Site**  is visible only to site administrators and is the context from which the initial administration activities are done.
- **Organizations** —Provides site and organization administrators access to manage organization contexts, including creating new organizations (site administrators only), managing groups and roles, access control, object initialization rules, preferences, and templates. **Organizations**  is visible to site and organization administrators only.
- **Libraries** —Provides users access to all libraries of which they are a member. In a library, team members can store and provide access to business information (such as in a document library) or can store and provide access to objects that are not related to a single product (such as in a common parts library). There are no out-of-the-box libraries. (Windchill PDMLink, Arbortext Content Manager, Pro/INTRALINK only)
- **Changes** —Provides users access to all change objects for contexts of which they are a member. (Windchill PDMLink, or Windchill ProjectLink installed with Windchill PDMLink only)
- **Projects** —Provides users access to all projects of which they are a member. For each project, team members have access to the project information, project schedule, resources, and plan details. There are no out-of-the-box projects. (Windchill ProjectLink only)
- **Programs** —Provides users access to all programs of which they are a member. A program is used to collect and manage the planning and execution of a set of projects. A program can be used solely as a means for organizing projects, or it can contain a plan, documents, and teams. There are no out-of-the-box programs. **Programs**  is visible only if programs have been enabled at your site. (Windchill ProjectLink only)
- **Products** —Provides users access to all products of which they are a member. For each product, team members manage all of the information that is relevant to the design, manufacture, and support of a product. When only base data is installed, there are no out-of-the-box products. (Windchill PDMLink, Arbortext Content Manager, Pro/INTRALINK only)
- **Recently Visited** —Displays your recently accessed contexts and workspaces.



Click anywhere on the **Navigator** bar to expand or collapse it. Click the **Search** or **Browse** links to open the **Navigator** to that tab.

---

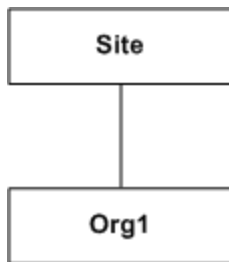
## Working With the Initial Organization Context

Your Windchill environment consists of a set of containers that hold all of the administrative areas (known as domains), rules, and data that make up the context from which Windchill users work. Although the underlying code refers to containers, the term **Context** is used throughout the user interface to identify where in the framework specific rules, domains, and data reside. Since **Context** is the label you see in the interface, this topic collection uses the term context (rather than container) so you can make the connection with the user interface. Unless you are working with the code, you can assume that context and container refer to the same thing.

The contexts are set up in a hierarchy so that the rules and data created in one context can be available to child contexts and the domains in one context can have child domains in a child context. The child domains inherit information from ancestor domains.

After installation, every Windchill solution has an installed top-level site context, and an initial organization context. Site context activities are performed from **Site** ; organization context activities are performed from **Organizations** .

The organization context is a child of the site context. The context name of the initial organization context is the organization name that was entered during installation. For example, assume that the organization name is Org1, then the following context hierarchy is established:



In this example, the Org1 organization context inherits rules and data from the site context.

Both the site and the initial organization contexts have the same owning organization participant (type WTOrganization). This becomes important if you want to segregate some of the objects created in an organization context from other contexts. The term participant is introduced here and used throughout Windchill as a way of categorizing Windchill objects that identify users, groups, and organizations. The organization participant created in the installation process becomes the owning organization for some of the objects created in both the site and the initial organization contexts. For example, subtypes are associated with

---

the owning organization. Therefore, any subtypes you create from within the initial organization context become site-level subtypes because the owning organization is the same.

To have subtypes created in an organization context that do not become available as site-level subtypes, the context from which the subtypes are created cannot be the initial organization context created during the installation.

---

 **Note**

With Windchill PDMLink, the installer can install demo data. As part of the demo data installation, the Demo organization context is created and the Demo user is created as the organization administrator. As is the case for all organization contexts, the Demo organization context inherits rules and data from the site context, but the Demo organization does not have the same owning organization as the site context or the initial organization context.

You can create additional organization contexts. PTC recommends that if you are considering using multiple organization contexts in the future, you should create at least one additional organization context in which to create your products, libraries, projects, or programs, rather than creating them within the initial organization context. This allows you to add additional organizations (participants and contexts) without having to restructure your administrative data so that members of one organization cannot see data from another organization.

You must set the organization administrator for each organization context. For more information on how to do this, see [Establishing Administrators on page 20](#).

For information about creating and using organization contexts, see [Organizations on page 137](#).

## Establishing Administrators

Before you attempt to use your Windchill solution, you should establish a minimum set of administrators for the solution. The types of administrators that are available are determined by the Windchill solutions that are installed.

The Administrators group is defined in every installed Windchill solution. Initially, the administrative user entered during installation (for example, wadmin) is the only member. Out of the box, the members of the Administrators group have full control over all Windchill objects and are commonly called the system or site administrators.

---

### **Best Practice**

If you want to use a site administrator to manage contexts or teams, you should create a second site administrator for these tasks to improve Windchill performance. For more information, see [Establishing Site Administrators on page 132](#).

---

The additional types of administrators available are:

- An organization administrator manages a specific organization.
- A product manager manages a specific product (for Windchill PDMLink, Arbortext Content Manager, Pro/INTRALINK).
- A library manager manages a specific library (for Windchill PDMLink, Arbortext Content Manager, Pro/INTRALINK).
- A project manager manages a specific project (for Windchill ProjectLink).
- A program manager manages a specific program (for Windchill ProjectLink).
- A shared team manager manages a specific shared team and has management privileges for any context using the shared team.



In the out-of-the-box configuration, there are two LDAP directory service nodes. Administrative users reside in the Administrative LDAP node. For more information about the LDAP services, see [Working with LDAP Directory Services on page 255](#).

---

### **Note**

For notification email messages to be sent, some mail servers require that a valid email address be specified in the **From** header of the email message. Windchill solutions use the `wt.mail.from` and `wt.notify.notificationSenderEmail` properties in the `wt.properties` file to populate the **From** header when sending email messages. Setting these properties to a valid Windchill user should have been done as a manual step after installing your solution. If this was not done, see the *PTC Windchill Installation and Configuration Guide* for details on how to set these properties to the email address of the Windchill administrator or some other authorized user.

---

The site administrative user (as defined by the **Administrators** group) can use the links that are under **Site**  and **Organizations** .

Selecting **Site**  ► **Administrators** displays the **Site Administrators** table. From this table, you can add users to the **Administrators** group.


---

Additionally, you can give system monitoring privileges to a group of Windchill users who are not in the **Administrators** group. By listing the user names of those users in the wt.util.jmx.AccessUtil.siteAdministrators property, the users have access to the **System Configuration Collector**, **Server Status**, and **Monitoring Tools** pages. These users should also be included in the JMX-Administrators list so that they automatically receive the JMX email notifications and the end user error report emails that are sent. For JMX-Administrators list and wt.util.jmx.AccessUtil.siteAdministrators property details, see the *PTC Windchill Specialized Administration Guide*

The following sections provide additional information about the administrators in each Windchill solution and describe how to add the administrators.

## Organization Administrators

An organization administrator manages a specific organization. Initially, there is no organization administrator defined for an organization context.

Select **Organizations**  ► **Administrators** to add one or more users as organization administrators to the organization. For more information, see [Creating Users to Select as Administrators on page 24](#).

## Windchill PDMLink Administrators

Additional Windchill PDMLink administrators include the following:

- A product manager for managing a specific product.

Initially, the product manager is the user who creates the product. Additional users can be added to the **Product Manager** role from the **Team** page of the product.

- A library manager for managing a specific library.

Initially, the library manager is the user who creates the library. Additional users can be added to the **Library Manager** role from the **Team** page of the library.



- A shared team manager for managing a specific shared team.

If a shared team is used in a product or library, then any users with the **Shared Team Manager** role act as product or library managers.

---

## Creating a Product or Library

To create a product or library, a user must be one of the following:

- The organization administrator.
- A member of the Product Creators group or the Library Creators group. These groups are maintained through the **Organizations**  **Creators** table. From the **Organizations**  **Creators** table, choose the type of creator from the table view drop-down list on the **Creators** table.


## Windchill ProjectLink Administrators

Additional Windchill ProjectLink administrators include the following:


- A project manager for managing a specific project.  
Initially, the project manager is the user who creates the project. Additional users can be added to the **Project Manager** role from the **Team** page of the project.
- A program manager for managing a specific program.  
Initially, the program manager is the user who creates the program. Additional users can be added to the **Program Manager** role from the **Team** page of the program.
- A shared team manager for managing a specific shared team.  
If a shared team is used in a project or program, then any users with the **Shared Team Manager** role act as project or program managers.

## Creating a Project or Program

To create a project or program, a user must be one of the following:

- The organization administrator.
- A member of the Project Creators group (to create a project).  
Depending on the setup options selected when an organization is created, all members of the organization who have logged in may be automatically added to the Project Creators group. If this behavior is not enabled, both the site administrator and the organization administrator of the current organization can add users to the Project Creators group. From **Organizations**  **Creators**, select the **Project Creators** view from the table view drop-down list. From this table you can add users.
- A member of the Program Creators group (to create a program).

---

Both the site administrator and the organization administrator of the current organization can add users to the Program Creators group. From **Organizations**  ► **Creators**, select the **Program Creators** view from the table view drop-down list. From this table you can add users.


## Creating Users to Select as Administrators

---

### Note

Only members of an organization can be organization administrators, product creators, library creators, project creators, or program creators.

---

In a production environment, users are usually defined in an enterprise directory that is set up during installation. If you are setting up a test system and do not have a set of users from which to select administrators, you can create a set of test users in the default directory service using the **Participant Administration** utility. The **Participant Administration** utility is available from **Site**  ► **Utilities**.

The Administrator user that is created during the installation (for example, wadmin) is not associated to a specific organization; this user does not have the organization attribute (usually “o”) set. Therefore, this user cannot be added as an organization administrator unless the Administrator user is updated to include the organization attribute. You can use the **Participant Administration** utility to update the Administrator user.

---

### Note

If your site does not use the organization attribute in the directory service entry, users can be assigned to an organization using the `usersOrganizationName` property. For more information on using this property, see *Configuring Additional Enterprise Directories* in the *PTC Windchill Installation and Configuration Guide*.

---

At a minimum, you need to either update the Administrator user so the user is a member of the default organization or create another user who can be the organization administrator. This user can then administer the organization and create products, libraries, projects, and programs.



---

### **Best Practice**

If you want to use a site administrator to manage organizations, you should create a second site administrator for these tasks to improve Windchill performance. For more information, see [Establishing Site Administrators on page 132](#).

---

## Establishing End Users

Depending upon how your Windchill solution was set up during installation, end users (users that do not have administrative privileges) are managed in one of two ways:

- [Using an Enterprise Directory Service on page 26](#)
- [Using the Participant Administrator Utility on page 26](#)

Windchill uses both the Windchill database and a directory service when creating users. For each user, there is an entry in a directory service and a Windchill object stored in the database.

In the out-of-the-box configuration, there are two LDAP directory services: the Administrative LDAP service and the Enterprise LDAP service. End users can reside in either service; although typically, the Administrative LDAP service should be used for administrative users and enterprise LDAP service should be used for all end users who are not administrators. For more information about the LDAP services, see [Working with LDAP Directory Services on page 255](#).

It is not required that end users be associated with an organization; however, categorizing users by organization provides an additional way in which you can identify a set of users. Windchill manages Windchill objects within each organization context and users affiliated with an organization can be given access to objects created from within an organization context.

---

### **Note**

If your site does not use the organization attribute in the directory service entry, users can be assigned to an organization using the `usersOrganizationName` property. For more information on using this property, see *Configuring Additional Enterprise Directories in the PTC Windchill Installation and Configuration Guide*.

---

---

If you want to manage users based on license type, the View and Print Only license group is available. This group has an access control rule in place that restricts group members to be able to search for and view object information, download any attachments, and view markups. For more information, see About the View and Print Only License Group in the Access Control section of the *PTC Windchill Specialized Administration Guide*.



## Using an Enterprise Directory Service

Instead of using the Windchill Directory Server that is bundled with your Windchill solution for the end users in the Enterprise LDAP service, you can use an enterprise directory service such as the Microsoft Active Directory Service (ADS). Each enterprise directory service entry contains attributes for the user. For example, user entries can have attributes for the user's full name, email address, and organization.

The installation process can set up the enterprise directory service as the Enterprise LDAP node. If this was not done, an additional directory service can be established that uses the enterprise directory service. For information about setting up enterprise directory services, see the *PTC Windchill Installation and Configuration Guide*.

Usually, users in an enterprise directory service are managed through a third party tool and the Windchill user database object is created automatically the first time the user logs into the Windchill solution.

## Using the Participant Administration Utility

The **Participant Administration** utility can be used to manage end users. The utility can be accessed from **Site**  **Utilities** and **Organizations**  **Utilities**. Both the LDAP entry and the Windchill user database object are created when a user is created from the Participant Administration utility.


End users can be added to the Windchill solution by either a site or an organization administrator using the **Participant Administration** utility. To create a new user, you must have write permission to the directory service in which you want the user directory entry to reside.

When you create a new user from **Site** , you can associate that user with any existing organization within the Windchill solution. When you create a new user from **Organizations** , the user is automatically associated with the organization from which the **Participant Administration** utility was launched.

When adding a new user in the **Participant Administration** utility, you can associate that user with a group and a profile. Groups can be created from either the **Participant Administration** utility or from the **Groups** link within the active organization context.

---

### **Best Practice**

You can create a new user with the same group and profile membership as an existing user with the **Save As New User** action, which is available from the **Participant Administration** utility. To add groups or profiles from other users, you can use the add groups from another user or add profiles from another user  actions.

For more information, see the help available from the **Participant Administration** utility.

---



The **Profile** link available from the organization and site contexts allows you to set up the visibility of actions in the user interface for users, user-defined groups, and organizations.






For more information on participants, the **Participant Administration** utility, and profiles, see [Understanding Participants \(Users, Groups, and Organizations\)](#) on page 251.

## The Next Steps

After your administrators are established, individual administrators can log on and perform their administrative duties. For example, they can create products, libraries, projects, programs, and end users.

To understand what those duties might entail, refer to the following table:

Type of Administrator	Recommended Sections to Read
All administrators	<a href="#">Administration Overview on page 29</a> - for general information. <a href="#">Contexts on page 59</a> - for major concepts about contexts.
Site administrator	<a href="#">Site on page 113</a> - for details on using the <b>Site</b>  functionality. <a href="#">Organizations on page 137</a> - for details on using the <b>Organizations</b>  functionality and creating organization contexts. <a href="#">Participants (Users, Groups, and Organizations) on page 251</a> - for details about creating and managing users, groups, and organizations.
Organization administrator	<a href="#">Organizations on page 137</a> - for details

Type of Administrator	Recommended Sections to Read
	<p>on using the <b>Organizations</b>  functionality and creating organization contexts.</p> <p><a href="#">Participants (Users, Groups, and Organizations) on page 251</a> - for details about creating and managing users and groups within your organization.</p>
Product manager	<p><a href="#">Products and Libraries on page 171</a> - for details on administering products and using the <b>Products</b>  functionality.</p>
Library manager	<p><a href="#">Products and Libraries on page 171</a> - for details on administering libraries and using the <b>Libraries</b>  functionality.</p>
Project manager	<p><a href="#">Projects and Programs on page 233</a> - for details on administering projects and using the <b>Projects</b>  functionality.</p>
Program manager	<p><a href="#">Projects and Programs on page 233</a> - for details on administering programs and using the <b>Programs</b>  functionality.</p>
Shared team manager	<p><a href="#">Teams on page 297</a> - for details on administering context teams and shared teams.</p> <p>See also the section recommended for the context manager of any context in which the shared team is used.</p>

# 2

## Administration Overview

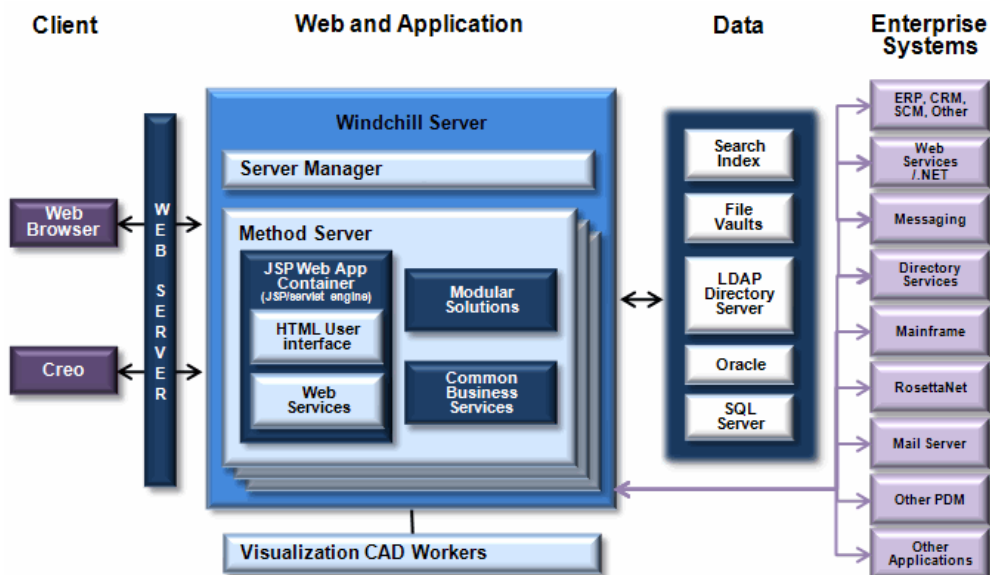
Your Installed Windchill Architecture .....	30
Your Installed Windchill Environment .....	30
Managing Your System .....	32
Managing User Access to Data .....	34
Managing Users .....	45
Managing Data .....	47
Managing Windchill Processes .....	52
Managing User Collaboration .....	57
Additional Administrative Groups .....	57
Post-Installation Activities .....	58

This section provides a general overview of your installed Windchill architecture and Windchill environment. It also introduces you to the main Windchill administration areas and gives some basic information about how to manage your Windchill solution. Later topics assume that you have read the information in this section.

## Your Installed Windchill Architecture

After a base Windchill solution is installed, the Windchill architecture consists of the following:

- Client applications that allow users access to Windchill. The clients can include the Windchill client pages, the visualization clients, the Creo Elements/Pro 5.0 client, and, possibly, workgroup manager clients.
- A web server that includes Windchill Info\*Engine web services and security modules.
- The Windchill server that includes the Windchill solutions and common business services.
- Data storage that includes the Windchill Directory Server and an Oracle or SQL Server database.
- Possibly, connections to other enterprise systems, such as an enterprise directory service, ERP, CRM, SCM, or other PDM systems.

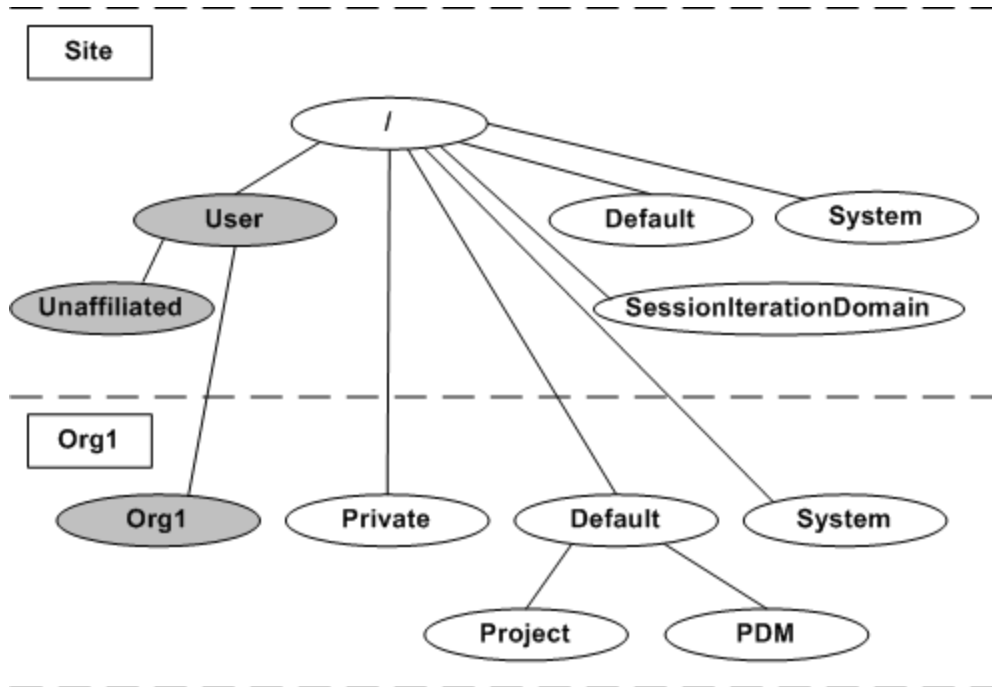


## Your Installed Windchill Environment

Your installed Windchill environment consists of a set of containers that hold all of the administrative areas (known as domains), rules, and data that make up the context from which Windchill users work.

The containers are set up in a hierarchy that is described in [Working With the Initial Organization Context](#) on page 19.

Within the installed containers, a set of domains are loaded during the installation process. For example, the site and Org1 contexts have the domains shown in following diagram:



In the diagram, the dashed line shows the container boundaries and the domain inheritance is shown by the lines connecting the domains. The top-level domain is labeled / (root) and is in the site context. The shaded domains are the domains associated with Windchill participants (users, user-defined groups, and organizations).

After containers are created and users become team members, the framework established is called the context from which the users work. In many instances, the context includes the contents of a specific container and the domains, rules, and data available from ancestor containers. For example, if a user entering Windchill ProjectLink navigates to a folder within the Bike Design project and creates a new document, that document is managed in the context of the Bike Design project. Persons with access to the Bike Design project may automatically have the right to see and modify the new document.

Depending on how container rules are set up, users may also be able to share data across containers. When this is the case, the user context can include data from multiple containers. You can think of the context as providing the framework from which user actions are executed. This framework is defined by a container, but can include data from multiple containers. For example, parts defined in one container can be used in an assembly structure that is saved in a different container.

---

Throughout the user interface, **Context** is used to identify where in the framework specific rules, domains, and data reside. Since **Context** is the label you see in the interface, the remainder of this guide uses the term context (rather than container) when referring to the framework that is in place. Each context provides the following:

- The context structure, which includes the default domains and folders, discussion forum topics, reference notebook folders, and user notebook folders (if used).
- Context participation, which includes the available roles, teams, and system groups.
- Default access policies.
- Data types and object initialization rules.
- Preferences established for the specific context.
- Default life cycle, workflow, context, team, and report templates.

The base data that is loaded during the installation process creates the out-of-the-box templates for contexts, workflows, life cycles, teams, and reports, and associates them with the System domain that is in the site context. These templates are then available to descendent contexts where appropriate.

The Administrator user and the Administrators group are created during the base installation and are also associated with the System domain. Out of the box, these administrators have full access control over all Windchill objects.

One important type of data that is loaded is the context template data. Context template data files are XML files that define what is initially in a context when it is created. The file contains the types of items that are similar to the type of data, rules, and domains that are loaded during the Windchill solution installation. When creating additional contexts, the administrator selects the context template data file to use to establish the context. For more information on context templates, see [Creating the Contexts from which Users Work on page 84](#)

## Managing Your System

Managing your Windchill system is done by administrators who can have specialized knowledge about different aspects of Windchill.

Descriptions of the operations needed to manage your system have been grouped into the following guides:

- *PTC Windchill Administration - Configuring Your PTC Windchill Environment*
- *PTC Windchill Specialized Administration Guide*
- *PTC Windchill Enterprise Administration Guide*



---

The *PTC Windchill Administration - Configuring Your PTC Windchill Environment* describes how system administrators can configure the out-of-the-box system that is installed, including the following:

- Running the Windchill Configuration Assistant
- Configuring the System Quality Agent
- Configuring password management options
- Setting up meetings
- Setting Windchill Desktop Integration options
- Configuring authentication
- Maintaining indexing

The *PTC Windchill Specialized Administration Guide* includes an architectural overview and describes how system administrators can perform system operations that change and improve the out-of-the-box system that is installed. The topic collections in this guide include the following:

- Type and Attribute Management
- Access Control
- Object Initialization Rules
- Indexing
- Notifications
- Site Maintenance, including working with background queues, managing logging options, temporary files, and backup and recovery options.
- Administering Security Labels
- Info\*Engine Administration

The *PTC Windchill Enterprise Administration Guide* describes how system administrators can perform enterprise operations. The topic collections in this guide include the following:

- External File Vaults
- Content Replication
- FvLoader and ReplicaLoader
- Windchill Import and Export
- Import and Export Policies, Mapping Rules, and Conflict Messages
- Windchill Scheduler

The *Using PTC Creo Parametric with PTC Windchill* guide describes how to change and improve the out-of-the-box system that is installed when your site has Creo Elements/Pro 5.0 clients that are using the system.

The *PTC Windchill Advanced Deployment Guide* describes how to deploy a complex Windchill environment, including firewalls, multiple method servers, and clustered servers.

---

## Managing User Access to Data

All Windchill installations establish an initial organization participant and organization context for the initial organization (as described in [Working With the Initial Organization Context on page 19](#)). To belong to the initial organization that is established, each user must have an entry in the user directory service that was set up as part of the installation process and the organization attribute of the entry (usually “o”) must be set to the organization name. By being a member of the initial organization, users can be given access to the data stored in the organization context or its child contexts (depending on the access control rules that are in place). Users who are not members of the initial organization usually do not have access to the data stored in the initial organization context or its child contexts (unless they are invited to participate by someone in the organization). Again, this is dependent on the access control rules that are in place.

---

### Note

If your site does not use the organization attribute in the directory service entries for users, all users can be assigned to an organization using the `usersOrganizationName` property. For more information on using this property, see the *PTC Windchill Installation and Configuration Guide*.

---

After analyzing the users who need access to data, the site administrator determines whether additional organization contexts are needed. Data access can be limited to members of an organization context using access control rules. For example, if your Windchill solution will be used by multiple companies where each company has a different set of data and rules that will be used from within the solution, then setting up an organization context for each company would be the best approach. However, if only one company will actively use the solution and other companies will just provide data that is managed by the initial organization, then one organization context is sufficient.

After determining the organization structure that is needed, the site administrator or organization administrator should determine if there are one or more sets of users who will need to have access to data in multiple application contexts that are created under one organization context. If there are sets of users who will be accessing multiple application contexts under one organization, shared teams can be created at the organization context level. A shared team identifies a set of users who will be working together in multiple application contexts and therefore, can be assigned together as a unit in the organization context rather than added individually to each application context.

---

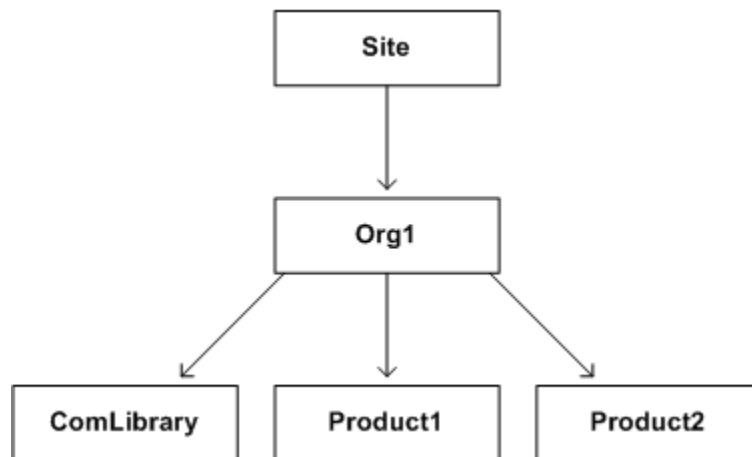
Members of the appropriate application context creators groups can then create product, library, project, or program application contexts under an organization, depending on the contexts available from your Windchill solution. Using application contexts further separates the access of data. In each context, unique policy rules can be set.

To use a shared team in an application context, it must be created before the application context is created.

For more information about policies, see [Administering Domains and Policies on page 86](#).

## Product and Library Hierarchy

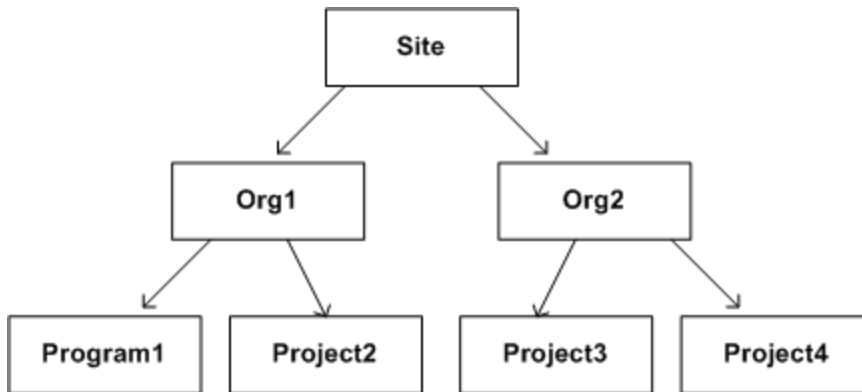
The following diagram shows the context hierarchy of products and libraries where administrators have created one library context and two product contexts under the Org1 context:



---

## Program and Project Hierarchy

The following diagram shows the context hierarchy of programs and projects where there are two organization contexts (Org1 and Org2) and administrators have created a program and project under the Org1 context and two project contexts under Org2 context:

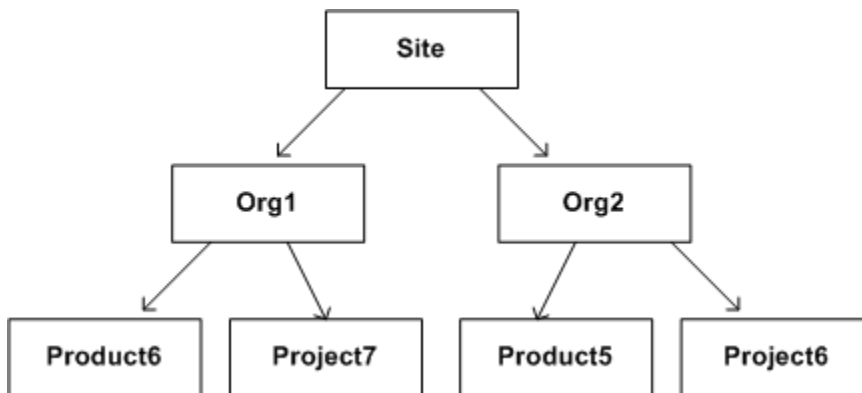


## Hierarchy for Integral Windchill Solutions

The following solutions can be installed in the same codebase:

- Windchill PDMLink and Windchill ProjectLink
- Arbortext Content Manager and Windchill ProjectLink

The following diagram shows the integral hierarchy where there are two organizations (Org1 and Org2) and administrators have created a product and project context under each organization:



---

## Managing Access to Data through Access Control Rules

In each context, a set of access control rules can be set when the context is created. These rules can be defined in the template that is used to create the context. Additionally, an administrator can define access control rules for the data that is in the context and in its child contexts, thereby further controlling the access to data. Generally, each access control policy rule does the following:

- Identifies a type of data stored in a specific administrative area (domain) to which access permissions are applied.
- Identifies the specific state (or all states) of an object to which access permissions are applied.
- Identifies participants (such as users, groups of users, roles, or entire organizations) for whom access is granted, denied, or absolutely denied.
- Specifies the access permissions (such as Read, Create, and Modify) given to the participants for the data type in the specified domain.

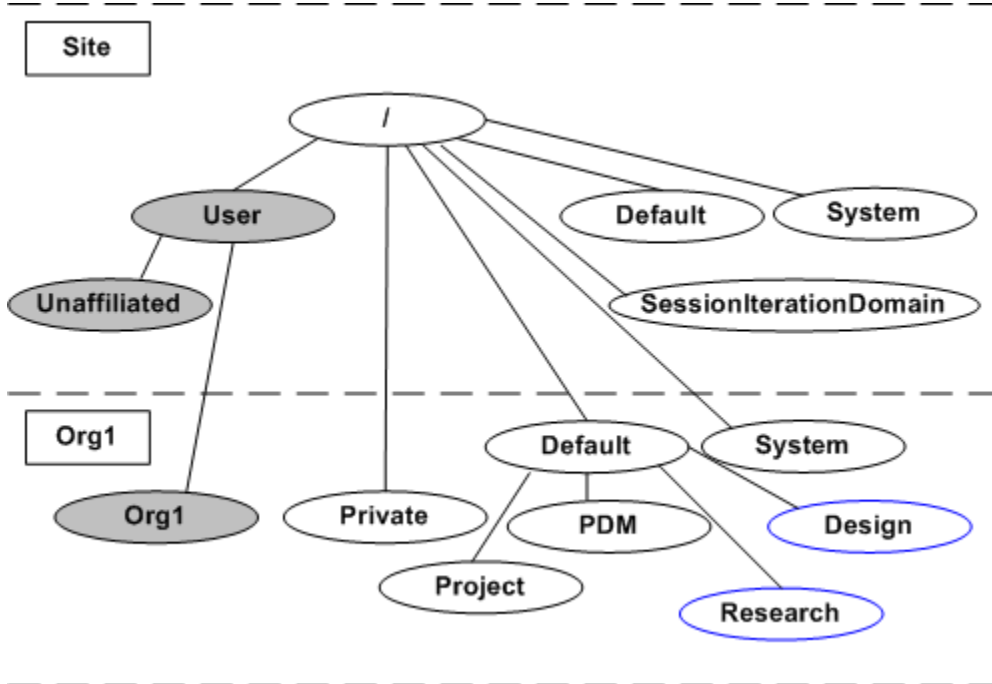
Access control policy rules have a hierarchy based on the domain hierarchy. Descendent domains inherit rules from ancestor domains. Policy rules granting permissions to a participant cannot override inherited rules denying or absolutely denying permissions to the same participant.

The following sections introduce the domains and context structure that are available.

---

## Shared Teams

All shared teams are created in an organization context and, as part of the creation process, domains with the same name as the shared teams are created as children of the Default domain in the organization context. For example, if the Research and Design shared teams are created in the Org1 context, then the additional domains created are shown in following diagram:



## Product, Library, Project, and Program Contexts

For each product, library, project, and program that is created, two domains are created in the context:

- A System domain.  
This domain is a child of the Private domain that is in the organization context. Therefore, the System domain inherits from the /Private domain.
- A Default domain.  
The placement of the Default domain is dependent on the following:
  - Whether a shared team is used.
  - If a shared team is not used, then whether **Private Access** is selected.

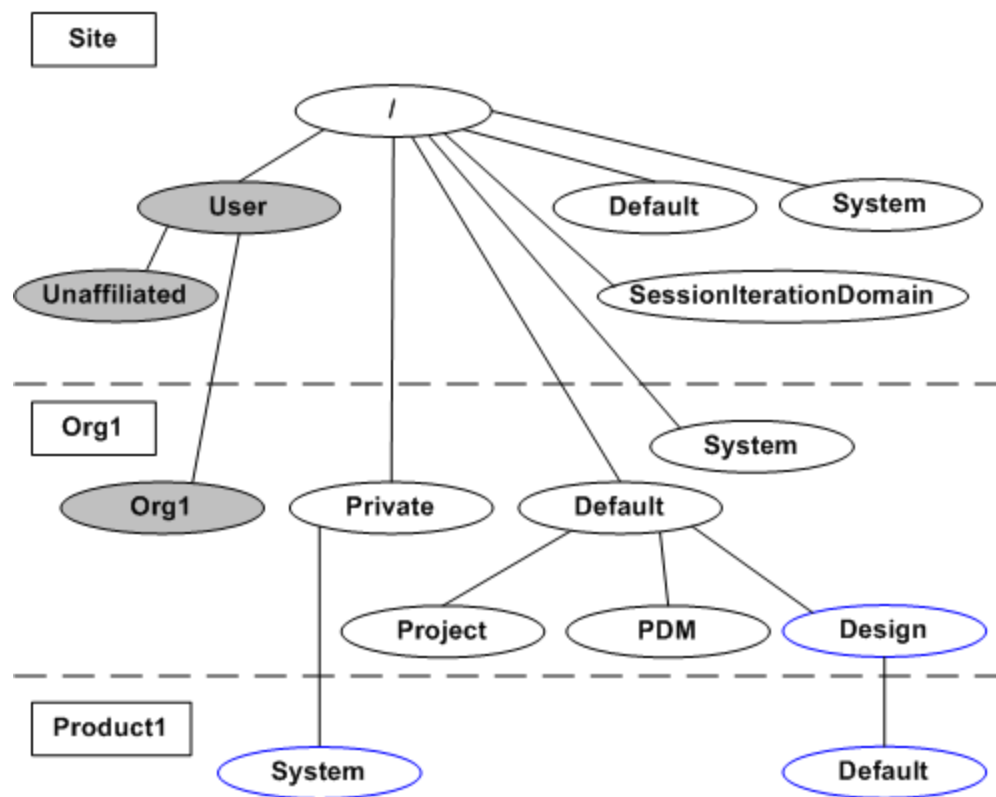
The following sections describe the possible placement of the Default domain and provide a diagram for each scenario.

---

## Contexts using Share Teams

### Note

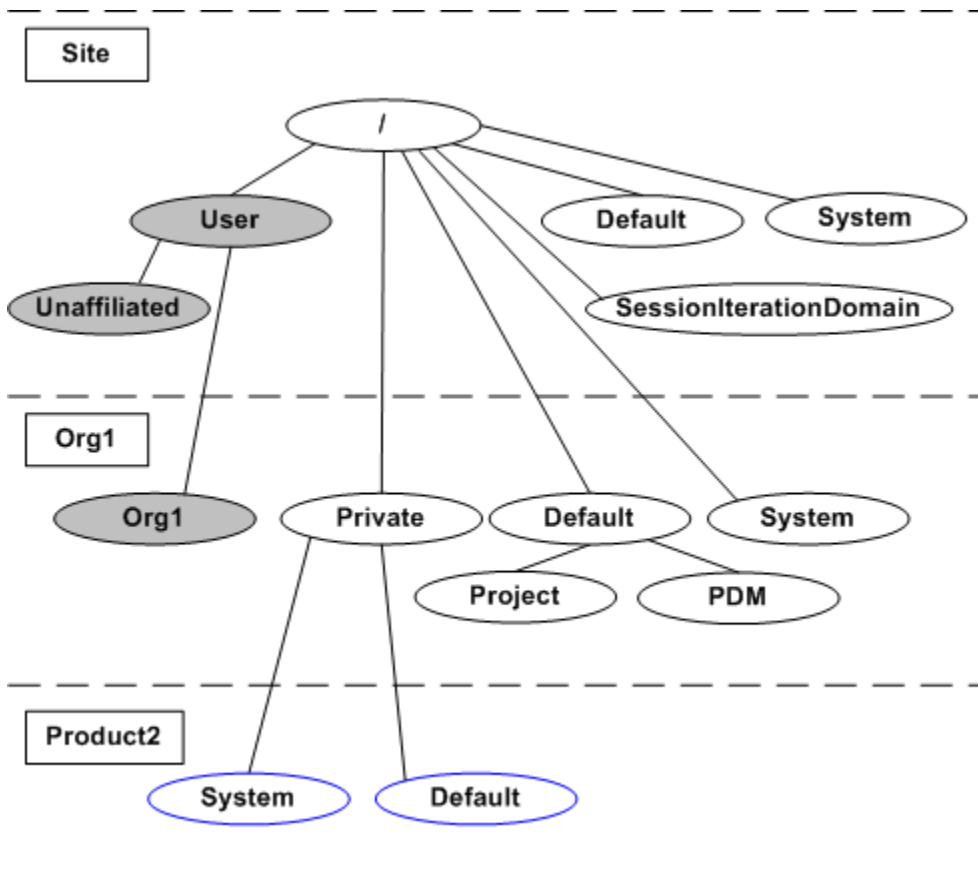
When the creation of a product, library, project, or program specifies that a shared team is used, the Default domain that is created inherits from the shared team domain that is in the organization context, as shown in the following diagram. (Depending on the template you use, other domains can also be created in the context.) The diagram shows the Site, Org1, and Product1 contexts, the Design shared team domain in the Org1 context, and the System and Default domains in the Product1 context:



In this scenario, the domain hierarchy for the System and Default domains in libraries, programs, and projects is the same as the hierarchy for products. If multiple contexts use the same shared team, their Default domains inherit from the same shared team domain. In this case, they inherit from the /Default/Design domain.

## Contexts with Private Access

When the creation of a product, library, program, or project does not specify a shared team but does specify **Yes** for the **Private Access** option (for product and libraries) or **Project Members Only** or **Program Members Only** for the **Private Access** option (for programs and projects), the Default domain that is created inherits from the /Private domain in the organization context instead of from either the /Default/PDM domain or the /Default/Project domain. The resulting hierarchy for a private Product2 context is as follows:

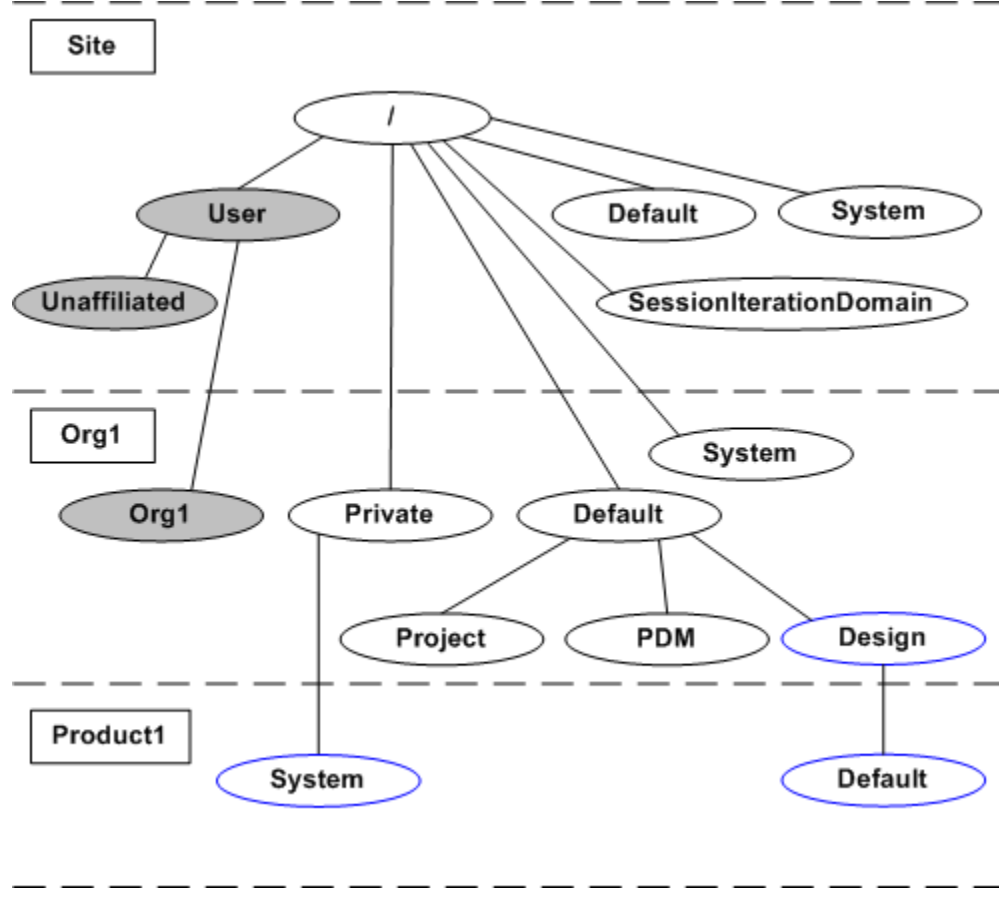


In this scenario, the domain hierarchy for the System and Default domains in libraries, programs, and projects is the same as the hierarchy for products.



 **Note**

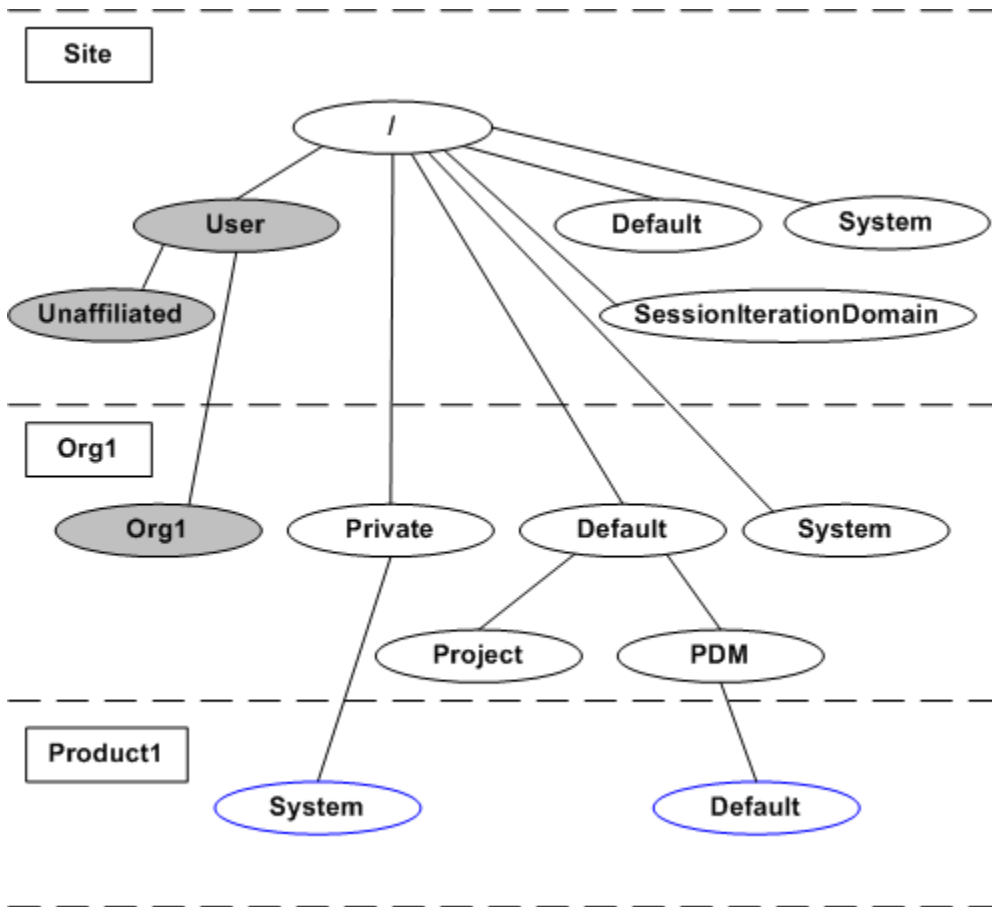
Specifying a shared team prevents selection of **Private Access**. When a shared team is used, the Default domain always inherits from the shared team domain, as shown below:



Products and Libraries without Private Access

When the creation of a product or library does not specify a shared team and does not specify **Private Access**, the Default domain that is created inherits from the /Default/PDM domain in the organization context, as shown in the following

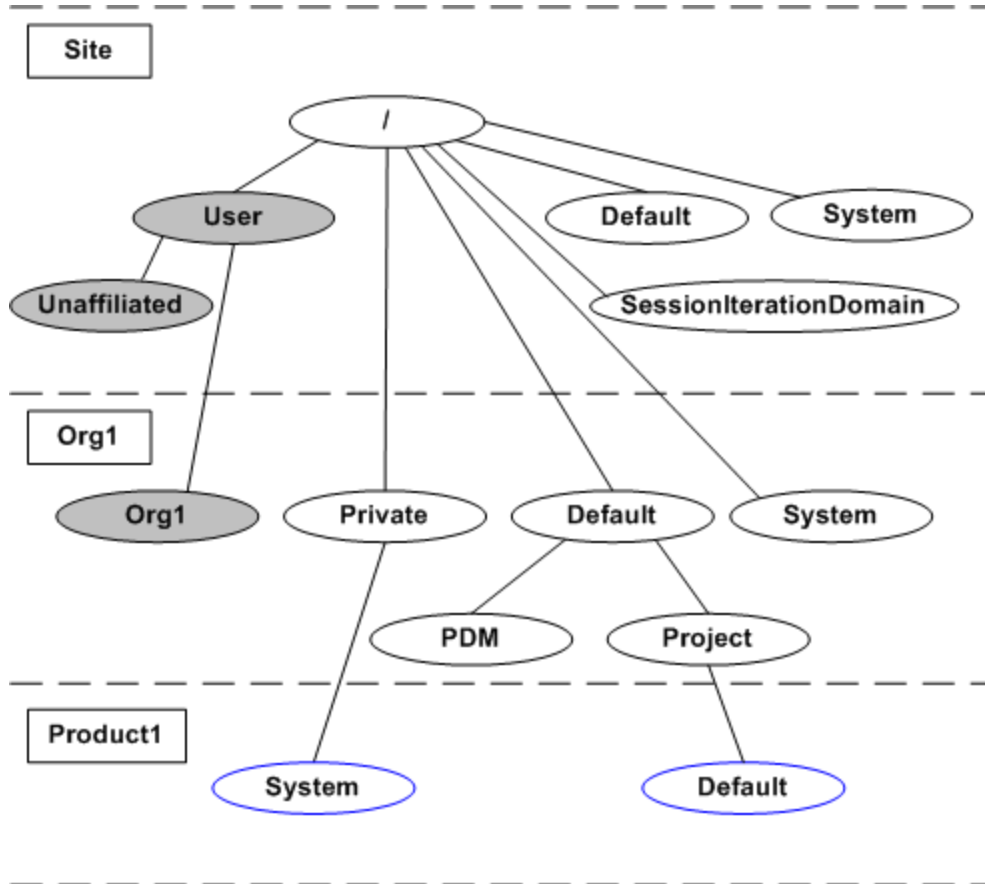
diagram. (Depending on the template you use, other domains can also be created in the product or library context.) The diagram shows the Site, Org1, and Product1 contexts and domains:



### Projects and Programs without Private Access

When the creation of a project or program does not specify a shared team and specifies **Default** for the **Private Access** option, the Default domain that is created inherits from the /Default/Project domain in the organization context and a System domain inherits from the /Private domain in the organization context, as shown in

the following diagram. (Depending on the template you use, other domains can also be created in the organization and project contexts.) The diagram shows the Site, Org1, and Project1 contexts and domains:



## Setting Up User Access to Data

You can determine which sets of users have access to the data in the context by setting access control rules in the domains associated with the context where the data resides. You can also establish the set of access control permissions users can view and edit when they manage the security of individual objects from within an application context.

Use the **Policy Administration** utility to create policy rules. For details on domain inheritance and setting policy rules, see [Administering Domains and Policies on page 86](#).

Use the **Preference Management** utility to establish the set of permissions users can view and edit. For details, see the Access Control chapter of the *PTC Windchill Specialized Administration Guide*.

---

The **Team** link that is available in each context allows you to set up the role and role memberships; these can be used as the system groups against which the access control rules are set, as described in [Managing Access to Data through Team Memberships](#) on page 44.

Use the **Participant Administration** utility to update users who have changed in your user directory service or create and update user-defined groups at the organization level that can be used as team members. For additional information about managing users, user-defined groups, and organizations, see [Participants \(Users, Groups, and Organizations\)](#) on page 251.

Additionally, you can limit the visibility of the actions in the user interface for users, user-defined groups, and organizations. For more information, see [Profile Management](#) on page 291.




## Managing Access to Data through Team Memberships

Another aspect of managing user access to data can be found in managing who becomes a member of an application context. The context team associated with a product, library, project, or program establishes which users are members of a specific application context. A context team can be made up of the following teams:



- A shared team that is established by the site or organization administrator (or by others given the rights to create shared teams) in the context of an organization and selected when creating the application context.
- A local team that is established by the application context manager as part of creating and managing the application context.
- Both a shared team and a local team.

Team members are added to a shared team according to their established role in multiple application contexts. For example, you could have a group of engineers who fill the Design Engineer role for many of the products or projects managed by your organization. This user-defined group could then be added to a shared team that is then selected when the application context is created.

Team members are added to a local team according to their role in a specific product, library, program, or project. For example, you could have an individual who will be in the Reviewer role for only a specific product or project. Then, this individual could be added to the local team for that product or project. The initial roles that are available for shared and local teams are determined when the teams are created; however, additional roles can be added.

For each role used in a context team there is a corresponding system group created that administrators can use to create access control rules for the members assigned to the role. The **Team** link under **Products** , **Libraries** , **Programs** , or

---

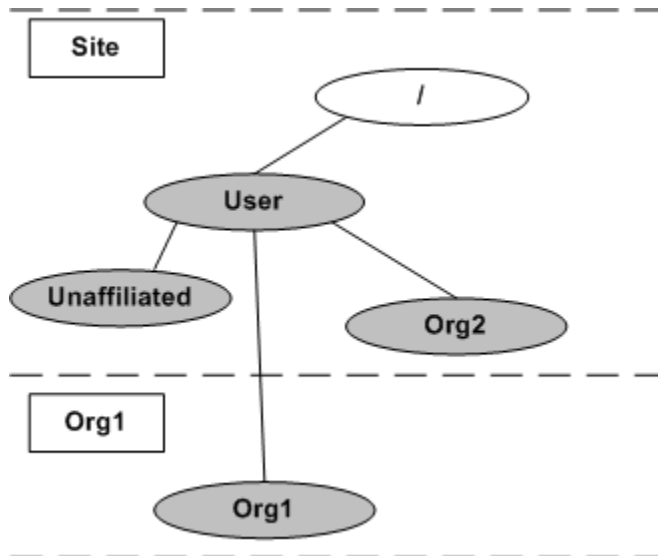
**Projects**  in the **Navigator** provides access to the interface for managing local teams. **Organizations**  ► **Team** provides access to the interface for managing shared teams. Use the **Policy Administration** utility to create access control rules.

Your Windchill solution also uses roles and corresponding users defined in life cycle templates and team templates (if they are defined for an object). For additional information about teams, see [Teams and Team Template Administration on page 297](#).

For additional information about access control rules, see [Administering Domains and Policies on page 86](#).

## Managing Users

As mentioned in earlier sections, the default domains associated with users are the User domain in the Site context or one of its child domains. For example, assume that the Org1 organization context has been created and users from both the Org1 and Org2 organizations and users that have no organization affiliation (the organization attribute is not set for the user) have accessed your Windchill solution. The following domains are then automatically created:

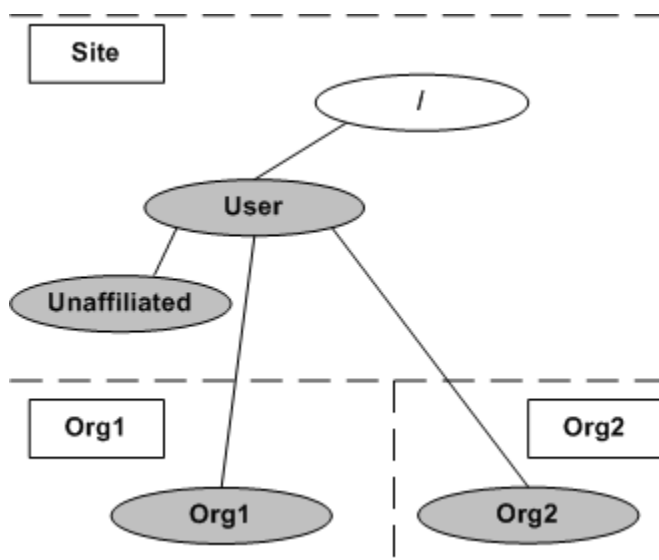


---

In this example the user and domain associations are as follows:

- Users from the Org1 organization (their organization attribute is set to Org1) are associated with the Org1 domain by default. This domain is in the Org1 context.
- Users from the Org2 organization (their organization attribute is set to Org2) are associated with the Org2 domain by default. This domain is in the Site context.
- Users who have no organization affiliation are by default associated with the Unaffiliated domain. This domain is in the Site context.

In the previous example, assume that the Org2 organization context is now created in your Windchill solution. Then the Org2 domain moves from the Site context to the Org2 context, as show in the following diagram:



By using the default domains for users, users are automatically grouped by organization and access policy rules for each organization are initially set using the organization context template used to create the organization. Rules for users not affiliated with any organization can be set using the Unaffiliated domain.

When your Windchill solution creates user objects, a personal cabinet is also created for each user. By default, the personal cabinet for a user is put in the same domain as the user. Using this approach allows the access control rules for personal cabinets to be in the same domain as the access control rules for the users.

In the previous examples, the organizations have short names. If the organization names you are using are longer than 193 characters, then the names are truncated when creating corresponding domain names. For more information, see [Creating Domains on page 92](#).

---

## Managing Data

The Windchill installation establishes a set of business object types that are available in the site context and then can be inherited by organization contexts and then by application contexts. The use of object types allows you to categorize objects by providing a set of attributes and user interface functions for each type. For example, objects that are typed as documents (using the type wt.doc.WTDocument) have a different set of attributes and actions available in the user interface than those objects typed as parts (using wt.part.WTPart).

Commonly used business object types include those described in the following table:

Display Name	Object Type	Description
Document	wt.doc.WTDocument	General documents such as text files or Microsoft Word documents
Analysis Activity	wt.change2.WTAnalysisActivity	Change data that assigns an analysis task to a user
Change Task	wt.change2.WTChangeActivity2	Change data that assigns product development work to a user
Change Investigation	wt.change2.WTChangeInvestigation	Change data that collects information about the root cause of a product problem
Problem Report	wt.change2.WTChangeIssue	Change data that reports a potential product problem
Change Notice	wt.change2.WTChangeOrder2	Change data that collects all tasks required to implement a product change
Change Proposal	wt.change2.WTChangeProposal	Change data that proposes a solution to a product problem
Change Request	wt.change2.WTChangeRequest2	Change data that collects all change impact data required for a decision
EPM Document	wt.epm.EPMDocument	This type is the parent type of subtypes for the following business objects: <ul style="list-style-type: none"><li>• CAD documents (type:&lt;prefix&gt;.DefaultEPMDocument)</li><li>• dynamic documents (type:&lt;prefix&gt;.DynamicDocument)</li><li>• burst configuration files</li></ul>

Display Name	Object Type	Description
		<p>(type: &lt;prefix&gt;.BurstConfiguration)</p> <ul style="list-style-type: none"> <li>notes (type: &lt;prefix&gt;.Note)</li> </ul>
Part	wt.part.WTPart	A database object that represents a component of assembly in a product structure
Promotion Request	wt.maturity.PromotionNotice	A request to change the state of one or more objects to a new life cycle state with the selection of a review process.
Part Instance	wt.part.WTProductInstance2	A serialized copy of a product built according to a specific configuration
Variance	wt.change2.WTVariance	An authorization to depart from the as-designed configuration for a specific number of units or for a specified time period. Variances consist of deviation and waivers. A deviation is a planned departure from the as-designed configuration before the part is built. A waiver is a written acceptance of nonconformance.
Variant Specification	com.ptc.wpcfg.doc.VariantSpec	The collection of options specified for a particular configurable part structure in preparation for creating a variant. The variant specification, in essence, defines the characteristics of the variant that should be created from the configurable part structure.



---

## Note

Not all Windchill solutions use all business object types and many additional object types are used by your Windchill solution to help manage administrative processes, such as updating user preferences, life cycles, and workflows. Additional information about the use of specific object types can be found throughout this topic collection.

---

## Data Types

All data stored in a Windchill solution are stored as objects of specific types. The type is identified when the object is created or imported. By typing data, you establish patterns for handling the data within the Windchill solution. For example, you can decide if part data is numbered automatically or manually and decide who has access to part data. Separate decisions can be made for each type of data by setting object initialization rules. A set of these rules is established when each context is created through the context template that is used. Additional object initialization rules can be set using the **Object Initialization Rules Administration** utility, accessed from the **Utilities** page of the context where you want the rule stored.

## Subtypes

In addition to the object types that are provided out of the box, object types can have subtypes. Your Windchill solution provides some document subtypes as part of its installation. Additionally, Windchill PDMLink and Arbortext Content Manager provide subtypes for dynamic documents and bursting configuration files that are used when authoring document content through the Windchill connection to Arbortext Editor.

If your site needs additional types, you can create specific subtypes from within the site or an organization context using the **Type and Attribute Management** utility.

## Visualization Data

Windchill Visualization Services (WVS) integrates Windchill with Creo View, a PTC data visualization tool that allows you to view, annotate, analyze, measure, and animate CAD documents and parts. You may also view, mark up, and print the content of documents in Creo View. All information viewed or annotated in Creo View is saved and stored back into the Windchill database.

---

Creo View supports watermarking of 3D, drawings, images, and documents. Watermarks are defined in INI files created and edited using the Creo View watermark editor. The administrator that manages watermarks manually transfers the INI files from the watermarks directory into the Windchill server.

Windchill Visualization Services can also be used to integrate Windchill with the Arbortext Publishing Engine for creating representations from dynamic documents. Supported formats include PDF and HTML. This is done through the WVS publisher.

For more information about administering visualization data, see the *PTC Windchill Visualization Services Administrator's Guide*

## CAD Data

Data files created by CAD applications and saved to Windchill using a workgroup manager or Creo Elements/Pro 5.0 are managed in Windchill as CAD documents.

CAD documents are associated with a subtype of the wt.epm.EPMDocument modeled object type and can be used to manage many different types of CAD files including parts, assemblies, drawings, layouts, and manufacturing files. In addition, a CAD document can have secondary content. The secondary content is typically used for additional supporting information or derived files such as STEP, IGES, JPEG, and others.

The CAD Document subtype defined as `<prefix>.DefaultEPMDocument` is established during the installation process, where `<prefix>` is generated by reversing the internet domain specified as part of the organization properties during the installation. For example, if the internet domain specified is `acme.com`, then the `<prefix>` used in the soft type name is `com.acme`.

Administrators can create and update CAD document templates. These templates can be used to create CAD documents.

## Dynamic Document Data

Windchill supports data files that are created by the Arbortext Editor. These files are saved to Windchill using the Windchill connection for the editor and are managed in Windchill as dynamic documents. The data files can then be published using the WVS publisher if the publisher has been configured for the Arbortext Authoring Application.

The Arbortext Editor and the Arbortext Publishing Engine are optional Windchill products that can be purchased through PTC.

Dynamic documents are associated with the `<prefix>.DynamicDocument` subtype or are possibly associated with a subtype of `<prefix>.DynamicDocument`, where `<prefix>` is generated by reversing the internet domain specified as part of the

---

organization properties during the installation. For example, if the internet domain specified is acme.com, then the subtype for dynamic documents is named com.acme.DynamicDocument.

Using additional subtypes helps categorize the types of dynamic documents and is often required when deploying a complex content authoring system that connects to the Arbortext Editor.

Understanding how Windchill and Arbortext Editor work together and the basics on setting up your Windchill PDMLink system to work with Arbortext Editor are covered in the Arbortext Editor and PTC Server Configuration help topics.

For general guidelines on creating product and library contexts to use with dynamic documents, see [Configuring Products or Libraries for Dynamic Documents on page 224](#).

For information on setting up the WVS publisher for publishing dynamic documents, see the *PTC Windchill Visualization Services Administrator's Guide*.

## Document Data

General documents (such as Microsoft Word files and text files) stored in the Windchill database have the wt.doc.WTDocument object type or are possibly associated with a subtype of wt.doc.WTDocument. Using subtypes helps categorize the types of documents.

Administrators can create and update document templates. These templates can be used to create documents.

Administrators can also change the preference settings related to documents (such as file name uniqueness and template file name length). These settings can be found under the **Documents** category in the **Preference Management** utility.

## Part Data

Parts stored in the Windchill database have the wt.part.WTPart object type.

Parts created in Windchill can be associated with a view. A view identifies what the part is used for. The Windchill installation provides two out-of-the-box views: design and manufacturing. Before allowing users to create parts, you can rename these views and add other views that make sense at your site by using the **View Administration** utility.

For more information, see the help available from the **View Administration** utility.

## Auditing

The auditing utilities are designed to record and report user and system events for auditing and traceability purposes.

---

## Managing Windchill Processes

Windchill provides you with the following types of Windchill data processes that can be used with the business objects stored in Windchill:

- A life cycle process defines a set of phases and gates that manage the life of an object as it progresses from conception to obsolescence.
- A workflow process defines rules which allow workflow participants to view and pass along information, tasks, and documents.
- A change process establishes how to get changes made to parts and many other data types including documents, document soft types, and product instances.

These three processes work together to help you manage data. Workflows are often used to drive the life cycle. That is, the workflow process is used to transition from one life cycle state to another. In most cases, a workflow process is initiated from a life cycle. In any case, life cycle-managed objects obtain a life cycle when they are created. In obtaining a life cycle, an object can have a workflow process instance created as well. Change objects are life cycle-managed objects. Each change object starts a change process when it obtains its life cycle.

Use the **Life Cycle Template Administration** utility to manage the life cycle templates that can be used. For details on managing life cycle templates, see [Life Cycles on page 299](#).

Use the **Workflow Template Administration** utility to manage the workflow templates that can be used. For details on managing workflow templates, see [Workflow on page 337](#).

## Planning Object State Change Policies

Business information and business objects become more mature throughout the product development cycle. During this cycle, circumstances change, such as who can access data, what processes are related, and where an object can mature to next. Life cycles define the way in which these business objects mature, providing a model for a product's commercialization process.

A life cycle is an automated, graphical model, employing phases and gates, used to manage business objects as they progress from conceptualization through obsolescence.

While an object is in a specific life cycle phase, certain business rules apply, such as access control rules or a specific workflow defined for that phase.

When created, an object modeled to be life cycle-managed enters a life cycle phase, where it is assigned an initial state, and is then associated with the initial phase of its life cycle.

---

Users can change the life cycle state of an object using one of three methods:

- **New Promotion Request** action—Users can create a promotion request to request a state change for a set of objects that reside in products or libraries when there is need for some oversight or review of the state change. The promotion process usually includes assigned participants to review and approve or deny the promotion of the object to the new state.

For more information, navigate to the following topic in the Help Center: [PTC Windchill Fundamentals > Collaborating with Others > Promotion Requests > Creating a Promotion Request](#).

Windchill provides two out-of-the-box workflow processes for promotion requests: Promotion Request Approval Process and Promotion Request Review Process. Administrators can edit these workflows or create additional promotion workflow processes as necessary.

- **Set State** action—Users can manually change the state of one or more objects if they have the appropriate permissions. The **Set State** action does not require review or approval.

For more information, navigate to the following topic in the Help Center: [PTC Windchill Fundamentals ▶ Working with Windchill Objects ▶ Actions Common Among Objects ▶ Setting the State of an Object](#).

A user can change the state of an object using the **Set State** action if they have one of the following access control permissions for the object:

- Set State permission for the object—Users who have Set State permission for an object can only change the state of the object using the **Set State** action if an administrator has defined a valid transition for that object. A transition specifies one or more destination states that are possible for an object in a specific originating state. Administrators control the available destination states for an object based on the originating state of the object by specifying transitions for the **Set State** action. For example, consider that an object life cycle has three defined states: In Work, Under Review, and Approved. Administrators can choose to define transitions from any originating state to any destination state. If an originating state is In Work, a transition can specify a destination state for the object is Under Review. Assuming that there are no other transitions defined for the object, if a user has Set State permission for the object in the In Work state, they can modify the state of the object to Under Review.

For more information about granting users permissions to the **Set State** action, see [Giving Users Permissions to Perform the Set State Action on page 56](#).

- 
- Administrative permission for the object—Users who have Administrative permission for an object can use the **Set State** action to modify the state of the object to any of the states defined in the life cycle associated with the object, irrespective of whether any transitions have been defined from the originating state to the destination state.
  - Change Management process—The change management process formally manages the release of objects to the organization. This can be leveraged any time there is a need to formally introduce a revision to an organization and could be a prototype level or production level release. The change management process provides robust methods of reviewing justification, planning, and implementation, as well as auditing the change. During the change process, a team defines who is involved in the various roles for review and execution of the change.

Windchill provides several out-of-the-box workflow processes for change management. Administrators can edit these workflows or create additional change management workflow processes as necessary.

The method used to change the life cycle state of an object depends on the needs or requirements of a site, the business processes and procedures, the type of object, the type of state change, and other possible factors. Administrators should consider such factors when making decisions about which method of state change is appropriate. The following table outlines a few specific considerations.


<b>Recommended Scenarios for Requiring the Use of the Promotion Process</b>	<b>Recommended Scenarios for Giving Users Permissions to the Set State Action</b>	<b>Recommended Scenarios for Using the Change Management Process</b>
<ul style="list-style-type: none"> <li>• A form of oversight or review is needed before changing the state of an object.</li> <li>• The state of many objects needs to be changed at once.</li> <li>• The promotion request needs to be used as a configuration specification.</li> <li>• A revision is part of the promotion, including changing the revision scheme (for example, changing the revision scheme from 1, 2, 3 to A, B, C).</li> </ul>	<ul style="list-style-type: none"> <li>• A user needs to correct or update a set of life cycle states administratively.</li> <li>• Oversight is not required to make the state change.</li> <li>• You want your users to more easily and quickly be able to change the state of an object, typically in an informal stage of product development.</li> <li>• You want to allow users to change the state of more than one object simultaneously.</li> </ul>	<ul style="list-style-type: none"> <li>• You need to formally introduce your data to the organization.</li> <li>• The improved traceability and review of the change management process is needed.</li> <li>• You need to release data to multiple states, such as Released and Obsolete, while also supporting actions such as Revise and Mass change as part of the work.</li> <li>• You need to be able to capture the justification for the revision and the release.</li> </ul>

<b>For more information about this concept</b>	<b>Refer to this PTC Windchill Help Center topic</b>
The Promotion Process and out-of-the-box Promotion Process Workflows	Promotion Process
Life Cycles and their Phases and States	Understanding Life Cycles
Life Cycle Transition Rules	Transition Rules
The Change Management Process	About Change Management

For more information about this concept	Refer to this PTC Windchill Help Center topic
Out-of-the-box Change Management Workflows	Change Management Workflows
Configuration Specifications	About Configuration Specifications And also: Selecting a Promotion Request Configuration Specification

### Giving Users Permissions to Perform the Set State Action

Users who do not have Administrative permission on an object can be given permissions to perform the **Set State** action on that object. Use the following steps to grant the appropriate permission:

1. Identify the life cycle template used by the object by reviewing the object initialization rule for the object type.
  - a. Launch the **Object Initialization Rules Administration** utility from the **Utilities** page.
  - b. Download the object initialization rule XML file for the appropriate object type using the **Download** action.
  - c. Open the XML file in a text editor to identify the life cycle state.
2. Define a valid transition for the life cycle template by selecting one or more destination states for the object in its originating state using the **Life Cycle Template Administration** utility. The originating state is the state the object is in when you want participants to be able to use the **Set State** action. A destination state is a valid state that the participant is able to select for the object when they use the **Set State** action.
  - a. Go to **Site**  **Utilities** **Life Cycle Template Administration**.
  - b. In the **Life Cycle Template Administration** window, select the desired life cycle template and click **Edit**.
  - c. In the **Edit Life Cycle** window, select the originating state, and then click the **Transitions** tab.
  - d. In the **Set State** row, select one or more destination states.
  - e. Save and check in the life cycle template.
3. Grant the appropriate participants the Set State permission for the desired object in the originating state using the **Policy Administration** utility.
  - a. Launch the **Policy Administration** utility from the context in which you want to create the access control rule. If you want the participant to be able to use the **Set State** action in all contexts in which the participant is a member, set the permission at the organization or site level.



- b. Grant the **Set State** permission in the appropriate domain for the participant, object type, and life cycle state you identified previously.

For more information about this concept	Refer to this PTC Windchill Help Center topic
Object Initialization Rules Administration	Understanding Object Initialization Rules
Defining State Transitions	Defining State Transitions
Policy Administration and granting permissions	Policy Administration

## Managing User Collaboration

User collaboration can be done using a specific Windchill solution and other PTC or third party products or using multiple co-installed Windchill solutions.

Windchill provides the following tools for collaboration:

- Windchill projects that are created using Windchill ProjectLink provide participants with a place in which they can share information. This information can include data that resides in either a Windchill PDMLink or Arbortext Content Manager solution.
- Creo Elements/Pro 5.0 provides users with the ability to share CAD drawings and other design-related information. For administration information, see the *Using PTC Creo Parametric with PTC Windchill* guide.

## Additional Administrative Groups

The following additional administrative groups are automatically created for all Windchill solutions to help define users for specific administrative activities in your solution:

- Attribute Administrators
- LifeCycleAdministrators
- Replication Managers
- Type Administrators
- WorkflowAdministrators
- Workflow Authors

For example, those users in the Attribute Administrators group can manage reusable attributes. Those users in the LifeCycleAdministrators group become participants in the Default life cycle template, when that template is used.

---

If Windchill Supplier Management is installed, the installation creates the following administration group:

- Supplier Administrators

For information on Supplier Management activities, see the *PTC Windchill Supplier Management Administrator's and User's Guide*.

By using the **Participant Administration** utility, you can add users to any of the administration groups.

Additional types of administrators are available as appropriate for the application contexts within your Windchill solution:

- An organization administrator manages a specific organization.
- A product manager manages a specific product.
- A library manager manages a specific library.
- A project manager manages a specific project.
- A program manager manages a specific program.
- A shared team manager manages a specific shared team, and acts as a context manager for any contexts that use the shared team.

For additional information about administrators, see [Establishing Administrators on page 20](#).

## Post-Installation Activities

Before allowing users to access the Windchill solution, be sure to do the following activities:

- Complete the activities described in [Getting Started on page 11](#).
- Determine if there are additional organization contexts that you want to create and create them. For more information, see [Organizations on page 137](#).
- Determine if additional organization participants are needed and whether or not to allow these organizations to own parts and documents.

By default, all parts and documents are owned by the organization from which they are created. For information on how to set up the ability to choose which organization owns a part or document, see [Organizations on page 137](#).

- Add participants to license groups. Currently, the View and Print Only license group is available. For more information, see About the View and Print Only License Group in the Access Control section of the *PTC Windchill Specialized Administration Guide*.
- Determine whether you want audit reports enabled. For more information see the Auditing help.

# 3

## Contexts – Distributed and Hierarchical Administration

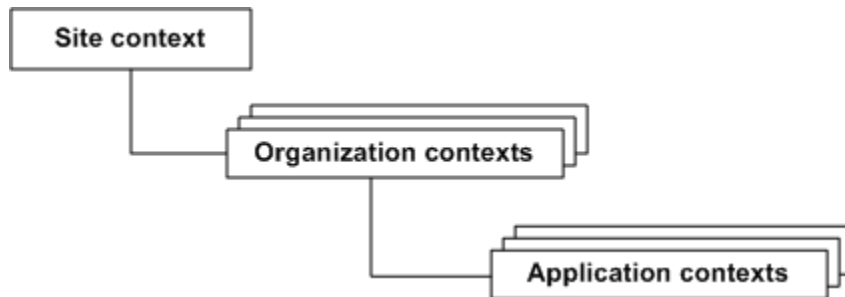
Contexts—An Administrative Overview .....	60
Context Administrative Items .....	61
Creating the Contexts from which Users Work .....	84
Administering Domains and Policies .....	86
Administering the Numbering of Parts, Documents, CAD Documents, Managed Baselines, and Change Objects .....	104
Administering the Versioning of Parts, Documents, and CAD Documents .....	105
Administering Preferences .....	107

This section provides the overall details relating to working with contexts. Later sections assume that you have read the information in this section.

---

## Contexts—An Administrative Overview

Windchill contexts provide the framework for collecting and finding related information. The set of contexts in your Windchill solution have a hierarchical relationship. The following depicts the basic context hierarchy:



The site context can have one or more child organization contexts. An organization context can have one or more child application contexts.

Application contexts include:

- Products
- Libraries
- Projects
- Programs

Data, such as template files, can be distributed among the contexts. For example, you can define general document templates, such as those used for presentations or memos, at the top level of the hierarchy (in the site context). The document templates are available to all contexts. Then you can define progressively more specific templates at each layer in the hierarchy, such as in an organization context or a library context. In a child context, you can also define templates with the same name as those templates in a parent context so that the templates in the child context can override and be used in place of templates in a parent context.

With distributed administration, application context administrators are responsible for their own administrative tasks. So, for example, each product, library, project, and program can have its own administrators (called product, library, project, and program managers). Additionally, if you are using shared teams in context teams, the shared team manager (established in the shared team) becomes the context manager for each application context that uses the shared team. This allows you to easily assign administrative duties for multiple contexts to one or more individuals.

To support distributed administration, the administrative utilities are context aware. For example, opening the Policy Administration utility in the context of a library initially displays the domains that are in the library context and the domains that are ancestors of the library context domains. Having context aware utilities allows the delegation of administrative duties to users who are recognized as application context managers.

---

With hierarchical administration, contexts inherit administrative items from parent contexts (or, in the case of policies, from parent domains). Administration performed at the level of a parent context is applicable to all of its child contexts. Except for policies, a child context can choose to override the administrative items of its parent contexts. For policies, rules from all parent domains are merged with the rules in a current domain to form the policy for the current domain. For more information about policies, see [Administering Domains and Policies on page 86](#).

In general, always think of performing administration duties from within a context, as follows:

- Site administrators can create, modify, delete, and view administrative items in the site context.
- Organization administrators can create, modify, delete, and view administrative items in the given organization context. They can generally view and override administrative items defined in the site context.
- Application context managers can create, modify, delete, and view administrative items in the given application context. They can generally view and override administrative items defined in the parent organization context and the site context.
- Site and organization administrators can administer child contexts; however, they do so by going into the child context and performing their administrative duties there.

---

 **Note**

Windchill users generally perform their activities within an application context, rather than in an organization or site context.

---

Non-administrative Windchill users generally do not create, modify, or delete administrative items; however, they may have visibility to, and are affected by, the following administrative items:

- The administrative items that are defined in a given application context.
- The administrative items that are defined in the parent organization and site contexts, but not overridden in the application context.

## Context Administrative Items

Each context can be populated with the following types of administrative items:

- Context configuration
- Context structure
- Context participation

- 
- Context policies
  - Context data types and attributes
  - Templates, including context templates, process templates, and data templates
  - Context object initialization rules
  - Context preferences

After you have created a context, you can update many of the administrative items that are associated with the context. The contexts that can be updated include the site context, as well as organization and application contexts.

Use the administrative utilities and specific user actions to edit the administrative items in a context. These utilities and actions are usually available to the administrator of the context. For the details on Windchill administrators, see [Additional Administrative Groups on page 57](#).

Each type of context has a slightly different set of administrative items that can be updated. For example, you can edit the set of life cycle and workflow templates provided in organization, product, and library contexts. Also, you can only edit the set of product, library, project, and program templates that are provided in an organization or the site context. This is because product, library, project, and program templates are not included in application contexts.

The following sections provide descriptions of administrative items, information on what is installed in the site context for each item, and how to edit the items.

## Context Configuration

Configuration items identify the type of context and other miscellaneous information about the context.

There are three general types of contexts:

- Site – The site context is the top-level context. There can be only one site context.
- Organization – Organization contexts are always children of the site context. There is always at least one organization context required to have an operational Windchill solution.
- Application – Application contexts are always children of an organization context. There are four types of application contexts:
  - Product
  - Library
  - Project
  - Program

---

The context configuration can include the following additional items:

- You decide whether an application context is public or private. This option is only available when you are not using a shared team.

The /Default domain in private contexts, by default, inherits access control rules from the /Private domain of the organization.

The /Default domain in public contexts, by default, inherits access control rules from a solution-dependent public domain within the organization context. For projects and programs, the default public domain is the /Default/Project domain. For products and libraries, the public domain is the /Default/PDM domain. This configuration allows an administrator to:


- Create policies in the organization context /Default domain that apply to all public child contexts and contexts using a shared team.
  - Create policies in the /Default/Project and /Default/PDM domains that apply to solution-specific child contexts.
  - Create policies in the /Private domain that apply to all private child contexts; however, PTC recommends that no additional access control rules be created within this domain as those policies would be inherited by all private contexts. If additional policies are required for a given private context, create the policies using a domain in the child context.
- For application contexts created with shared teams, the default behavior is that the /Default domain in the contexts inherits access control rules from the shared team domain in the organization context where the shared team was created. The shared team domain has the same name as the shared team and is a child of the /Default domain in the organization context. This configuration allows an administrator to:
    - Create policies in the organization context shared team domain that apply to all child contexts that use that shared team.
    - Create policies in the Private domain that apply to all private child contexts; however, PTC recommends that no additional access control rules be created within this domain as those policies would be inherited by all private contexts. If additional policies are required for a given private context, create policies using a domain in the child context.
  - For project contexts, you decide whether or not data can be shared to other contexts.
  - For an organization context in Windchill solutions including projects and programs, you decide whether the project creators group is auto-populated with members of the organization. The project and program creators groups determine who can create projects and programs.

---

The configuration of the context is set when the context is created based on the options chosen through the user interface or through data loading, and are not set in a template.

## Editing the Context Configuration

The configuration of an organization or application context is set when the context is created based on the options chosen through the user interface. Only a few of the options can be updated:

- For an organization context, update the context using the **Edit Organization** icon or the **Edit** action on the organization information page. Site administrators can navigate to the **Organizations** table (accessed by selecting **Organizations**  ► **View All**) select the **Edit** action for the organization they want to update.

For details on how to edit and what can be edited, see the help available from the **Edit Organization** window.

- For an application context, edit the context using the edit context icon or the **Edit** action from the context information page. First, navigate to the context in the **Navigator**, and then selecting the specific product, library, project, or program that you want to edit.

For details on how to edit and what can be edited, view the help available from the context information page.

## Context Structure

Structure items identify the domains, cabinets, folders, notebook folders, discussion topics, and reference folders for notebooks that are in the context and the domain inheritance scheme that is in place. Contexts define a structure in which related information is organized. This structure can be represented by a domain hierarchy, folder hierarchy, product structure hierarchy, collection of discussion topics, or predefined milestones in a schedule. The structure defined by the context enforces consistency and improves efficiency.

The use of the context structure is very apparent when you look at how domains can help organize rules for users. For example, the Administrator user is associated with the site context /System domain and, therefore, is segregated from other users by default. The other users are associated with child domains of the /User domain. The User domain is in the site context, and the child domains of the /User domain can be in the site context or in an organization context.



---

## Installed Site Context Structure

The site context has the top-level / (root) domain, the /System, /Default, /User, and /SessionIterationDomain domains that are children of the root domain, and the /Unaffiliated domain that is a child of the /User domain. (For an explanation of these domains, see [Administering Domains and Policies on page 86](#).)

For Windchill PDMLink, Arbortext Content Manager, and Pro/INTRALINK, there are no folders installed in the site context.

For Windchill ProjectLink, the following folders, which are associated with /Default domain in the site context, are installed:

- Change Log
- General
- Policies

## Editing Context Structure

The context structure is set either by the load files used (in the case of the site context) or by the template selected when the context is created. The template (and its underlying code) sets the domains, cabinets, folders, notebook folders, discussion forum topics, and reference folders that are in the context and the domain inheritance scheme, which identifies parent and child domain relationships.

Although you can modify the set of domains in a context using the Policy Administration utility, you should refrain from doing so unless the purpose of the domain is clearly defined. For example, a new domain may be needed to provide a unique set of access control policy rules for a specific folder.

Windchill solutions do not expose the creation of cabinets through their user interface. Use the default cabinets defined. Administrators can update the set of folders available in a context by navigating to the specific product, library, project, program, or organization and then clicking the **Folders** link. Similarly, discussion forum topics can be created in a product, library, project, or program by clicking the **Discussions** link that is available from the product, library, project, or program.

## Context Participation

Participation items establish the following:

- Roles that are automatically available in a context.
- System groups that are automatically created in a context.

Product, library, project, and program contexts are associated with teams of users and user-defined groups. Any user can display all products, libraries, projects, or programs in which the user is identified as a team member. The users and user-

---

defined groups in a team are associated with roles that identify the responsibilities and permissions of the team members. For example, the Product Manager role establishes who is in charge of the product; similarly, the Project Manager role establishes who is in charge of a project.

The set of roles and system groups that are automatically available in a context consist of the roles and system groups established in parent contexts, as well as those defined specifically for the context.

If the team established is in a context that includes a shared team, the shared team roles and system groups are defined and managed in the organization context where the shared team was created.


## Installed Site Context Participation

Through the site context, roles and system groups that are useful throughout your Windchill solution are made available to the site.

### Roles

The roles that are available to the entire site are defined in the `<Windchill>\src\wt\project\RoleRB.rbinfo` resource bundle, which is translated to all supported languages and made available through the application clients.

All of these role names are available to all child organizations and then to the product, library, project, and program contexts created within those organizations.

To see the roles, navigate to **Organizations**  **► Roles**. For products, libraries, projects, and programs, click the **Team** link under the corresponding context.

### Groups

The following group is defined in the site context /System domain:

Administrators (known as the system or site administrators)

---

#### **Note**

This group defines the administrators for your entire site.

---

The following groups are defined in the site context /User/Unaffiliated domain:

- Attribute Administrators
- LifeCycleAdministrators
- Type Administrators
- Unrestricted Organizations
- WorkflowAdministrators

---

These groups and any other groups established when your Windchill solution is installed are used during the normal operation of your Windchill solution and should not be removed. Domain-based access control rules can be automatically loaded in the site context /System domain granting permissions to members of these groups, except the Unrestricted Organizations group. The rules for the members of the Unrestricted Organizations group are loaded in the site context /User domain.

## Editing Context Participation

Context participation is set by the template selected when the context is created. The roles defined in the template can be modified in the organization context as well as in an application context. Those roles defined in the organization are inherited by the child contexts of the organization.

From within an organization, use the **Groups** link to add or update user-defined groups and use the **Roles** link to add or remove roles from the organization.

From within a product, library, project, or program, use the **Team** link to add or remove roles. From the **Members** table, you also add and remove members from the roles. For additional information, see [Teams and Team Template Administration on page 297](#).

## Context Policies

Context policy items can include the following domain-based rules:

- Access control rules that establish the access control against specific participant, object type, life cycle state, and domain combinations.  
For example, there can be an access control rule for objects with the wt.doc.WTDocument object type in the /Default domain that gives read permission to the Engineers system group.
- Indexing rules that define which collections an object is included in when the object of a specified object type and domain combination moves to a specific life cycle state. Collections are used to create indexing lists which help improve performance when searching for objects.
- Notification rules that define which participants get notified when a specified event occurs for an object type and domain combination.

Contexts provide a means for controlling access to the contained information. In application contexts, access is controlled through context team membership, policy rules, and ad hoc rules. Context contents can be restricted so that access is limited to the members of a context team, or so that the context information can be made more broadly available to the enterprise through policies that grant additional participants (such as users, groups, or organizations) access to specific object types.

---

The policies that are in effect in a context are determined by the policies set in the domains that are in the current context, as well as those set in the parent domains. For details, see [Administering Domains and Policies on page 86](#).

## Installed Site Context Policies

The site context policies that are set consist of the domain-based access control rules and one indexing rule. No notification rules are set in the site context domains, and no policy rules are set in the site context /SessionIterationDomain domain.

---

### Note

Your solution may vary from the following description, as the name of the Administrators group, and the names of the some initial domains are configurable from the `wt.properties.xconf` file prior to the installation.

The following sections describe the rules that are set in the site context.

### Access Control Rules for / (Root) Domain

The following domain-based access control rules are set when the data is loaded during the installation. The rules are in the site context / (root) domain for all life cycle states. Permissions granted are indicated with a plus sign (+), permissions denied are indicated with a minus sign (-), and permissions absolutely denied are indicated with an exclamation mark (!).

For more information, see the Policy Administration help.

---

### Note

These rules ensure that users can operate within the Windchill solution and should not be changed without fully understanding the reason for the change.

Object Type	Participant	Permissions	Comment
AccessPolicyRule	ALL	+Read	Allows organization and application context administrators to see inherited access rules.
AdministrativeDomain	ALL	+Read	Allows all users

Object Type	Participant	Permissions	Comment
			to view domains.
DeliverableDefinition	ALL	+Read and +Create	Allows all users to create and read deliverable definitions.
EPMDocConfigSpec	ALL	+Full Control (All)	Allows all users to perform configuration management of business objects within their workspace when using Creo Parametric or other workgroup managers.
ExchangeContainer	ALL	+Read	Allows all users to complete a variety of general actions.
Meeting	OWNER	+Full Control (All)	Grants owners full access to meetings that they own.  For information about setting up meetings with WebEx, see the <i>PTC Windchill Specialized Administration Guide</i> .
NotificationSubscription	Administrators	+Full Control (All)	Grants administrators full access.
NotificationSubscription	ALL	+Read and +Create	Grants all users read and create access.
NotificationSubscription	OWNER	+Full Control (All)	Grants the owner full access.
Team	OWNER	Read	Grants the team

Object Type	Participant	Permissions	Comment
			owner read access.
WTDocumentConfig-Spec	ALL	+Full Control (All)	Grants full control to all users.
WTMarkup	ALL	+Read, +Download, and +Create	Allows all users to create and read markups. These permissions are required because view markups are not life cycle managed.
WTMarkup	OWNER	+Modify, +Modify Content, and +Delete	Allows the owner of a markup the ability to modify and delete it.
WTObject	Administrators	+Full Control (All)	Grants full control to all site administrators.
WTObject	View and Print Only	!Modify, !Modify Content, !Modify Identity, !Create By Move, !Create, !Set State, !Revise, !New View Version, !Change Domain, !Change Context, !Change Permissions, !Delete, and !Administrative	Absolutely denies users in the View and Print Only license group all permissions except those required to view and download objects.
WTPartConfigSpec	ALL	+Full Control (All)	Allows all users to perform configuration management of business objects within their workspace when using Creo

Object Type	Participant	Permissions	Comment
			Parametric or other workgroup managers.
WTRolePrincipal	ALL	+Read	Grants all users read access.
FvPolicyRule	ALL	+Read	Grants all users read access.
FvFolder	ALL	+Read	Grants all users read access.
FvHost	ALL	+Read	Grants all users read access.
FvVault	ALL	+Read	Grants all users read access.
ReplicaFolder	ALL	+Read	Grants all users read access.
ReplicaVault	ALL	+Read	Grants all users read access.
RootFolder	ALL	+Read	Grants all users read access.
Site	ALL	+Read	Grants all users read access.
DerivedImage	ALL	+Read, +Create, and +Download.	Allows all users to create, read, and download derived images.
DerivedImage	Team Members	+Full Control (All)	Grants full control to all team members.

---

### Access Control Rules for /User Domain

The following domain-based access control rules are set in the site context /User domain for all life cycle states:

<b>Object Type</b>	<b>Participant</b>	<b>Permissions</b>	<b>Comment</b>
WTGroup	Unrestricted Organizations	+Read	Allows read access to groups for the organizations that are in this group.
WTObject	OWNER	+Full Control (All)	Grants full control to the owner of an object.
WTUser	Unrestricted Organizations	+Read and +Download	Allows read and download access to users for the organizations that are in this group.

### Access Control Rule for /User/Unaffiliated Domain

The following domain-based access control rule is set in the site context /Unaffiliated domain (which is a child of the /User domain) for all life cycle states:

<b>Object Type</b>	<b>Participant</b>	<b>Permissions</b>	<b>Comment</b>
WTPrincipal	ALL	+Read	Allows read access to participants for all users.



---

### Access Control Rules for /Default Domain

The following domain-based access control rules are set in the site context /Default domain for all life cycle states:

Object Type	Participant	Permissions	Comment
Meeting	ALL	+Read	Allows read access to meetings for all users. This rule is used to provide visibility of WebEx meetings for all users.  For information about setting up meetings with WebEx, see the <i>PTC Windchill Specialized Administration Guide</i> .
RelationshipMap	ALL	+Read	This object type is used for collecting dependent objects when archiving objects. For details on archiving, see the <i>PTC Windchill Archive Administration Guide</i> .
NavigationFilter Template	All	+Read	Allows read access to all users.

### Access Control Rules for /System Domain

The domain-based access control rules set in the site context /System domain are used to control access to administrative objects. For normal operations, you should not modify these rules.

To view the rules, access the Policy Administration utility from the site context. For information about accessing the Policy Administration utility, see [Administering Domains and Policies on page 86](#).

---

## Indexing Rule for / (Root) Domain

The following indexing rule is set in the site context / (root) domain for all life cycle states:

Object Type	State	Collections	Comment
WTOBJECT	All	WbLib	Indexes all objects in all states and puts the indexes into the WbLib collection.

## Updating Context Policies

Use the Policy Administration utility to update context policies. For information about using the Policy Administration utility, see [Administering Domains and Policies on page 86](#).

## Context Data Types and Attributes

Data type and attribute items identify data types (defined as subtypes) and attributes that are in addition to the Windchill modeled classes.

The data types available in a context are determined by the data types defined in the organization context, as well as those defined in the site context.

For example, if your organization context has defined Plan and Report document subtypes, then these subtypes are available in any project, program, product, or library context created from your organization context.

## Installed Site Context Data Types and Attributes



All data types that are modeled in your Windchill solution are available for administrator use from the site context.

If Windchill ProjectLink is installed, then the following document subtypes are also available from the site context:

- Agenda
- General
- Minutes
- Plan
- Presentation
- Reference Document

---

## Editing Context Data Types and Attributes

You can use the **Type and Attribute Management** utility from **Site**  ► **Utilities** and **Organizations**  ► **Utilities** to view and edit data types and attributes.

During the installation process, an organization participant (the organization object) is created and associated with the site context. Any types owned by this organization participant are available to all organizations.

Each organization participant has an internet domain that is used to identify the organization contexts for subtypes and attributes. When subtypes and attributes are created, Windchill provides a suggested prefix for the name of the new type or attribute. The suggested prefix is based on the context from which the **Type and Attribute Management** utility is launched. The suggested prefix is the reverse of the internet domain for the owning organization participant of the organization context. For example, an organization with the internet domain, acme.com would suggest the prefix, com.acme.

For more information, see the help available from the **Type and Attribute Management** utility.

## Templates

Template items identify the templates that provide users with the required information used when creating and processing Windchill objects.

Windchill provides the following types of templates (not all types of templates are available from all Windchill solutions):

- Context templates provide the required and optional administrative items that are used to create context. There are five types of context templates:
  - Product templates define default values and other information, such as team roles and access policies, which are used when an administrator creates a product.
  - Library templates define default values and other information, such as team roles and access policies, which are used when an administrator creates a library.
  - Project templates define default values and other information, such as folder structure and team roles, which are used when an administrator creates a project.
  - Program templates define default values and other information, such as folder structure and team roles, which are used when an administrator creates a program.
  - Organization templates define default values and other information, such

---

as folder structure and user-defined groups, which are used when an administrator creates an organization context. Each Windchill solution provides a unique set of organization templates.

- Document templates provide content files and default values, which are used when users create different types of documents. For example, content might include skeleton documents for memos or reports.
- CAD document templates define the content and default values, which are used when users create CAD documents.
- Life cycle templates define the phases and gates associated with various business objects when the objects are initialized.
- Report templates define default values, which are used when users run reports.
- Team templates define default roles, which are used when users populate teams associated with life cycles.
- Workflow templates define default values, which are used when users initiate a workflow.
- Note templates provide a starting point for creating a note from standardized text that can be associated to parts. Note templates can be modified and attachments can be associated to communicate important information about a part.
- Task form templates contain various form fields, such as labels, text fields, and radio buttons. These form fields are place holders to display the attributes of a task like variables, process name and type to the task participant. For more information, see [Using Task Form Templates in a Workflow on page 344](#).

## Installed Site Templates

The templates loaded in the site context are associated with the /System domain.

The following sections describe the templates that are loaded and how to remove or hide templates.

---

### Note

**CAD Document Templates** and **Note Templates** appear in the list for Windchill PDMLink and Windchill ProjectLink, but do not have installed templates.

---

## Organization Context Templates

When Windchill PDMLink is installed, the following organization context templates are loaded in the site context:

- General (PDM)
- DemoTemplate (not enabled)

---

When Windchill ProjectLink is installed, the following organization context templates are loaded in the site context:

- General
- Enterprise
- Supplier
- Customer

For additional information about organization context templates, see [Out-of-the-box Organization Templates on page 147](#). For specific information about creating organization context templates, see [Organization Templates on page 396](#).

### Workflow Templates

The following workflow templates are loaded in the site context for all Windchill solutions:

- Submit
- Review

For Windchill PDMLink, the following workflow templates are loaded in the site context (these templates are not used by Arbortext Content Manager or Pro/INTRALINK):

- Problem Report Workflow
- Change Request Workflow
- Change Notice Workflow
- Change Activity Workflow
- Promotion Request Approval Process
- Promotion Request Review Process
- Variance Workflow

For Windchill ProjectLink, the following workflow templates are loaded in the site context:

- Approval Process
- Notify Process
- Release Process
- Review Process
- Two Level Approval Process

### Life Cycle Templates

For the details on out-of-the-box life cycle templates, see [Out-of-the-box Life Cycle Templates on page 306](#).

---

## Team Templates

Team templates are used with life cycle templates.

For Windchill PDMLink, the following team templates are loaded in the site context (these templates are not used by Arbortext Content Manager or Pro/INTRALINK):

- Default
- Change Activity Team
- Change Notice Team
- Change Request Team
- Promotion Request Team
- Variance Team
- Problem Report Team

For Windchill ProjectLink, there are no team templates loaded.

## Document Templates

For Windchill ProjectLink, the following document templates are loaded in the site context:

- Agenda Template
- Memo Template
- Minutes Template
- MS Project Plan Template
- Presentation Template
- Requirements Template

No document templates are loaded for Windchill PDMLink.

## Project Templates

For Windchill ProjectLink, the following project templates are loaded in the site context:

- Custom
- Design
- General
- Manufacturing

No project templates are loaded for Windchill PDMLink.

---

## Program Templates

For Windchill ProjectLink, the following program template is loaded in the site context:

- General

No program templates are loaded for Windchill PDMLink.

## Product Templates

For Windchill PDMLink, the following product templates are loaded in the site context:

- Demo Product Template (not enabled)
- General Product
- Product Design

No product templates are loaded for Windchill ProjectLink.

If Windchill MPMLink is installed then additional product and design templates are available.

## Library Templates

For Windchill PDMLink, the following library templates are loaded in the site context:

- Document Library
- General Library
- Part Library

No library templates are loaded for Windchill ProjectLink.

## Report Templates

For Windchill PDMLink, the following report templates are loaded in the site context (these templates are not used by Arbortext Content Manager or Pro/INTRALINK):

- All Average Change Notice Completion Time
- All Average Change Request Completion Time
- All Average Problem Report Completion Time
- All Change Notice Influx and Resolution
- All Change Request Influx and Resolution
- All Open Change Notices
- All Open Change Requests
- All Open Problem Reports
- All Problem Report Influx and Resolution

- 
- Average Change Notice Completion Time
  - Average Change Request Completion Time
  - Average Problem Report Completion Time
  - Change Notice Influx and Resolution
  - Change Request Influx and Resolution
  - Change Request Track Breakdown
  - ChangeNotice\_ChangeAdmin\_Given
  - ChangeNotice\_ChangeAdmin\_NotGiven
  - ChangeRequest\_ChangeAdmin\_Given
  - ChangeRequest\_ChangeAdmin\_NotGiven
  - Domain Reports
  - Open Change Notices
  - Open Change Requests
  - Open Problem Reports
  - Overdue Running Processes
  - Problem Report Influx and Resolution
  - ProblemReport\_ChangeAdmin\_Given
  - ProblemReport\_ChangeAdmin\_NotGiven
  - Process Initiated by Current User
  - Variance\_ChangeAdmin\_Given
  - Variance\_ChangeAdmin\_NotGiven

For Windchill ProjectLink, the following report templates are loaded in the site context:

- Project Action Items
- Project Activities
- Project Deliverables
- Project Milestones
- Project Summary Activities
- Project Tasks
- Project-Program Status Report Query
- Projects Created Query
- Projects Owned Query



---

## Task Form Templates

The following task form templates are loaded in the site context for all Windchill solutions:

Primary Business Object Class	Type	Name
wt.fc.WTObject	XDP	default
wt.fc.WTObject	JSP	default
wt.fc.WTObject	Native	default
wt.change2.WTChangeRequest2	Native	Analyze Change Request
wt.change2.WTChangeOrder2	Native	Audit Change Notice
wt.change2.WTChangeActivity2	Native	Complete Change Notice Task
wt.change2.WTChangeRequest2	Native	CRB Review Change Request
wt.change2.WTChangeActivity2	Native	Review Change Notice Task
wt.change2.WTChangeIssue	Native	Review/Approve Problem Report
wt.maturity.PromotionNotice	Native	Review/Approve Promotion Request
wt.change2.WTVariance	Native	Review/Approve Variance

## Editing Templates


To edit templates, navigate to the **Templates** table by clicking the **Templates** link within a specific context and then select the type of template from the table view drop-down list. The list of templates that are available from the context appears in the table. Each type of template has its own method of editing the templates. Generally, editing can be initiated either by clicking an icon at the top of the **Templates** table or selecting an action from a row in the table.

For details on templates and how to edit them, see the help that is available from the **Templates** table. For specific information about editing context templates, see [Context Templates on page 393](#).

## Removing, Hiding, or Disabling Templates

You can remove, hide, or disable the templates that have been loaded. If you do not want a template to be used by anyone, PTC recommends that you disable the use of the template instead of removing it. By disabling it, the template is not available for use in any context, but remains in the system in case it is needed in the future. If you do not want a template to be used in a specific context, but want to allow its use in other contexts, you can hide the template in the specific context and show the template in other contexts.

---

To view the templates that have been loaded, select **Site**  ► **Templates**. Select the type of template from the view drop-down list to display the templates in the table. You can then use the disable row action to make individual templates unavailable throughout the user interface or use the hide action to hide the visibility of individual templates in a specific context.

For additional help on template actions, click the help icon on the **Templates** table to display the templates help.

## Managing Document Template Preferences

When your Windchill solution is installed, default preference settings for document templates are established. For example, the default name of a document that is created from a template is set in the **Document from Template Filename** preference. You can change the defaults to better meet the needs of users by opening the **Preference Management** utility from within the context in which you want the settings to take effect. Document template preferences are listed under the **Documents** category.

## Object Initialization Rules

Object initialization rule items consist of documents that contain XML elements that are formatted according to the object initialization rules DTD and are used in the following activities:

- Initializing objects – Rules can define specific default attribute values that are used when instances of objects of a specific type are created.
- Constraining the display characteristics of attribute values – Rules can set the following types of constraints on attributes:
  - Hidden – the user interface does not display a value or label for the attribute.
  - Immutable – The user cannot change the attribute value that is being displayed.
  - Server assigned – The user interface does not display a value for the attribute; the value is generated and assigned when the instance of the object is saved.
  - Pregenerated – The user interface displays a value for the attribute. The value is generated before the attribute is presented in the user interface.
  - Discrete set – The user interface is constrained to picking from a discrete set of values.

Additionally, you can qualify when default values are set or when constraints are used for Windchill attributes by integrating the use of conditional logic algorithms in object initialization rules.

---

For details on the use of object initialization rules, see the Understanding Object Initialization Rules chapter of the *PTC Windchill Specialized Administration Guide*.

## Installed Site Object Initialization Rules

The object initialization rules established for each Windchill solution vary slightly, but include the following types of rule definitions:

- Out-of-the-box numbering and versioning schemes for parts, documents, CAD documents, dynamic documents, and change objects. These schemes are simple Oracle sequences that have been loaded into the Windchill database. Each starts at 1 and increments by 1.
- Default attribute values for folder paths, life cycles, and team templates for many object types.
- Display constraints on attribute values such as numbering, life cycles, team templates, and organization identifier.
- Conditional logic that allows for variations when setting constraints, numbering, versioning, and default attribute values.

For the complete set of object initialization rules established during the installation process, log in as the site administrator and navigate to **Site Utilities**. Open the **Object Initialization Rules Administrator** to view the rules.

---

### Note

The rules set in the site context work with the installed interface for each Windchill solution. PTC recommends that you do not modify the out-of-the-box object initialization rules that are set in the site context without understanding what the change affects.

---

Windchill PDMLink provides a demonstration template named Product Design that uses a different versioning scheme and two life cycle templates that you can use in evaluating what object initialization rules should be set for your site. For more information on the Product Design template, see [Out-of-the-box Product and Library Context Templates on page 182](#).

For additional information about the out-of-the-box numbering and versioning schemes, see [Administering the Numbering of Parts, Documents, CAD Documents, and Change Objects on page 104](#) and [Administering the Versioning of Parts, Documents, and CAD Documents on page 105](#).

For more information, see the help available from the **Object Initialization Rules Administration** utility.

---

## Adding and Changing Object Initialization Rules

You can add and change object initialization rules by using the **Object Initialization Rules Administration** utility or by including the rules in a context template.

For more information, see the Understanding Object Initialization Rules chapter of the *PTC Windchill Specialized Administration Guide*.

## Context Preferences

Preferences are used to enable, specify, or otherwise affect functionality within a particular context.

For more information, see the help available from the **Preference Management** utility.


## Creating the Contexts from which Users Work

All Windchill solutions provide the capabilities for creating organization and application contexts.


There is only one site context, which is created when your Windchill solution is installed. No additional site contexts can be created.

---

### Note

The base data installation can create an organization context. If one was not created by loading the base data, the site administrator creates the organization context from **Organizations** .

---

Application context managers can create application contexts. You become an application context manager for products, libraries, projects, or programs by being in the creators group for products, libraries, projects, or programs. The creators groups are maintained from **Organizations**  ► **Creators**. When you create an organization from Windchill ProjectLink, you can choose to automatically add those organization members who log on to the project creators group; you manually add users to the program creators group. In all other Windchill solutions, you manually add users to the product and library creators groups.

As part of the process of creating a context, you select a context template. Context templates provide the administrative items (as described in [Context Administrative Items on page 61](#)) that you want set in the context, thus establishing the initial context framework for users. For the details on creating context templates, see [Context Templates on page 393](#).

---

For information about creating organization contexts, see [Creating an Organization Context on page 155](#).

For information about creating product and library contexts, see [Products and Libraries on page 171](#).

For information about creating project and program contexts, see [Projects and Programs on page 233](#).

## Using Out-of-the-box Context Templates

Your Windchill solution provides a set of out-of-the-box context templates that you can use when creating contexts.

The text in the templates has been translated, and translated files are provided in the loadFiles and loadXMLFiles directories where your Windchill solution is installed. As part of the installation process, the installer can change the load set so that the base data loaded includes files translated into the language of choice at your site. The base data that is loaded determines which language set of context templates is available.

For details on setting which language files are used when loading base data, see the Database Initializing and Data Loading chapter of the *PTC Windchill Installation and Configuration Guide*.

Use one of the out-of-the-box organization templates when creating organization contexts, or you can create a customized organization template, as described in the next section.

For application contexts, you can use one of the out-of-the-box product, library, project, or program templates, or you can create additional application context templates, as described in the next section.

The details of what is in each out-of-the-box context template can be found in the following chapters:

- Organization templates are described in [Organizations on page 137](#).
- Product and library templates are described in [Products and Libraries on page 171](#).
- Project and program templates are described in [Projects and Programs on page 233](#).

For information on creating context templates, see [Context Templates on page 393](#).

---

 **Note**

The role names used in Windchill solution context templates are included as references to the `<Windchill>\src\wt\project\RoleRB.rbinfo` resource bundle so that when they are used, they appear in the language specified by the browser language. This means that the translated templates do not contain translated role names.

---

## Administering Domains and Policies

This section describes how Windchill domains and policies are defined. A domain is an administrative area that defines a set of administrative policies, such as access control, indexing, and notification. Objects associated with a Windchill domain are subject to its policies.

---

 **Note**

Windchill domains are not the same as internet domains.

---

A policy is a collection of rules designed for various types of objects associated with a domain. For example, an indexing policy consists of rules that determine the types of objects for which metadata should be entered into specified collections, when the objects belong to the domain.

Before creating a context in your Windchill solution, you should determine which domains are needed and use a template that creates the domains and the access control policies for those domains when you create the context. For details on what domains and policies are included in the out-of-the-box templates, see the following chapters:

- Organization templates are described in [Organizations on page 137](#).
- Product and library templates are described in [Products and Libraries on page 171](#).
- Project and program templates are described in [Projects and Programs on page 233](#).

For the details on creating additional context templates, see [Context Templates on page 393](#).

After a context is created, you can use the Policy Administration utility to administer the domains in the context.

---

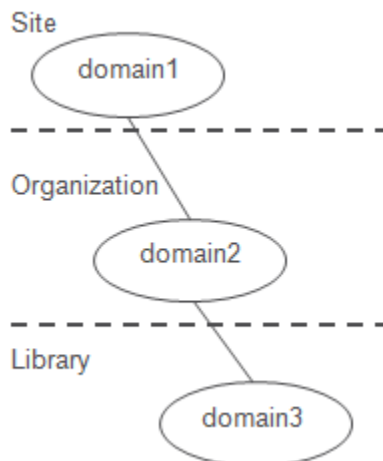
The following sections provide information about installed domains and how to use the Policy Administration utility to administer the domains.

## Context and Domain Hierarchy Overview

Context types have the following established hierarchy:



When each context is created, a set of domains is also created for use within the context. Generally, the domain hierarchy is established using the context hierarchy. A parent domain is either in the same context as its child domain or in the parent context of its child domain's context. In the following diagram, the site, organization, and library contexts are shown with one domain defined in each context. The domain hierarchy shows domain3 (in the library context) as a child of domain2 (in the organization context) and domain2 as a child of domain1 (in the site context):



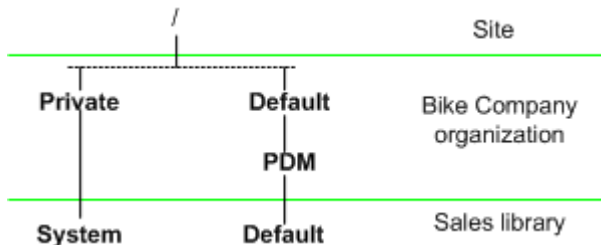
The actual domain structures are determined in part by whether an application context is created as a private context or a public context, or created using a shared team. The domain structure for the /Default domain in private contexts

starts under the /Private domain in the organization context. The domain structure for the /Default domain in public contexts and contexts using a shared team starts under the /Default domain in the organization context.

To illustrate the domain structures for shared team, private, and public contexts, consider the following examples:

- Assume that the Windchill installation creates the site context and has a child organization context that is named Bike Company, and that an administrator (using an out-of-the-box library template) creates a public library context using the following:
  - The team is a local team.
  - The context is named Sales and is a child of the Bike Company context.

Then the domain hierarchy for the Sales library is as follows:



From within the Policy Administration utility, the hierarchy is shown as follows:

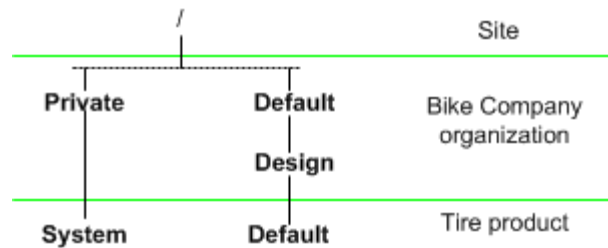
```

 / (Site)
 |-Default (Organization Bike Company)
 |--PDM (Organization Bike Company)
 |---Default (Library Sales)
 |-Private (Organization Bike Company)
 |--System (Library Sales)
  
```

- Assume that the Windchill installation creates the site context and has a child organization context that is named Bike Company, and that an administrator (using an out-of-the-box product template) creates a product context using the following:
  - The team is a shared team named Design.
  - The context is named Tire and is a child of the Bike Company context.



Then the domain hierarchy for the Tire product is as follows:



From within the Policy Administration utility, the hierarchy is shown as follows:

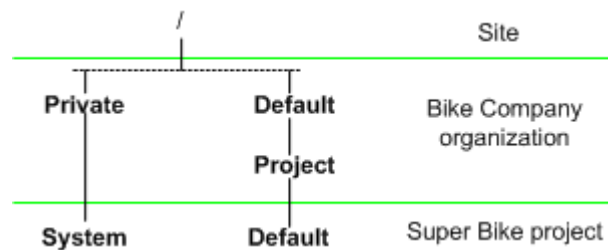
```

/ (Site)
|-Default (Organization Bike Company)
|--Design (Organization Bike Company)
|---Default (Product Tire)
|-Private (Organization Bike Company)
|--System (Product Tire)

```

- Assume that the Windchill installation creates the site context and has a child organization context that is named Bike Company, and that an administrator (using an out-of-the-box project template) creates a public project context using the following:
  - The team is a local team.
  - The context is named Super Bike and is a child of the Bike Company context.

Then the domain hierarchy for the Windchill ProjectLink Super Bike project is as follows:



From within the Policy Administration utility, the hierarchy is shown as follows:

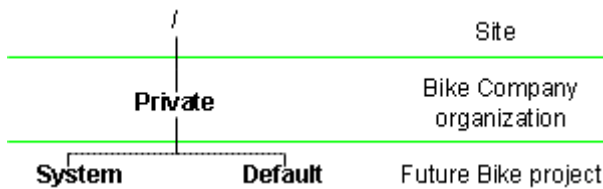
```

/ (Site)
|-Default (Organization Bike Company)
|--Project (Organization Bike Company)
|---Default (Project Super Bike)
|-Private (Organization Bike Company)

```

- ```
|--System (Project Super Bike)
```
- Assume that the Windchill installation creates the site context and has a child organization context that is named Bike Company, and that an administrator (using an out-of-the-box project template) creates a private project context using the following:
    - The team is a local team.
    - The context is named Future Bike and is a child of the Bike Company context.

Then the domain hierarchy for the Windchill ProjectLink Future Bike project is as follows:



From within the Policy Administration utility, the hierarchy is shown as follows:

```

/ (Site)
|-Private (Organization Bike Company)
|--Default (Project Future Bike)
|---System (Project Future Bike)

```

The domain hierarchy for the /Default domain in a product, library, project, or program depends on whether a shared team is used, or if a shared team is not used, on the **Private Access** selection. If a shared team is used, the **Private Access** selection is disabled. When creating a project (or program), the manager selects the **Private Access** option **Project Members Only** (or **Program Members Only**) to create a private project (or program) that uses a domain hierarchy branch that starts with /Private. Selecting any other **Private Access** option creates a public project (or program) that uses a domain hierarchy branch that starts with the /Default domain in the organization context.

When creating a product (or library), the manager selects **Yes** for the **Private Access** option to create a private product (or library) that uses a domain hierarchy branch that starts with /Private. Selecting **No** creates a public product (or library) that uses a domain hierarchy branch that starts with the /Default domain in the organization context.

The /Private domain in the organization context only contains an out-of-the-box policy rule granting access rights to the organization context administrators, which is why it is named /Private. The /Default domain and its child domains in the organization context have a set of out-of-the-box policy rules that provide access rights to a broader set of participants, and so application contexts inheriting from these domains are referred to as public contexts.

---

## Domains in the Site Context

When a Windchill solution is installed, the following domains are initially defined in the site context:

| Domain Names            | Description                                                                                                                                                                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| / (root )               | Sets rules that govern the entire enterprise.                                                                                                                                                                                                             |
| /System                 | Serves as the default domain for most system administration objects, including queues and life cycle definitions. /System is the default domain of the Administrators group.<br><br>The /System domain is not intended for general user business objects. |
| /User                   | Serves as the default domain for organization objects and as the parent domain for the /Unaffiliated domain and for organization context domains that hold the users (and their personal cabinets) for that organization.                                 |
| /Default                | Serves as the default domain for the initialization of business information objects.                                                                                                                                                                      |
| /SessionIterationDomain | Serves as the default domain for internal session processes. Do not modify the policies set for this domain.                                                                                                                                              |
| /Unaffiliated           | Serves as the default domain for users who are not associated with any organization. These users do not have the organization attribute set in their directory service entry. The /Unaffiliated domain is a child domain of the /User domain.             |

The root, /System, /User, and /Default domains cannot be moved or deleted. Also the domain names of these domains and of the /Unaffiliated domain are configured through the `wt.properties` file.

The /System, /User, /Default, and /SessionIterationDomain domains belong to the / (root) domain. Additional domains can be defined and associated with the root domain, or domains can be nested by defining them as children of another domain. This allows you to define a hierarchy of domains and then define policies at each level in the hierarchy.

---

## Creating Domains

Windchill automatically creates domains as follows:

- During installation, as described earlier in this chapter.
- When you create contexts. Each context template defines a set of domains that are created.
- Each time Windchill identifies a user that is affiliated with an organization that does not have an associated domain, Windchill creates the corresponding domain for the organization as a child domain of the User domain.

In addition, administrators can manually create domains.

The name of a domain can be a maximum of 200 characters. When Windchill automatically creates the domains associated with organizations, the domain name is usually the same as the organization name. However, organization names can be up to 200 characters. Therefore to name the domain, Windchill truncates the organization name to 193 characters. This allows Windchill to add a maximum of seven more characters to the domain name to identify a unique name when two or more organizations have the same beginning 193 characters in their names. When the truncated domain name is not unique, Windchill appends [1] to the truncated name. If appending [1] to the name does not make it unique, then Windchill appends [2] instead of [1]. If appending [2] does not make the name unique, then [3] is appended and so on until a unique name is found or until the maximum number of attempts to find a unique name is achieved. The maximum number of attempts is defined in the following property in the `wt.properties` file:

```
wt.inf.container.WTContainerServerHelper.maxDomainCreationAttempts
```

The default value for this property is 25.

If the organization name contains a forward slash (/), Windchill automatically converts the forward slash to a dash (-) in the domain name. For example, if the organization name is "ABC/Main", the domain name created would be "ABC-Main".

---

### Note

After Windchill creates a domain that is associated with an organization, an administrator can change the domain name to something more meaningful; Windchill does not rely on the organization domain name matching the organization name.

---

---

## Defining Domain-based Policies

Using the Policy Administration utility, you can create additional domains and define or change the rules set for each domain. For example, you can define the following:

- An access control policy, which determines a participant's permissions to access objects associated with the domain.
- An indexing policy, which determines the collections into which metadata for an object is entered when the object is in a specific life cycle state.
- A notification policy, which determines who is informed when an event of interest occurs to an object in the domain.

Load files can include sets of domain-based policies for access control and indexing. Templates that are used to create contexts can only include sets of domain-based policies for access control.

---







### Note

Policy rules apply to object types. Access to an instance of an object type can be governed by ad hoc access control rules in addition to policy rules.

For more information, see the Access Control chapter of the *PTC Windchill Specialized Administration Guide*.


---

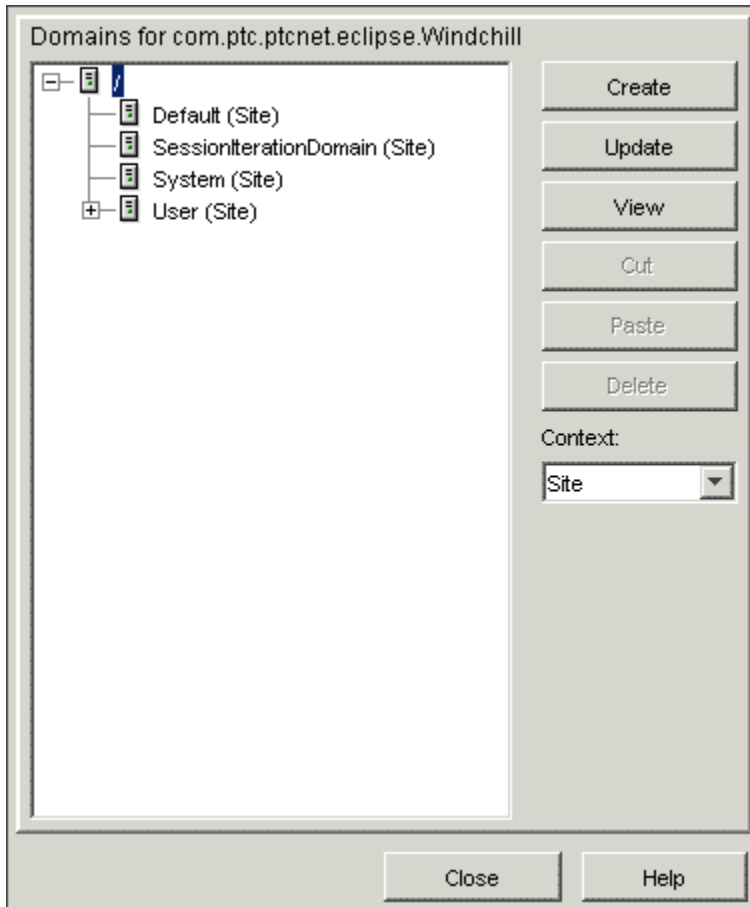
## Using the Policy Administration Utility

The **Policy Administration** utility initially operates within the confines of the context from which it is started. You can access the **Policy Administration** utility from the **Utilities** pages that are under the **Site** , **Organizations** , **Products** , **Libraries** , **Projects** , and **Programs** .

You begin policy administration on the **Policy Administration** window. From this window, you have access to the following domains:

- The domains that are in the current context.
- The parent domains of the domains in the current context.

When accessing the **Policy Administration** utility from **Site**  ► **Utilities**, the initial window is similar to the following:



The domains display in a tree view which is open to the domains at the top of the domain hierarchy within the current context. The current context appears selected in the **Context** drop-down list.

The format of each domain in the list includes the domain name followed by the following information in parentheses:

- The type of context (for organization and application contexts)
- The name of the context where the domain resides

For example, if a domain in the list is shown as **Default (Library Common Parts)**, then the domain name is Default and the domain resides in the library context named Common Parts. If the Default domain is in the Site context, then you will see **Default (Site)**. In this case, the context type is not displayed.

---

You can select any of the domains listed in the tree, or you can expand the tree to show child domains within the current context and then select a domain. You can also change the contents of the domain tree by using the **Context** drop-down list, as follows:

- Selecting a parent context from the **Context** drop-down list updates the domain tree so that the domains in the selected context and direct parent domains are available.

The contexts listed in the **Context** drop-down list are formatted as the context type followed by the context name.

- Selecting **All Contexts** from the **Context** drop-down list updates the domain tree so that all domains from all contexts are available.

---

 **Note**

The buttons that are enabled when you select a domain are determined by the **Policy Administration** utility. Buttons are disabled if the action cannot be performed on the domain based on current selections or if the action can never be performed on the domain; buttons are not disabled based on user permissions. For example, if you select a domain that can never be deleted (such as the Default (Site) domain), the **Delete** button is disabled. If a button is enabled and a user who does not have permission to execute the action clicks the button, the user receives an error.

---

## Specifying Policy Rules in a Context Template

For Windchill PDMLink, the recommended method for including a specific set of policy rules in a context template is to set the rules in an existing context using the Policy Administration utility. Then, either save the current context as a template or export the context to a ZIP file on your system. Be sure to select the **Access Policy Rules** option when you save or export an existing context. Using this method provides access control policy rules for domains within a context.

After you have a ZIP file containing the access control policy rules (along with any other administrative items you want in the template), import the template using the ZIP file as input.

For Windchill ProjectLink, you cannot save the policy rules set in the current context when creating a template from the current context or when exporting the context.

For the details on creating context templates, see [Context Templates on page 393](#).

---

## Assigning Domains to Folders in Solutions with Products and Libraries

When creating folders, the default behavior is that the domain associated with the new folder is the same domain that is associated with the parent cabinet or folder.

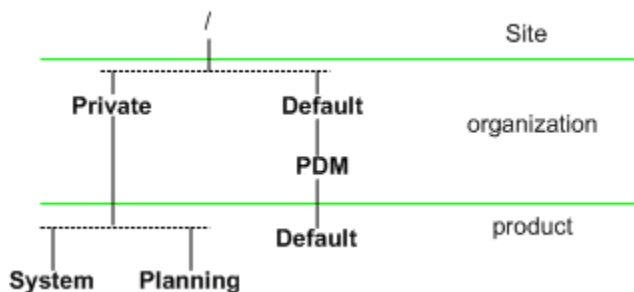
The ability to create folders is controlled through the access control policy rules that are set for folders. Out-of-the-box, only product or library managers and organization administrators (in Windchill solutions with products and libraries) and the site administrators (in Windchill solutions with products and libraries) can create folders (or update the domains in existing folders). To allow others to create folders, you can add access control policy rules that grant Create and Modify permission for the SubFolder object type to those participants who you want to have this capability.

For more information about adding access control policy rules, see the Access Control chapter of the *PTC Windchill Specialized Administration Guide*.

To allow those who can create folders the ability to associate a domain other than the domain that is associated with the parent folder, you must set the **Display Folder Domains** preference.

Setting this preference to true reveals domain information on the dialogs used when creating or updating folders and on folder information pages. Providing the domain information allows users who have the appropriate access control rights to assign different domains to folders and to see which domain is currently assigned to a folder. In Windchill solutions with products and libraries, the interface allows a user to select a domain from the domains established in the context other than the /System domain and any of its descendants. You can set this preference at any context level through the **Preference Management** utility from the product, library, organization, and site **Utilities** pages.

You can use the ability to create folders that are associated with a domain other than the domain that is associated with the parent folder in conjunction with the ability to create top-level domains in an application context. For example, assume you have created the /Planning domain in following domain structure for a product:





---

The access control rules in the /Planning domain only inherit the rules from the Site / (root) domain and the organization /Private domain and not the rules from the organization /Default and /Default/PDM domains. When creating folders in a product, the domain associated, by default, is the /Default domain in the product. By allowing the user to select a different domain, the user could select the /Planning domain instead of the /Default domain. Creating a folder associated with the /Planning domain provides a different access policy for objects in the folder since the access control rules for objects associated with the /Planning domain can be different than the rules associated with the product /Default domain and a different set of rules are inherited from the organization.

## Organization Domain Algorithm

Windchill requires that each organization context must be assigned to the same domain as the associated organization participant. Because the organization participant may already exist, it may be already associated with a particular domain. When a new organization context is created, the following steps occur behind the scenes the domain association of the organization participant may change.

1. Windchill determines if an appropriate domain exists.
  - If a domain with the same name as the organization already exists as a child of the site-level /User domain and an organization participant with the same name is associated with the domain, a new domain is not created.
  - If a domain with the same name as the organization already exists as a child of the site-level /User domain and an organization participant with the same name is not associated with the domain, a new domain is created and a naming algorithm is used to create a unique name. For more information about the naming algorithm, see [Creating Domains on page 92](#).
  - If a domain with the same name as the organization does not exist and an organization participant with the same name does not exist or there is an organization participant with the same name that is associated with one of the default domains (/User or /User/Unaffiliated), a domain with the name of the organization is created as a child of the site-level /User domain.
  - If a domain with the same name as the organization does not exist and there is an organization participant with the same name that is associated with another domain, a new domain is not created.
2. Associate the organization participant with the domain.

- If an organization participant with the same name already exists and is assigned to the /User or the /User/Unaffiliated domain, it is reassigned to the domain created in the previous step.
  - If an organization participant with the same name already exists and is assigned to another domain, the organization participant retains the same domain association.
  - If an organization participant with the same name does not exist, one is created and assigned to the domain created in the previous step.
3. Create the organization context and associate it with the domain associated with the organization participant. This will be either the domain created in step 1 or the domain with which the organization participant was originally associated.
  4. The domain created or found in step 1 is moved from the site level to the organization level unless the domain was associated with an organization participant but the domain name was not the same as the organization name.
  5. Access control rules are established for the domain.
    - If a new domain was created in step 1 or an existing /User/<organization name> domain was associated with the organization context in step 3, the following access control rules are established for the domain:

| Type           | State | Participant                |   | Permissions        |
|----------------|-------|----------------------------|---|--------------------|
| WTOrganization | All   | All Participating Members  | + | Read               |
| OrgContainer   | All   | All Participating Members  | + | Read               |
| WTObject       | All   | Organization Administrator | + | Full Control (All) |
| OrgContainer   | All   | <organization participant> | + | Read               |

- No access control rules are created if the organization context was associated with some other pre-existing domain in step 3. PTC recommends creating access control rules in the alternate domain to satisfy your business needs.

---

 **Caution**

Because access control policy rules are associated with a particular domain, if an organization changes domains, user access control may also change. Carefully review any policies associated with the domain to which the organization will move prior to creating a new organization context to avoid access control issues.

---

In the following example, an organization participant called Umbrella Division already exists and its domain is the site-level /User domain. A site-level /User/Umbrella Division domain does not exist. The following occurs when a new organization context is created:

1. A site administrator is creating a new organization context and selects the Umbrella Division participant for the **Organization Name**.
2. A new site-level domain named Umbrella Division is created as a child of the /User domain because the domain associated with the Umbrella Division participant is a child of the /User domain.
3. The Umbrella Division participant is moved to the new /User/Umbrella Division domain.
4. The Umbrella Division organization context is created and is associated with the Umbrella Division participant and the /User/Umbrella Division domain.
5. The /User/Umbrella Division domain is moved from the site level to the organization level.
6. The following access control rules are created in the /User/Umbrella Division domain:

| Type            | State | Participant                |   | Permissions        |
|-----------------|-------|----------------------------|---|--------------------|
| WTOrganiza-tion | All   | All Participating Members  | + | Read               |
| OrgContainer    | All   | All Participating Members  | + | Read               |
| WTObject        | All   | Organization Administrator | + | Full Control (All) |
| OrgContainer    | All   | Umbrella Division          | + | Read               |

---

In this example, an organization participant called Construction Machinery Corporation already exists and its domain named Machinery Division is a child of the site-level /User domain. The following occurs when a new organization context is created:

1. A site administrator is creating a new organization context and selects the Construction Machinery Corporation participant for the **Organization Name**.
2. A new domain is not created because the Construction Machinery Corporation participant is associated with a domain that is not a site-level /User/ Construction Machinery Corporation domain.
3. The Construction Machinery Corporation participant remains associated with the existing domain.
4. The /User/Machinery Division domain remains at the site-level.
5. The Construction Machinery Corporation organization context is created and is associated with the Construction Machinery Corporation participant and the existing domain. No access control rules are created since the domain associated with the organization participant already existed.

## Using Dynamic Roles

Dynamic roles can be used in setting up access control policy rules. They represent the system groups that are created for the roles assigned to team members in context teams and shared teams, and the system groups created in an application context representing the organizations that have members in the context team. For information about system groups, see [Teams and Team Template Administration on page 297](#).

Dynamic roles are available from the **Roles** tab of the **Access Control Rule** window of the **Policy Administration** utility and are maintained from the site and organization contexts as follows:

- In the site context, the dynamic roles consist of the following:
  - Organization roles that represent the system groups that are created in an application context representing the organizations that have members in the context team. There will only be organization roles for the organizations to which you have access. Each role name is the name of an organization participant and is qualified by the phrase **Organization Role**. Organization roles are automatically created; you do not create organization roles.
  - A context team role for each role defined in the `wt.project.RoleRb.rbinfo` file. Using the site context, you cannot create additional context team roles; however, as part of a customization,

---

you can change the content of the `wt.project.RoleRb.rbinfo` file. For information on modifying the content of `.rbinfo` files, see the *PTC Windchill Customization Guide*.

- In an organization context, the dynamic roles consist of the following:
  - Organization roles that represent the system groups that are created in an application context representing the organizations that have members in the context team.

There will only be organization roles listed for the organizations to which you have access. Each role name is the name of an organization participant and is qualified by the phrase **Organization Role**. Organization roles are automatically created; you do not create organization roles.

- The context team roles for the roles that are set as visible in the **Roles** table from a given organization context.

The initial set of roles that are visible in the **Roles** table from a given organization context is inherited from the site context. In an organization context, organization administrators can add, delete, show, and hide the context team roles displayed in the **Roles** table. Therefore, they can manage the set of context team roles that display in the **Roles** tab on the **Access Control Rule** window when the Policy Administration utility is launched from the organization context.

Policy rules that use dynamic roles can be set at the site and organization level. These rules are then inherited by domains that are children of the domain specified in the policy rule. This allows the administration of these roles and their access control policy rules to be at the organization (or site) level instead of at the application level. Setting rules at the organization (or site) level provides simplified administration for sites where many projects, programs, products, or libraries exist. If you set policy rules for dynamic roles in an application context, the rules only apply to that context.

Dynamic roles can be used by editing the existing access control policy rules through the Policy Administration utility or by creating organization and application templates that use dynamic roles as participants. For more information about dynamic roles and examples of their use, see “Dynamic Role Use in Access Control Rules” in the PTC Windchill Help Center.

Out-of-the-box, the following dynamic roles can be created from a template:

- Package Creator
- Received Delivery Manager

PTC provides sample XML files that you can use to create a set of new templates that specify dynamic roles in the access control policy rules for an organization context. The sample files are located in the `<Windchill>/LoadXMLFiles/dynamicRole` directory, where `<Windchill>` is the location where Windchill is

---

installed. Using the following sample files, you can create a set of dynamic role templates and then use the templates when creating your organization context and child application contexts:

- `generalOrganizationTemplate.xml`
- `generalLibraryTemplate.xml`
- `generalProductTemplate.xml`
- `generalProjectTemplate.xml`



In the sample organization template XML file, dynamic roles are identified in `WTPrincipalReference` elements using the `groupName` and `groupType` subelements. Dynamic roles have the same names as the system group that they represent. To identify the participant in an access control policy rule as a dynamic role, the value of the `groupType` element must be `DynamicRole`. For example, the following `WTPrincipalReference` element is used to identify the Team Members dynamic role:

```
<WTPrincipalReference isInternal="true">
  <groupName>teamMembersgroupName>teamMembers>
  <groupType>DynamicRoleDynamicRole>
</WTPrincipalReference>
```

When the sample organization context template is used to create an organization context, the set of access control policy rules defined in the template establishes the policy rules that are in place in the context. Then the rules are inherited in the child application contexts that are created. When creating the child application contexts, the sample dynamic role product, library, and project templates should be used. The access control policy rules that are set in the organization context have been removed from these templates.


## Using Dynamic Roles in a New Organization

To use dynamic roles in access control policy rules for a new organization, perform the following actions:

1. Navigate to **Site**  ► **Utilities**.
2. Set the view to **Organization Templates**.
3. Click the create template icon .


The **New Organization Template** wizard opens.

4. Browse to the location of the `generalOrganizationTemplate.xml` sample file that contains access control policy rules for dynamic roles. Select only the file that pertains to the organization context.
5. Supply a unique **Organization Template Name**.
6. (Optional) Provide a description of the template.
7. Click **OK**.


- 
8. Navigate to **Organizations**  ► **View All**.
  9. Create a new organization using the organization template you just created.

For more information on creating a new organization, see the Organization Administration help.

For the new templates to be used, the product, library, project, and program creators must select the appropriate application template when creating their application context. To ensure that the appropriate templates are chosen, complete the following actions:

1. Navigate to the **Organizations**  ► **Templates** page for the new organization that you created in the previous procedure.
2. Set the view to the appropriate context. For example, select **Product Templates**.
3. Create a new context template using the appropriate sample template content file that is in dynamicRole directory described earlier (for example, `generalProductTemplate.xml`).
4. In the same view, hide the out-of-the-box templates so that the people creating new application contexts do not see them when they create new contexts. For example, select **Hide** from the actions list for the General Product template.
5. Repeat steps 2 through 4 for each application context template type: product, library, and project. To create a program template that uses the access control rules for dynamic roles, modify the sample project template so that it works for programs.

## Using Dynamic Roles in an Existing Organization

If your site already has an organization context and would like to update the organization context to set up policy rules that use dynamic roles, the access control policy rules for the existing organization and child contexts can be modified using the **Policy Administration** utility found on **Organizations**  ► **Utilities**.

After setting new access control policy rules in an organization context that uses dynamic roles, you need to create new application context templates that do not duplicate the rules set at the organization level. To accomplish this you can use the sample templates provided by PTC as described in the previous section. The rules set at the organization level will then be inherited by the child application contexts.

---

# Administering the Numbering of Parts, Documents, CAD Documents, Managed Baselines, and Change Objects

Numbering schemes control how numbers are generated for parts, documents, CAD documents, managed baselines, and change objects. Each object class has its own numbering scheme.

For all Windchill solutions, a rules load file sets the initial numbering rules for documents, CAD documents, parts, and change objects. These rules affect the following:

- Documents, CAD documents, parts, managed baselines, and change objects created from within a product, library, organization, or site context (if Windchill PDMLink is installed)

---

## Note

Autonumbering must be turned on for the Dynamic Document subtype and its subtypes. See [Configuring Products or Libraries for Dynamic Documents on page 224](#).

---

- Documents, CAD documents, and parts created from within a project, organization, or site context (if Windchill ProjectLink is installed)

## Out-of-the-box Numbering Schemes

The loaded numbering schemes for parts, documents, CAD documents, managed baselines, and change objects are simple Oracle sequences that have been loaded into the Windchill database. Each starts at 1 and increments by 1. This means that the numbers for all parts, documents, CAD documents, managed baselines, and change objects are autogenerated according to the numbering scheme that is in place.

## Changing Numbering Schemes

To change an out-of-the-box numbering scheme, you can change to a scheme that is defined for you or you can define your own scheme. You can view the rules that are being used for numbering from the **Object Initialization Rules** table using the **Object Initialization Rules Administration** utility.

Object initialization rules can be set in context templates or by using the **Object Initialization Rules Administration** utility from within a specific context.



---

For details on how to change a numbering scheme, see the Object Initialization Rules chapter of the *PTC Windchill Specialized Administration Guide*.

For the details on creating context templates, see [Context Templates on page 393](#).

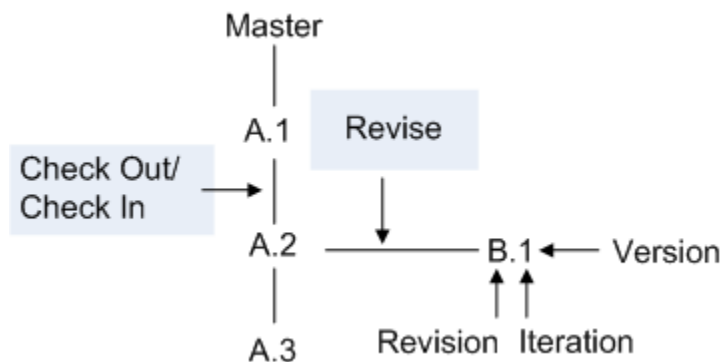
For details on accessing the **Object Initialization Rules Administration** utility see the Object Initialization Rules chapter of the *PTC Windchill Specialized Administration Guide*.

## Administering the Versioning of Parts, Documents, and CAD Documents

Versioning schemes define the labels, or identifiers, that are automatically applied as object versions are created in a Windchill solution.

### Understanding the Use of Versioning Schemes

The following diagram and the sections that follow provide some context on how versioning schemes are used:



#### Master

When users create a document or part, your Windchill solution creates a master as well as an initial version, which is identified in the previous diagram as revision A, iteration 1 (A.1). The master consists of common attributes for all versions, such as part number or document name.

#### Version

The version of a part or document is identified by the combination of revision and iteration.

---

## Revision

When users select the **New Revision** action, your Windchill solution creates a new version as the start of a new revision of the part or document. For example, if the previous version was A.2, the new revised version would be B.1.

## Iteration

When users select the **Check Out** action, modify the part or document, and select the **Check In** action, your Windchill solution creates a new version of the part or document as the next iteration of the current revision upon check in. For example, if the previous version was A.2, the new iteration would be version A.3.

## Initial Versioning Rules

For all Windchill solutions, load files set the initial versioning rules for parts, documents, and CAD documents in the site context. These rules affect the parts, documents, and CAD documents created from within a product or library.

The default versioning scheme used is set when site context rules are established unless you choose to set them in an organization, product, or library context. The out-of-the-box demonstration template named Product Design sets versioning for a product context. For details on the Product Design template, see [Out-of-the-box Product and Library Context Templates on page 182](#).

---

### Note

PTC recommends that you establish one versioning scheme for all of your contexts and that you set the versioning scheme in the site context. However, you can override the default versioning scheme for a specific organization, product, or library context.


---

Documents, CAD documents, and parts that are created from within a project or program context are not versioned objects.

---

## Preferences for Revision Labels

The **Revise** category in the **Preference Management** utility has the following preferences for changing the user interface to allow users to select the revision label:

- **Allow Override On Revise** – when set to **Yes**, activates the set revision icon  on the **New Revision** window. This allows users to select the next revision label from a drop-down list or enter a valid revision label.
- **Allow Override On Insert** – when set to **Yes**, allows users to select the revision label from a drop-down list or enter a valid revision label when inserting an object.
- **Allow Override On Create CAD Document** – when set to **Yes**, allows users to select the initial revision label from a drop-down list or enter a valid revision label when creating a CAD document.

By default, these preferences are set to **No**.

Additionally, if you are using file-based or state-based versioning scheme, you can define alternate revision labels for revisions. For more information, see the Object Initialization Rules chapter of the *PTC Windchill Specialized Administration Guide*.

## Changing Versioning Schemes

To change an out-of-the-box versioning scheme, you can change to a scheme that is defined for you or you can define your own scheme. You specify the versioning scheme in an object initialization rule for a particular object type, such as wt.doc. WTDocument. You can view the rules that are being used for versioning from the **Object Initialization Rules** table using the **Object Initialization Rules Administration** utility.

Object initialization rules can be set in context templates or by using the **Object Initialization Rules Administration** utility from within a specific context.

For more information about changing a versioning scheme, see the Object Initialization Rules chapter of the *PTC Windchill Specialized Administration Guide*.


For more information about creating context templates, see [Context Templates on page 393](#).

## Administering Preferences

Administrators for the site, organization, and other application contexts (such as a projects, programs, products, or libraries) can set preferences for the contexts which they administer.

---

To access the preferences for a particular application context, click the **Preference Management** link on the **Utilities** page of that application context. The complete list of preferences for that context is displayed.

Site and organization administrators can switch between contexts by clicking the find icon  next to the **Context** field at the top of the page, and searching for other available application contexts.

Preference values set at one level are inherited by the application contexts below. For example, preference values set at the site level are inherited by the organization; application contexts within the organization inherit preference values from the organization, as shown in the following figure:



---

 **Note**

User preferences can be inherited directly from the organization level, from individual application contexts, or can be unique (able to be set only at the user level).

Preference values can be set for each application context, or for an individual user, unless the preference value is locked at a higher level. For example, if a preference is not locked at the organization level, then it may have one value at the organization level, but individual products or projects within that organization could each specify a different value. Similarly, if a preference is not locked at an organization level, but is available at the user level, individual users could each set different values for that preference.

Preferences can be locked at any level above the individual user. If a preference is locked, then the value cannot be changed for any lower levels. A site or organization administrator can choose to delete all values for a particular preference that may be set at levels below the current context. These values at lower levels are known as child instances.

---

If a preference is not explicitly set for a particular application context, then the value for that preference is inherited from the level above. For example:

- If a preference is not set for a particular product or project, then the value set for that preference at the organization level is used.
- If the preference is not set at the organization level, then the value set for that preference at the site level is used.
- If no preference is set at any level, then the default value defined for that preference is used.

For more information on managing preferences, see the help available from the **Preference Management** utility.



# 4

## Best Practices for Monitoring and Maintenance

Regular monitoring and maintenance administrative activities are essential to maintaining the health of your Windchill system. A Windchill deployment is a complex system with multiple components and data repositories. Proper monitoring and maintenance of Windchill is an ongoing process consisting of a number of tasks and checks that should be performed at regularly scheduled intervals.

Neglect of essential maintenance tasks, lack of regular system monitoring, and failure to properly configure alert notification settings can lead to unexpected system outages, data loss, and lost productivity.

Regular maintenance and proactive monitoring by the administrator will contribute greatly to the ongoing health, performance, and availability of the Windchill system. Since maintenance activities include backups, this also assures data integrity over time. Performing regular maintenance also promotes faster troubleshooting if an error occurs.

PTC provides tools for you to use in your monitoring and maintenance activities, as well as guidance in using third-party utilities. These tools and activities are detailed in the *Best Practice Activities for Windchill System Monitoring and Maintenance* document, found on the PTC Reference Documents website using the following URL:

[http://www.ptc.com/view?im\\_dbkey=123340](http://www.ptc.com/view?im_dbkey=123340)






# 5

## Understanding the Site

Site Administration Overview.....	114
Typical Duties of Site Administrators .....	114
Out-of-the-Box Site Configuration .....	131
Site Administration Best Practices .....	131

This section provides an overview for administering the site and describes the typical duties that a site administrator performs. It also provides additional information about some of the main administrative tasks for sites.


For details on performing many of the tasks described in this section, and additional information on the **Site**  context, see the Site Administration online help.

---

## Site Administration Overview

The site administrator manages the organizations within the site and is responsible for the common information and rules inherited by all contexts within the site. For general information about context contents and how to create contexts, see [Contexts – Distributed and Hierarchical Administration on page 59](#).

The site administrator (for example, wadmin) created at installation time may be a temporary administrator specified only to get the system up and running. If that is true, create a user who is associated with the hosting organization and add that person to the Administrators group. That person will then take over as the site administrator once the initial installation and setup is completed.

The general information in this chapter pertains to all Windchill solutions. The site administrator performs most of these actions from **Site**  on the **Navigator**.

## Typical Duties of Site Administrators

Site administrators are responsible for the configuration and management of the Windchill system as a whole. They create organizations representing business units of a hosting company and organizations representing partners and suppliers. Site administrators control how authorized users are added to the system. They also define the information that is common across all organizations and their products, libraries, projects, and programs.

Typical duties of the site administrator include the following:


- Create and update organizations participating in the site.
- Determine if new organizations are subscribers (able to host product, library, project, or program contexts).
- Manage a group of users with site administration privileges.
- Manage site-level folders, documents, and links.
- Manage site-level types and type-specific attributes that are inherited by all contexts.
- Manage the rules governing object creation.
- Manage site-level templates that are inherited by child contexts.
- Manage site-level object initialization rules that are inherited by child contexts.
- Create and manage security auditing reports for audit records of who did what causing changes in the Windchill database.
- Manage site configuration (such as vaulting, replication, calendar, property options, and preferences).

- 
- Create profiles to define which parts of the user interface (e.g., actions, tabs, and attributes) should be visible to users, groups, or organization members. Site administrators determine whether application context managers can override profiles that are created at the site context.
  - Manage processes (such as workflow, life cycles, CAD viewable publishing, and replication).
  - Manage package configuration
  - Manage security access for workflow expressions.
  - Export and import site-level information.
  - Define and manage reports.
  - Determine searchable object types.
  - Manage saved searches.
  - Manage site-level access policies and rules.
  - View and manage access control rules for individual objects.
  - Make program contexts visible and available for use in your Windchill solution.
  - Add participants to applicable license groups. Currently, the View and Print Only license group is available.
  - Creating public information page tabs visible to all users

## Creating and Managing Organizations

When a Windchill solution is created, an organization participant is created and associated with the site context. The default data loading process creates an initial organization context, also associated with the organization participant. Both the site and this initial organization have the same name. If the data loading process was modified so that the organization context is not created, you must create an organization context before users access the solution.


Users who have an organization attribute (the "o" attribute, by default) on their directory service entry that matches the organization participant's name automatically become members of that organization. If your site does not use the organization attribute in the directory service entry, users can be assigned to an organization using the usersOrganizationName property. For more information on using this property, see *Configuring Additional Enterprise Directories in the PTC Windchill Installation and Configuration Guide*.

Organization contexts are created by site administrators from **Organizations** . For more information, see [Creating an Organization Context on page 155](#).

---

## Note

Site administrator users, such as wadmin, should not be used to create contexts (products, libraries, projects, or programs) within organization contexts, nor should they create objects within those contexts.

The site administrator can review the list of organizations in the site and navigate to update each of the organizations from the **Organizations** page, accessed by clicking the **View All** link on **Organizations** . (The **Organization** page is visible only to site administrators.) A company will probably choose to administer the organizations representing their partners or customers. In this way, you become the organization administrator on behalf of any number of organizations defined in the site.

For more information on organizations, see [Understanding Organizations on page 137](#).

## Adding and Editing Members

You control how users are added to the site to enable them to log on and view and author information in the site. You can add and edit users using the **Participant Administration** utility. You can also define the users who have site administration privileges so that several individuals in the company can perform this duty.

For more information about using the **Participant Administration** utility, see [Using the Participant Administration Utility on page 265](#).

## Creating and Managing Site Folders and Documents

You can define documents, folders, and links within the site context. The site folders are intended to hold any documents that are important for administering the site.

Types of documents that administrators might define at the site include the following:


- Site configuration documentation.
- Site change log that captures a record of changes made to the site.
- Operation rules and procedures (such as shutdown, backup, and restart procedures).
- Site administrator responsibilities document.
- Key contact list for site administrators.

- 
- Deployment schedule and plans (this might also be defined in a project but referenced by providing a link in the site folder).
  - Documents describing site-level document, life cycle, and workflow templates.

## Changing Default Configuration Options

You can use properties and preferences to change the configuration options that are set by default. Preferences are accessed using the **Preference Management** utility on the **Utilities** page for a context. Properties are contained in properties files in your codebase.

## Managing Site-level Types and Type-specific Attributes

Using the **Type and Attribute Management** utility from **Site**  **Utilities**, you can define object types and type-specific attributes to make available to all organizations in the system. For example, a company might define a change impact report document type with specific attributes for several categories, including replacement cost, production tooling cost, and so forth.

You can define types and attributes within a context of an organization. When subtypes and attributes are created within an organization context, they are kept separate from all other organizations and remain private to the organization they are created in. For more information about types and attributes, see the help available from the **Type and Attribute Management** utility.

You can associate document types with life cycles which identify the various states of maturity of the document. For more information about life cycles, see [Life Cycles on page 299](#).

## Configuring Numbering and Versioning Schemes and Units of Measure

You can configure the number and version schemes used to uniquely identify parts, documents, and other items in the system. The site-level schemes and units of measure are inherited by the organizations, but each organization can optionally define its own schemes or override the site-level schemes. In general, when a company is hosting Windchill for its use, the numbering, versioning, and units of measure should all be defined at the site context and should not be overridden by individual organizations. This approach ensures consistency of basic identification and units across the company.

For more information on numbering, see [Administering the Numbering of Parts, Documents, CAD Documents, Managed Baselines, and Change Objects on page 104](#).

---


For more information on versioning, see [Administering the Versioning of Parts, Documents, and CAD Documents](#) on page 105.

For more information on units of measure, see the online help available from the **Type and Attribute Management** utility.

## Managing Site-level Templates

A company may choose to define a number of document, life cycle, and workflow templates that they want all their business units and partners to use. For example, the site may want to define a document template and associated life cycle and workflow process for capturing enhancement requests for the Windchill system. Or a company may want to make a corporate presentation template available to all its business units.

The site can define product, library, project, program, and organization templates. Organization templates are required to create organizations. For more information, see [Understanding Context Templates](#) on page 393.

You can restrict which templates are made available to the applications within the site by choosing to hide certain templates at the site level. For more information, see the help available from **Site**  **► Templates**.

## Managing Site-level Object Initialization Rules

You can configure how attributes (such as number) are displayed and generated using the **Object Initialization Rules Administration** utility. This utility defines how the initial attribute values for the object are established, how the attributes are displayed, and can determine basic relationships, such as life cycle association, when an object is created. The rules established by the parent site are inherited by each organization by default, but they can be overridden at the organization level. The rules are defined in an XML format, which the site administrator can view and edit.

For more information, see the Object Initialization Rules chapter of the *PTC Windchill Specialized Administration Guide*.

## Managing Workflow Security

Workflow authors are permitted to write workflow-embedded Java code to facilitate the execution of the workflow process. This embedded Java code is executed on the server, and there are no restrictions on the APIs available for use.

Considering this capability, a user with permissions to create workflow templates (for example, a project or program manager) could add malicious code in one of the workflow expressions, causing a possible security threat. For this reason, workflow templates that contain Java expressions must be written, reviewed, and thoroughly tested by individuals that are trusted by the organization. The site

---

administrator has an additional level of control to prevent a user who is not a member of at least one of three specific site context groups (Administrators, Workflow Administrators, or Workflow Authors) from embedding Java code in workflows.

For more information about workflow security, see [Workflow on page 337](#).

## Auditing System Information

The auditing framework provides a mechanism to enable event-based logging that provides a historical record of who did what that caused changes in the Windchill database. The security auditing feature also provides a mechanism to retain historical records of security related events, such as privilege changes, team changes, and denial of access. Security audit reporting is helpful to customers in highly regulated industries that need to identify events that may have resulted in a potential security breach.

The only events that are enabled out-of-the-box are system usage, organization usage, cross site request forgery events, and download events. Any other specific events that you want recorded in the audit log must be enabled on an individual basis. For more information, see the Auditing Administration online help.

## Creating and Managing Profiles

You can dynamically control which actions are visible to a user, group of users, or users in an organization by associating that information with a profile. Profiles are not an access control mechanism; they are a user interface control mechanism. A profile represents a typical category of user within a company and is based on the roles and privileges associated with that particular user category.

Profiles expose only the necessary functionality and information needed by a user. This creates a focused and simplified user interface, reducing confusion by eliminating areas of the user interface that could be distracting.

For more information about profiles, see [Profile Management on page 291](#).

## Configuring External Vaults or Replication Sites to Optimize Performance

You can configure external file vaults so that document and part content is stored on a file system rather than in the database. This type of configuration can provide significant upload performance improvements and is appropriate when the site is frequently used to exchange large files (such as CAD model files).

By default, external storage rules are based on individual domains in each context. You can launch the External Storage Administrator client from the **Utilities** page in the context of a product, a library, or the site. (The client is not available from the context of a project, program, or organization.) When launched from a product or

---

library context, product and library managers can set only the vaulting rules. The additional functionality within the External Storage Administrator is available only to site administrators. The client allows you to create vaulting rules for the System and Default domains associated with the context in which the client is launched.

---

 **Note**

The rules needed for setting up an external file vault for a product or library cannot be inherited from the site.

---

If the increased number of vaults and file vault rules becomes unmanageable, you can force vaulting to be accomplished through a single vault by setting the `wt.fv.forceContentToVault` property to true. For how to set external file vault rules or set up a single vault, see the External File Vaults chapter of the *PTC Windchill Enterprise Administration Guide*.

You can also configure replication sites so the document and part content files are replicated at a remote site where local users have only very low bandwidth connections to the Windchill server. You can launch the **File Server Administration** client from the **Utilities** page in the context of a product, a library, or the site. For a project or program, you can launch the **Content Replication Rules** from the project or program **Utilities** page.

---

 **Note**

The **File Server Administration** is not available from the context of an organization.

---

As a site administrator, you would typically define only the replica site and the replication schedule. The product, library, project, or program managers would configure the replication rules for a particular context. The additional functionality within the **File Server Administration** is available only to site administrators.

For more information on content replication and how to set replication rules, see the External File Vaults chapter of the *PTC Windchill Enterprise Administration Guide*.

## Configuring and Managing CAD Publishing Utilities

You can configure CAD workers that publish viewables for CAD models that can be accessed by participants that do not have native CAD authoring tools. The site includes utilities to configure the CAD workers and monitor and manage the publishing schedules and queues.




---

For more information, see *PTC Windchill Visualization Services Administrator's Guide*.


## Manage Package Configurations

Before your site begins working with packages, there are some optional configurations to consider. All of these features are available through the use of a type-based property. These properties are established in an XML file that is then loaded into Windchill and enabled through the **Preference Management** utility. You can enable any of these options for each package type available at your site.

For more information, see the *PTC Windchill Customization Guide*.

Feature	Default Behavior	Optional Behavior
Filtering Options	<p>You can apply filters to the package content through the <b>Set Collection Rules</b> window, which is available when creating a package or when adding content to a package. Applying the filters from this window refreshes the package content and reapplies the collection rules.</p>	<p>If you enable the filtering property, the edit filters icon  appears in the <b>Package Content</b> table and the <b>Edit Filters</b> action appears in the package <b>Actions</b> menu. In addition to the default behavior of applying filters, you can now apply filters to the package without refreshing the content and reapplied the collection rules. It also provides visibility to the package contents excluded by the filters.</p>
Content File Inclusion	<p>All content files associated with the package contents are included in the delivery ZIP file. Content files associated with the <b>Include in Delivery Attachments</b> table are also included. Content files associated with the package contents can be filtered out based on the file extension when locking the package.</p>	<p>If you specify the content role of files using the <code>IncludedContentRoles</code> property, additional files that match the specified content roles and are attached to the package object are included in the package ZIP file. The files that are attached through the <b>Include in Delivery Attachments</b> table are included regardless of the property setting. Files included because of the property setting are visible only in the resulting ZIP file.</p> <p>If you enable the <code>EnableContentControl</code> property, the <b>Select Files</b> action is available when the package is locked. Using the <b>Files</b></p>

Feature	Default Behavior	Optional Behavior
		<p>table, you can manually exclude content files from the package prior to creating the ZIP file. This allows an additional level of control over the ZIP file contents. The action is only available for packages, technical data packages, CDRL packages, or SDRL packages.</p> <p>For more information, see the Files Table help and the Best Practices for Working with Packages help.</p> <p>If you enable the <code>ExcludedMemberContentRoles</code> property, you can filter content files based on content role. Files filtered by content role or by file extension do not appear in the <b>Select Files</b> table, if you have it enabled.</p>
Zipping Options	<p>The <b>Zip Package for Delivery</b> action has three components that are configurable: Format Option, Delivery Option, and Manifest Option. For packages, technical data packages, CDRL packages, and SDRL packages, the package ZIP file supports either the export only or PTC Windchill 10.2 format (depending on licensing), the offline viewer, and an</p>	<p>Depending on which properties you choose to enable, multiple configurations for the ZIP file are available. These include the type of delivery and the type of manifest. For details about each of these options, see the following topics in the Packages - Exchanging Design Information help</p> <ul style="list-style-type: none"> <li>• Format Options</li> <li>• Delivery Options</li> </ul>

Feature	Default Behavior	Optional Behavior
	<p>incremental delivery. For replication packages, the package ZIP file supports the PTC Windchill 10.2 format and an incremental delivery, but no manifest file.</p>	<ul style="list-style-type: none"> <li>• Manifest Options</li> </ul> <p>If you enable only one option for choice for any of these options, that choice is used when the ZIP file is generated. If more than one choice is defined per option, the user is presented with a set of choices when generating the ZIP file.</p> <p> <b>Note</b></p> <p>If you allow incremental deliveries of a package, the initial delivery of a package is always a full delivery and other options are disabled.</p>

## Creating, Updating, and Managing Reports

You can create and update reports against the objects and attributes in the system as a whole. For more information about reporting functionality, see the help available from the **Reports** table.


## Importing and Exporting Information Among Systems

You can exchange information between a staging server and production server, between servers, or between a server and a file system using the Windchill import/export utilities. These utilities read and write system information in an XML format. For information on exporting and importing XML template files, see [Creating the Contexts from which Users Work on page 84](#).

The workflow and life cycle administration utilities accessible to the site and organization administrator integrate the import and export functions with administering workflows and life cycles. For life cycle import and export information, see [Importing and Exporting Life Cycle Templates on page 326](#). For workflow import and export information, see the help available from the **Workflow Template Administration** utility.

---

## Managing Calendar Settings

The **Calendar Management** utility, available from **Site**  ► **Utilities**, allows you to view and change calendar schedules, and delegate work to others.


As the site administrator you can set up the calendar environment for the system to include non-working days such as company holidays. For more information, see the help available from the Calendar Management utility.

## Monitoring Enterprise Systems Transactions Log

If you configured Windchill to exchange information with an Enterprise Resource Planning (ERP) system, you can monitor the transactions with the ERP system through the Enterprise Systems Transactions Log.

For more information, see the *ERP Connector Administration Guide*.

## Purge, Archive, and Restore Jobs

You can create and manage purge jobs with the **Purge Management**, accessed from **Site**  ► **Utilities**. You can create purge jobs to permanently remove data from the Windchill system, or (if the archive functionality is installed at your site) you can create an archive of the data to restore at a later time.

For more information, see the help available from the **Purge Management**.


## Managing Searches

You can search for and delete searches created by other users. This can be useful if a user or other administrator has created saved searches, but has since left the company.

You can also set many search related preferences for your site such as determining whether a search includes only the latest version of an object rather than all versions, or setting the default types to search for global searches, and lock the preferences so that they cannot be changed at a lower level.

For more information, see the **Search** tab of the **Navigator**.

## Creating and Managing Access Control Policy Rules

The **Policy Administration** utility is used to create access control policy rules that control the level of access to information in the system. To establish site-level policies, create those policies that apply to all organizations in the system from **Site**  ► **Utilities**. For example, as site administrator, you may want to give an engineering group read access to all documents of type Engineering Specification. You need to first define an Engineering Group and populate it with the appropriate

---

members, then define a document type of Engineering Specification at the site level, and then use the **Policy Administration** utility at the site level to define the access policy based on the document type, the group or groups provided access and the access level.

Another way to centralize the administration of access control policy rules is to use the dynamic roles that are available from the **Roles** tab in the **Policy Administration** utility. By using dynamic roles, you can create access control policy rules in the root domain from the site context that apply to the members of roles in the local and shared teams that inherit the rules. For additional information, see [Using Dynamic Roles on page 100](#).

In the root domain (/), you should create only those site-level policies that apply to the types of information that is available in all contexts. In some cases (such as with administrative items like document templates), the rules in place grant broad access. In other cases, you may want to grant more restrictive access.

For more information about access control, see the Access Control chapter of the *PTC Windchill Specialized Administration Guide*.

## Viewing and Managing Access Control Rules for Objects

You can view both the ad hoc and policy access control rules that are set for objects (such as folders, parts, and documents) and then manage the ad hoc access control rules for the objects. Navigate to the object, and select the **Edit Access Control** action, depending on your configuration. Using this action you can view access control for the object and set ad hoc access control rules for the object.

For more information, see the Access Control chapter of the *PTC Windchill Specialized Administration Guide* and the “About Security Management” topic in the PTC Windchill Help Center.

## Creating Public Information Page Tabs

You can create custom information page tabs that can be **Set Public**, making them visible to all users in your site, in every organization.

For more information about creating and managing information page tabs, see the Site Administration help.

---

## Exporting and Importing All Shared and System Table Views

---

### Note

For information on exporting and importing selected shared and system table views, see [Exporting and Importing Selected Shared and System Table Views](#) in the PTC Windchill Help Center.

---

A site administrator can export all shared and system table views from a Windchill system. This export includes:

- All system table views (the table views provided when the product was installed)
- All shared table views created by a site administrator
- All shared table views created by an organization administrator

The exported table views can be imported to another Windchill system, so long as both Windchill systems are of the same release level. For example, you can export all shared and system table views from a test system and import them into a production system of the same release level.

1. Open a windchill shell.
2. Run the following command:

```
windchill com.ptc.core.htmlcomp.tableview.ixb.TableViewIXUtil -f <file_name>  
-u <user_name> -p <password>
```

where

- *<file\_name>* will be the name of the exported file.
- *<user\_name>* is the user name of a user with site administrator privileges. Optional.
- *<password>* is the password for the user. Optional.

---

### Note

If *-u* and *-p* are omitted, the system will prompt for credentials.

---

For example, to export all published and system table views to a file named `export.jar` by a user whose user name is `wcadmin` and password is `wcadmin`, use the following command:

```
windchill com.ptc.core.htmlcomp.tableview.ixb.TableViewIXUtil -f export.jar
```

---

```
-u wadmin -p wadmin
```

To import the exported table views, use the **Import/Export Management** utility. For more information, see *Working with the Import/Export Management Utility* in the PTC Windchill Help Center.

## Managing Arbortext Editor Installation Bundles

Before Arbortext Editor can be downloaded by users from the PTC server, Arbortext Editor installation bundles must be made available from the user's **Software Downloads** page. To accomplish this, an Arbortext section must be added to the **Software Downloads** page, and Arbortext Editor installation bundles be made available for download. Available installation bundles can later be updated or removed from the **Software Downloads** page. Only site administrators can perform these tasks.

An installation bundle is an executable file (.exe) approximately 60 MB in size that is created using the Arbortext Editor Deployment Kit. For more information, see the *Arbortext Editor Deployment Kit Guide*, available from your Arbortext Editor Help Center.

### Adding the Arbortext Section to the Software Downloads Page

To add the Arbortext section to the user's **Software Downloads** page, use the following procedure:

1. Open a windchill shell.
2. Run the following command:

```
cd bin
```

3. Run the following command:

```
ant -f setupAE.xml enableSoftwareDownloads
```

4. When prompted to authenticate, provide the username and password of a user with site administration privileges.

When any user now views their **Software Downloads** page, an **Arbortext** section appears. A message displays indicating that no downloads are available at this time.


Running this command also creates the **Arbortext Downloads** folder in the **Site**  **Folders** table.



---

## Making Arbortext Editor Installation Bundles Available For Download

To make an Arbortext Editor installation bundle available for download, use the following procedure:

1. Navigate to **Site**  **Folders**.
2. From the **Folders** table, select the **Arbortext Downloads** folder and click **New Document** to upload the installation bundle as a Windchill document. (The **Arbortext Downloads** folder is automatically created when the command in the previous section is run.)
3. On the **New Document** window, specify the following information in the appropriate fields:
  - **Name**—Enter the text that you want displayed to users on their **Software Downloads** page. As a best practice, include the Arbortext Editor version (including the datecode) and indicate whether the bundle is targeted for a specific user community. For example: “Arbortext Editor 5.4 M020 for the Engineering Group”.
  - **Local File Path**—use the exact file name of the installation bundle as provided by Arbortext information architect.
  - **Location**—ensure that the location is the **Arbortext Downloads** folder.

Accept the defaults or follow your company’s best practices to fill in the other fields.

4. Click **OK**.

After a short delay, the installation bundle will appear as a hyperlink under the **Arbortext** section on the user’s **Software Downloads** page.

More than one installation bundle can be available for download.

## Updating Arbortext Editor Installation Bundles

When an update to an installation bundle is received from the Arbortext information architect, a site administrator can update the installation bundle using either the **Replace Content** or the **Check Out and Edit** action for the document. Only the latest iteration of the document is displayed on the **Software Downloads** page, along with the last updated date.

---

### **Note**

If the document containing the installation bundle is checked out, the installation bundle does not display on the **Software Downloads** page.

---

---

Keep in mind the following best practices when updating installation bundles:

- Use the check-in comments to indicate who provided the new installation bundle iteration, when it was received, and so on. These comments are visible on the information page for the document, where they provide useful information for the administrator. The comments are not visible on the user's **Software Downloads** page.
- If the disk space used by each iteration of an installation bundle (approximately 60MB) is a concern, use the **Delete Non-latest Iterations** action to remove previous iterations.

### Removing an Installation Bundle From the Software Downloads Page

To remove an installation bundle from the **Software Downloads** page, making it unavailable to users, use one of the following options:


- Use the **Delete** action on the document containing the installation bundle. The document is deleted from the **Arbortext Downloads** folder, and is no longer available to users.
- Revert to a previous version of the document by downloading the desired iteration, and checking it in as the new latest iteration.
- Change the lifecycle state of the document to **Canceled**. The document remains in the **Arbortext Downloads** folder, but is no longer displayed on the user's **Software Downloads** page. This option is useful for retaining a record of installation bundles used, or for retaining the installation bundle for future use.

## Managing Overall System Configuration

There are many system configuration settings you can view, set, and update remotely using the system configuration utilities. Use these utilities to view and set system properties, view and manage queues, and view server status and logs.

For more information, see the *PTC Windchill Specialized Administration Guide* and the *PTC Windchill Enterprise Administration Guide*.

## Making Program Contexts Visible

By default, programs are hidden. To make programs visible and available for use in your Windchill solution, you can set the value of the **Display ► Hide Program** preference to “No”. This preference is available from the **Preference Management** utility on **Site**  **► Utilities**. For more information on managing preferences, see the help available from the **Preference Management** utility.

---

## Administering the Windchill Mobile App

---

### Note

The Windchill mobile app requires a separate license. Ensure that your site has purchased this license before continuing.

---

A site administrator must configure the Windchill mobile app to connect it to the site's Windchill data. The configuration steps are described in the following topic in the Windchill Help Center: Administrator Actions for Windchill Mobile App. Once the mobile app has been configured, you can configure attribute layouts and set preferences related to the mobile app. For information on how users will download the app and connect to Windchill, see [Connecting to Windchill from Your Mobile Device](#) in the Windchill Help Center: .

## Out-of-the-Box Site Configuration

When your Windchill solution is installed, the following are defined for the site:

- Context structure; for more information, see [Installed Site Context Structure on page 65](#).
- Context participation; for more information, see [Installed Site Context Participation on page 66](#).
- Context policies; for more information, see [Installed Site Context Policies on page 68](#).
- Context data; for more information, see [Installed Site Context Data Types and Attributes on page 74](#).
- Context templates; for more information, see [Installed Site Templates on page 76](#).
- Context rules; for more information, see [Installed Site Object Initialization Rules on page 83](#).

## Site Administration Best Practices

This section includes best practices that are recommended for all Windchill solutions on [page 131](#) and for Windchill solutions with products and libraries on [page 135](#).

### For All Windchill Solutions

The following best practices are recommended for all Windchill solutions.

---

## Managing User Licenses

In an out-of-the-box installation, the View and Print Only license group and profile is available. A policy access control rule limits the members of this group according to the license agreement with PTC. Users in this group are able to search for and view object information, download attachments, and view markups. The group is associated with the View-Print profile, which reduces visibility to actions unavailable to participants with the profile applied.

For more information, see the Windchill License Groups topic in the Windchill Help Center.

## Establishing Site Administrators

When Windchill is installed, an administrator user is established (for example, wadmin). This initial administrator is verified any time the method server is restarted. The initial administrator is also the first member of the Administrators group. In an out-of-the-box installation, the members of the Administrators group have full control over all Windchill objects and are commonly called the system or site administrators. While it is possible to use this initial administrator to create other contexts and establish teams, PTC recommends creating another site administrator to oversee context creation and management. Creating another administrator improves the performance of Windchill start-up. You can create another site administrator using the **Participant Administration** utility by assigning a user to the Administrators group.

## Enabling Display of Quantity, Unit, and Reference Designator Attributes on Substitute Parts

You can choose to enable the display of the **Quantity**, **Unit**, and **Reference Designator** attributes on substitute parts on the **Structure** tab of the part information page. This functionality can be enabled at either the site or the organization level.

To enable this functionality:

1. In the **Preference Management** utility, set the **Part Management ▶ Enable quantity and reference designators for substitute parts** preference to **Yes**.
2. In the **Type and Attribute Management** utility, display the **Part Master** type.
3. On the **Layouts** tab for the **Part Master**, select the **Part Structure Replacement Attributes** layout.
4. Add the **Quantity**, **Unit**, and **Reference Designator** attributes to the layout.
5. Save the layout.

The **Quantity**, **Unit**, and **Reference Designator** attributes will now display on the **Attributes** tab for substitute parts on the **Structure** tab of the part information page.


---

## Displaying Alias Attribute Information for a Workflow Primary Business Object on the My Tasks Table

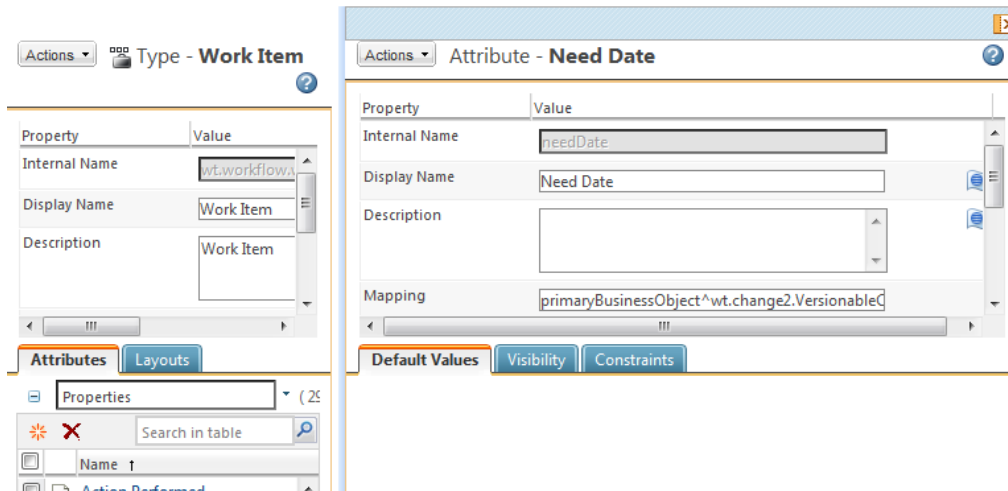
A workflow process is typically launched in the context of a primary business object (PBO), such as a change notice, change request, change task, or promotion request. Site and organization administrators can choose to display attributes from the primary business object on a work item as columns in the **My Tasks** table for a user by:

1. Mapping an alias attribute on the **Work Item** type to the desired attribute on the primary business object. For more information, see the Creating a New Attribute and Alias Attribute Mapping help topics in the PTC Windchill Help Center.
2. Creating or editing a table view on the **My Tasks** table to include the alias attribute mapped in step 1. For more information, see the Creating and Editing New Table Views help topic in the PTC Windchill Help Center.
3. Share this table view with all users in your site or organization. For more information, see the Administering Table Views for the Site or Administering Table Views for the Organization topics in the PTC Windchill Help Center.

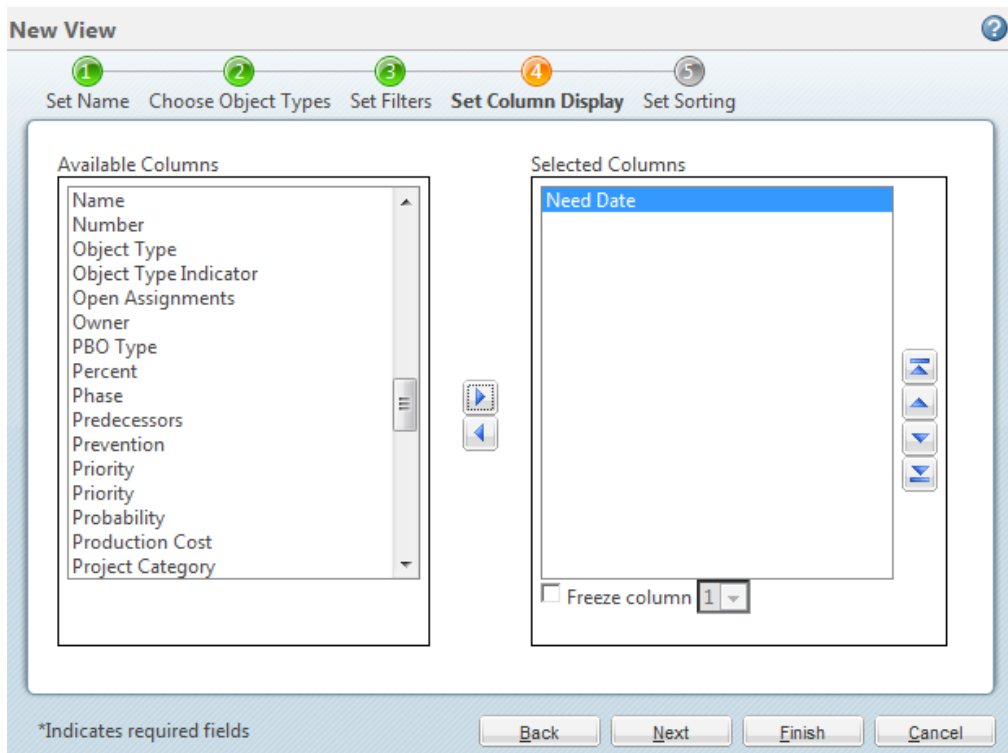
For example, to display the **Need Date** attribute of a change task on the assigned work item on a user's **My Tasks** table:

1. In the **Type and Attribute Management** utility, view the **Work Item** type.
2. Select **Edit** from the **Actions** menu to enter edit mode.
3. Click the new attribute icon .
4. On the **Define Attributes** step, specify the **Internal Name** for the attribute as "needDate", and select the **Alias** type for the attribute.
5. On the **Choose Data Type** step, select **Date and Time**.
6. On the **Set Properties** step, specify the following mapping syntax for the **Mapping** property: *primaryBusinessObject^wt.change2.VersionableChangeItem~needDate*

- Click **Save** to finish creating the attribute.



- From the **My Tasks** table on the **Home** page, select **Customize** from the view drop-down list, and create or edit a view.
- (Optional) On the **Set Name** step of the **New View** or **Edit View** window, ensure that the **Share with all users** checkbox is selected, if you want to make this table view available to all users.
- On the **Set Column Display** step, select the **Need Date** attribute.



- Click **OK**.

---

When users select the table view, the **Need Date** attribute will now display as a column in the **My Tasks** table.

## For Windchill Solutions with Products and Libraries

The following best practices are recommended for Windchill solutions that use products and libraries.

### Setting Object Initialization Rules

The object initialization rules include the ability to set default values and display characteristics for the following attributes:

- Folder paths
- Default life cycle template
- Default team template
- Default numbering scheme
- Default version scheme

Additionally, rules can be used to set the following:

- Available life cycle templates
- Attribute values
- Display characteristics for other attributes

Although these rules can be set for individual product and library contexts, PTC recommends that you set them at either the organization or site level so that an entire organization or site is using the same set of rules. This promotes reuse and reduces unnecessary duplication at lower context levels.

For more information, see the Object Initialization Rules chapter of the *PTC Windchill Specialized Administration Guide*.

### Setting Up Enhanced Life Cycle Templates

The Product Design template introduces default settings different from those established out-of-the-box at the site level. The out-of-the-box Product Design template includes object initialization rules that set simplified life cycle templates and versioning schemes for the following objects:

- Parts
- Documents
- CAD Documents

Unless you have overriding business practices that require unique rules, PTC recommends that if you want to use these features, you modify the site object initialization rules and remove them from the Product Design template.

---

## Overriding and Reassigning Life Cycle and Team Templates

The life cycle and team templates for objects such as parts and documents can be manually selected during object creation. For existing objects, life cycles can be reassigned and team templates can be reset.

For more information, including the preferences used to enable this functionality, see [Overriding and Reassigning Life Cycle and Team Templates on page 329](#).

## Enabling Set Revision While Creating a New Object

You can enable the revision of a part or document to be set when the part or document is created.



### Note

This functionality can be enabled at either the site or organization level.

---

To enable this functionality, add the **Revision** attribute to the **Create New Layout** for the object. Click the edit icon next to **Revision** in the layout, and set the value of the **Data Utility Id** property to `revisionPicker`. The **Revision** field will now display for all users on the object creation window. For more information on attribute layouts, see the Type and Attribute Management help in the Windchill Help Center.

To limit the set of users who have the ability to set the revision on a part or document when the object is created:

1. Create a profile which includes the **Restricted Directory Search** attribute on the **Set Attribute Visibility** step.
2. Set the constraint for the **Restricted Directory Search** attribute to **Hide Attribute** in the **Global Attributes** table.
3. Add all users to the profile for which you want to hide the **Revision** attribute.
4. Create a second profile which includes the **Restricted Directory Search** attribute on the **Set Attribute Visibility** step.
5. Set the constraint for the **Restricted Directory Search** attribute to **Edit Attribute** in the **Global Attributes** table.
6. Add the users or groups to the **Profile Members** table for which you want to expose the **Revision** label.

The **Revision** field will now display on the object creation window only for the specified set of users. For more information on creating and managing profiles, see the Profiles help in the Windchill Help Center.




# 6

## Understanding Organizations

Organization Administration Overview .....	138
Typical Duties of Organization Administrators .....	139
Out-of-the-box Organization Templates .....	147
Creating an Organization Context .....	155
Owning Organization Participants .....	158
Using the Organization Utilities Page .....	161
Changing an Established Internet Domain .....	162
Using the OrganizationSync Utility for User Organization Changes .....	162
Best Practices .....	164

This chapter provides an overview for administering organizations and describes the typical duties that an organization administrator performs. It also provides additional information about some of the main administrative tasks for organizations.

For details on performing many of the tasks described in this section, and additional information on **Organizations** , see the Organization Administration Tools online help.

---

## Organization Administration Overview

Organization administrators are responsible for the configuration and management of an organization within the Windchill system. The organization may represent a business unit of the parent company hosting the Windchill system or it may represent a supplier or partner to the parent company. In an exchange environment, an organization represents a company paying for the ability to create projects.

There are two types of organizations, an organization participant (WTOrganization type) and an organization context.

- An organization participant (made up of an object of type WTOrganization and a directory server LDAP entry) represents a group of users. Each organization participant can be associated with and manage an organization context that allows creation of products, libraries, projects, and programs within that organization.

Not every organization participant should have a corresponding organization context. Only create an organization context if the organization participant has a need to manage its own products, libraries, projects and programs.

---

### Note

Within the user interface, for example within the **Policy Administration** utility, you may see the current organization participant represented by "This Org", rather than the organization participant's name.

---

For more information on organization participants, see [Participants \(Users, Groups, and Organizations\)](#) on page 251.

- The organization context is associated with an organization participant, and provides the framework from which other application contexts (products, libraries, projects, and programs) can be created, and organization-level administrative actions can be carried out, as discussed in this chapter.

The development of products and the subsequent management of product information throughout their entire life cycle can be a collaborative process involving a number of organizations, including suppliers, contract manufacturers, and design partners. Windchill uses organization contexts as follows:

- To define your digital product value-chain.
- To define data ownership responsibilities.
- To define the level of engagement that organizations have within your system and business processes.

---

All Windchill solutions, when configured, contain an initial organization context. This organization represents your enterprise and is associated with the organization participant created during installation.

In your Windchill solution, organization contexts (and corresponding organization participants) can be created for each of the business organizations or business units that are collaborating together through the Windchill solutions. Each organization inherits templates (document, workflow, and life cycle templates) and has access to user-defined groups defined in the parent site context. You can then define organization-specific templates, user-defined groups, types and roles. A separate group of administrators (the Organization Administrator group) is associated with each organization to manage the organization templates, user-defined groups, and policies. The organization administrator can control who is allowed to create application contexts (products, libraries, projects, and programs) within their organization.

---

 **Note**

PTC recommends that if you are considering using multiple organization contexts in the future, you should create at least one additional organization context under which your products, libraries, projects, or programs are created, rather than creating them within the initial organization context. This allows you to add additional organizations (participants and contexts) without having to restructure your administrative data (such as subtypes) so that members of one organization cannot see data from another organization.

---

Windchill solutions provide client user interfaces for doing most activities that are related to administering organizations. Organization administrators define the information that is common across all products, libraries, projects, and programs created within their organization.

This chapter contains information that an organization administrator needs to know, as well as information that a site administrator needs in order to make the organization functional.


## Typical Duties of Organization Administrators

Responsibilities of the organization administrator include the following:

- Managing organization members, groups, roles and shared teams
- Creating, updating, and managing organization folders and documents
- Managing organization-level types and attributes
- Managing organization templates

- 
- Managing object initialization rules
  - Auditing activities within the organization
  - Creating and managing profiles
  - Creating and managing access control policy rules
  - Viewing and managing access control rules for individual objects
  - Configuring numbering and versioning schemes
  - Monitoring and managing viewable publishing
  - Viewing reports
  - Importing and exporting information
  - Purging, archiving, and restoring jobs
  - Managing organization preferences
  - Undoing a user checkout
  - Creating public information page tabs visible to all users in the organization

## Managing Organization Members, Groups, Roles, and Shared Teams

From **Organizations** , you control the users who can administer the organization (known as organization administrators) using the **Administrators** page and those who can create and administer application contexts (products, libraries, projects, and programs) using the **Creators** page.

To enable a user to create products, projects, libraries, or programs, the user must be added to the Product, Project, Library, or Program Creators group for the organization. Only members of the organization can be added to the creators groups. Additionally, organization and site administrators who are members of the organization can create products, libraries, projects, or programs; otherwise, you must be a member of the project creators group to create projects, a member of the program creators group to create programs, a member of the product creators group to create products, or a member of the library creators group to create libraries within the organization.

In Windchill ProjectLink, all members of the organization, by default, are allowed to create projects and administer the projects they create. However, if the organization is set up so that members are not automatically added to the project creators group and empowered to create projects, you must manually add members to the project creators group. Organization members must be manually added to the program creators group in order for them to create a program. Projects are considered the least formal of the application contexts (product, library, project, and program), so it is generally appropriate to allow all users to create and administer a project.

---

User-defined groups created at the site and organization level can be used when members create product, library, project, program, and shared teams or when access policies are defined. For example, an organization may want to define user-defined groups for each of the functional teams with membership in the organization. For example, assume that the organization defines a sales and marketing group, an engineering group, a publications group, and a quality control group. These user-defined groups can then be added as members of a product or project team without adding each member individually. Furthermore, when user-defined groups are updated, the updates can be refreshed to update all the teams referencing the user-defined groups without the need for each product or project manager to update their team membership.

For additional information about updating team membership, see [Context Teams on page 298](#).

Shared teams minimize user administration by allowing a collection of roles and associated participants (a shared team) to be used in many application contexts. Any changes to a shared team are immediately available in the contexts where the shared team is used. By default, the site administrator can create shared teams in any organization context and organization administrators can create shared teams in their organization context. Additionally, on the **Creators** page, you control who can create shared teams by adding users to the shared team creators group. Adding a user to this group allows the user to create shared teams from the organization **Teams** page.

For additional information about creating and managing shared teams, see [Shared Teams on page 298](#).

An organization inherits the roles defined at the site (as defined in the system roles resource bundle). All the roles from the RoleRB.rbInfo file are displayed on the organization **Roles** page. Organization administrators can explicitly hide the roles that they do not want their organization to use.

For more information, see [Creating an Organization Context on page 155](#).

## Creating, Editing, and Managing Organization Folders and Documents

Organization administrators can create folders, documents, and links in the organization **Folders** page. The following are examples of the types of documents that administrators might create at the organization level:

- Organization configuration documentation.
- Organization environment change log that captures a record of changes to the organization.
- Organization administration rules and procedures.
- Internal training information for organization administrators.

- 
- Key contact list for organization administrators.
  - Documents describing organization-level types, document templates, life cycle templates, and workflow process templates.

## Managing Organization-level Types and Attributes

Organization administrators can create and modify subtypes and relationship constraints in the organization context; however, they cannot create or modify global attributes, units (quantities of measure and measurement systems), or global enumerations unless they are part of the Attribute Administrators group. You can use existing global attributes, units, and global enumerations created by the site administrator on types for your organization.

When subtypes and attributes are created within an organization context, they are kept separate from all other organizations and remain private.

For more information about types and attributes, see the help available from the **Type and Attribute Management** utility.

## Managing Organization Templates

An organization context can define a number of document, life cycle, and workflow process templates that can be used by all the application contexts within the organization. To ensure consistency and maximize efficiency, an organization may want to define templates for specifications, presentations, reports, proposals, meeting minutes, and so forth. Life cycle and workflow process templates may be associated with each of the defined templates. Each organization inherits the templates defined in the site and can either use these site-defined templates or override them by defining organization-specific templates with the same name.

The organization can inherit the product, library, project, and program templates defined at the site level, or you can override these templates by defining templates for your organization. If Windchill ProjectLink is installed, you can create project and program templates. If Windchill PDMLink is installed, you can create product and library templates. For more information, see [Understanding Context Templates on page 393](#).



You can restrict which templates are made available to the applications within your organization by choosing to hide certain templates at the organization level. By only hiding templates, you limit the templates displayed by default and still allow context managers to override which templates are hidden in their particular application context. If you want to prevent a template from being used, you can disable it.

For more information, see the help from **Organizations**  **Templates** table.

---

## Managing Organization-level Object Initialization Rules

You can configure how attributes (such as number) are displayed and generated using the **Object Initialization Rules Administration** utility. This utility defines how the initial attribute values for the object are established, how the attributes are displayed, and can determine basic relationships, such as life cycle association, when an object is created.

The **Object Initialization Rules Administration** utility is available from the **Site**  or **Organizations**  **Utilities** page. The rules established by the parent site are inherited by each organization context by default, but they can be overridden at the organization level. The rules are defined in XML format; you can view and update them.

For more information, see the Object Initialization Rules chapter of the *PTC Windchill Specialized Administration Guide*.



## Auditing Activities Within the Organization

The auditing framework allows the system to capture historical information of who did what that caused changes in the Windchill database. The security auditing feature also provides a mechanism to retain historical records of security related events, such as privilege changes, team changes, and denial of access. Security audit reporting is helpful in highly regulated industries where it is necessary to identify events that may have resulted in a potential security breach.

Out-of-the-box, only the **Organization Usage** events are enabled. Any other specific events that you want captured must be individually enabled by the site administrator.

For more information, see the *PTC Windchill Specialized Administration Guide*.

## Creating and Managing Access Control Policy Rules

The **Policy Administration** utility is used to create access control policy rules. You can create organization-level policies that apply to the entire organization from **Organizations**  **Utilities**. To establish site-level policies, create those policies that apply to all organizations in the system from **Site**  **Utilities**.

You can define policies that control the level of access to information by organization members. For example, you may want to provide read access to all documents of type Engineering Specification to an engineering group in your organization. In this case, you need to first define an Engineering user-defined group and populate it with the appropriate members, then define a document type of Engineering Specification in your organization. Finally, you need to use the **Policy Administration** utility to define the access policy based on the document type, the group or groups provided access, and the access level.

---

Another way to centralize the administration of access control policy rules is to use the dynamic roles that are available from the **Roles** tab in the **Policy Administration** utility. By using dynamic roles, you can create access control policy rules using a domain established in the organization context that apply to the members of roles in the local and shared teams that inherit the rules. For additional information, see [Using Dynamic Roles on page 100](#).

For more information about access control, see the *PTC Windchill Specialized Administration Guide*.

## Viewing and Managing Access Control for Objects

You can view both the ad hoc and policy access control rules that are set for objects (such as folders, parts, and documents) and then manage the ad hoc access control rules for the objects. Navigate to the object, and select the **Edit Access Control** action. Using this action, you can view access control for the object and set ad hoc access control rules for the object.

For more information, see the *PTC Windchill Specialized Administration Guide* and the “Security Management” help available from the PTC Windchill Help Center.

## Creating and Managing Profiles

You can dynamically control which actions are visible to user, or group of users, within your organization by associating that information with a profile. Profiles are not an access control mechanism; they are a user interface control mechanism. A profile represents a typical category of user within a company and is based on the roles and privileges associated with that particular user category.

Profiles expose only the necessary functionality and information needed by a user. They create a focused and simplified user interface, reducing confusion by eliminating areas of the user interface that could be distracting.

For more information about profiles, see [Profile Management on page 291](#).

## Configuring Numbering and Versioning Schemes

You can configure the number and versioning schemes used to uniquely identify parts, documents, and other objects in the organization. The organization context inherits the site-level schemes, but can optionally define its own schemes. In general, when a company is hosting Windchill for its internal users, the numbering and versioning schemes should be defined at the site level; you should not override the site-level schemes by defining schemes at the organization level.

For more information about numbering, see [Administering the Numbering of Parts, Documents, CAD Documents, and Change Objects on page 104](#).



---

For more information about versioning schemes, see [Administering the Versioning of Parts, Documents, and CAD Documents](#) on page 105.

## Monitoring and Managing Viewable Publishing

You can monitor and manage the publishing of viewable files that are optionally generated when CAD models are checked into products, libraries, and projects. You can also configure and update the watermarks used by the visualization tool when viewing document and part content.

For more information, see the *PTC Windchill Visualization Services Administrator's Guide*.

## Viewing Reports

You can access several predefined reports for information contained within your organization.

For more information on available reporting functionality, see the online help available from **Organizations**  **Reports**.

## Importing and Exporting Information

You can exchange information with another server, or between servers, or between a server and a file system using the Windchill import/export utilities. These utilities read and write system information in the Windchill XML format. The workflow and life cycle administration utilities accessible to you integrate the import/export functions.


For more information, see [Importing and Exporting Life Cycle Templates](#) on page 326, and the help available from the **Workflow Template Administration** utility.

## Purging, Archiving, and Restoring Jobs

You can create and manage purge jobs with the **Purge Management** utility. If you have the applicable functionality installed, you can create purge jobs to permanently remove data from the Windchill system or create an archive of the data to restore at a later time. This would apply to viewing, restoring, and deleting the contents of projects and programs.

---

## Managing Preferences

Using the **Preference Management** utility on the **Organizations**  **► Utilities**, you can manage preferences at the organization level. Preferences set at the organization level affect all application contexts and users within the organization. Some preference values can be overridden by application contexts within the organization, unless locked at the organization level.

## Undoing a User Checkout

If a user in your organization has an object checked out, you can undo the checkout, reverting to the last modified version or iteration of the object. This is useful in situations where the user who had the object checked out has left the company, or if they are out of the office when the checked out object is needed.

You can perform the undo checkout action on the object from the **Folders** page of the organization, from the **Folders** page of a product, library, project, or program within your organization, or from the information page for the checked out object.

An organization administrator can also delete an individual user's workspace. For more information, see the *Using PTC Creo Parametric with PTC Windchill* guide.

## Creating Public Information Page Tabs

You can create custom information page tabs that can be **Set Public**, making them visible to all users in your organization.

For more information about creating and managing information page tabs, see the Organization Administration help.

## Administering the Windchill Mobile App

---

### Note

The Windchill mobile app requires a separate license. Ensure that your site has purchased this license before continuing.

---

Once the mobile app has been configured by a site administrator, you can configure attribute layouts and set preferences related to the mobile app. For more information, see Administrator Actions for Windchill Mobile App in the Windchill Help Center.

For information on how users will download the app and connect to Windchill, see Connecting to Windchill from Your Mobile Device in the Windchill Help Center.

---

## Out-of-the-box Organization Templates

At installation, the following organization templates are loaded:

Template Name	Description
General (PDM)	A sample template that can be used to create an organization for Windchill PDMLink.
General	A sample template that can be used to create a general organization for Windchill ProjectLink.
Enterprise	A sample template that can be used to create an enterprise organization.
Supplier	A sample template that can be used to create a supplier organization.
Customer	A sample template that can be used to create a customer organization.

The organization templates can define the same basic information that is discussed in [Context Administrative Items on page 61](#). The out-of-the-box organization templates define the following:

- Context structure
- Context participation
- Context access control policies
- Context data

The following sections describe the items that are defined in the templates.

### Context Structure

The organization templates define the following folder structure: Change Log, General, and Policies.

Some organization templates define user-defined groups and dynamic roles that are automatically included in the organization. You can add users to the groups and dynamic roles.

### Context Participation

The following groups are automatically created when an organization is created using any template:

- Organization administrators
- This Org (current organization participant)
- All participating members
- Shared team creators

- 
- Filter template creator
  - Product creators (Windchill PDMLink)
  - Library creators (Windchill PDMLink)
  - Project creators (Windchill ProjectLink)
  - Program creators (Windchill ProjectLink)

In addition to the groups created using any template, the following groups are created when using the Enterprise template:

- Administration
- Engineering
- Manufacturing
- Procurement
- Sales
- Marketing
- Service
- Quality Assurance
- Customer
- Supplier
- Partner
- Facilities

## Context Access Control Policies

Users who are members of the site Administrators group are granted Full Control to all object types at the site root domain. Users who are members of the Organization Administrator group (ORG ADMIN) are granted Full Control to all object types at the root domains of the organization (Default, System, Private, and the child of the site context /User domain with the same name as the organization).

During the creation of an organization, additional domain-based access control rules are automatically created as follows:



- In the organization context System domain, the organization's All Participating Members group is granted read access to templates (such as document templates, life cycle templates, and workflow templates), objects, and initialization rules. For the complete list, see [System Domain Rules on page 152](#).
- In the organization-specific domain that is a child of the site context /User domain, the organization's All Participating Members group is granted read access to the organization context and organization content.

---

Additional domain-based access control rules can be defined within an organization template. The following is a list of the access control rules defined in the out-of-the-box organization templates:

- In the General (PDM) organization template, organization members (all users) are granted read access to all Released objects in the organization's /Default/PDM domain. Only product and library contexts are affected by this rule.
- In the Enterprise organization template, project type groups are granted read access to projects contained in the project type domains. For example, a project of type Engineering has a corresponding group and organization domain. An access control rule is defined granting read access to the Engineering user-defined group in the Engineering domain. When a project of type Engineering is created, the project is put in the Engineering domain. A user who is added to the Engineering group is able to see all projects of type Engineering.

PTC recommends that you do not modify or delete the default set of access control rules automatically created during the creation of organization, product, library, project, or program contexts. It is acceptable to modify access control rules created from a template.

To adjust access control rules, use the **Policy Administration** utility. To launch the **Policy Administration** utility in the context of the organization, navigate to **Organizations**  **Utilities**, and click **Policy Administration**. By launching the **Policy Administration** utility from **Organizations**  **Utilities**, the context is set to the organization context. In this context, only the domains and subdomains of the organization, plus any ancestor domains from the site are visible. Members of the Organization Administrators group can create and modify rules within the organization's domains. Below is a list of some of the automatically created organization domains with some basic rules:

- /Default – Rules created at this level are inherited by the default domains of all public products, libraries, projects, and programs contained within the organization and contexts created that have a shared team. Typically, only business objects belong to this domain.
- /Default/PDM – Rules created at this level are inherited by the default domains of all public products and libraries contained within the organization. Typically, only business objects belong to this domain.
- /Default/Project – Rules created at this level are inherited by the default domains of all public projects contained within the organization. Typically, only business objects belong to this domain.
- /Private – Rules created at this level are inherited by the system domains of products, libraries, projects, and programs contained within the organization.

The default domain of private products, libraries, projects, and programs also inherit these rules. PTC recommends that no additional access control rules be created within this domain.

- /System – Typically, only administrative objects (such as document templates, team templates, and life cycle templates) are in this domain.

To update the access control rules for an organization domain within the **Policy Administration** utility, select a domain and click **Update**. From the **Administrative Domain** window, click the **Access Control** tab. This provides the list of existing access control rules for this domain. From this tab, you can modify or delete existing rules and create new rules. When creating or updating rules, the list of user-defined groups available from the **Groups** tab include groups defined at the site and organization levels. For more information, see [Searching for Participants in Administrative Clients on page 255](#).

## Access Control Rules

Out-of-the-box access control rules are described in the following sections.

### Default Domain Rules

The following table lists the combination of object type, life cycle state, and permissions that the Default domain out-of-the-box rules define for the organization. Most permissions are granted to the listed participant.

Object Type	State	Permissions	Participant
Meeting	All	Read	All Participating Members
Meeting	All	Read	This Org
NavigationFilterTemplate	All	Full Control (All)	Filter Template Creator
NavigationFilterTemplate	All	Read	This Org
WObject	All	Full Control (All)	ORG ADMIN (Organization Administrator group)
AbstractWorkPackage	All	Read, Create, and Download	PACKAGE CREATOR (Package Creator dynamic role)
AbstractWorkPackage	In Work	Modify and Modify Content	PACKAGE CREATOR
AbstractWorkPackage	Approved	Revise and Modify	PACKAGE CREATOR
AbstractWorkPackage	Released	Modify and Revise	PACKAGE CREATOR

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>	<b>Participant</b>
AbstractWorkPackage	Completed	Modify, Revise, and Modify Content	PACKAGE CREATOR
AbstractWorkPackage	Rework	Revise, Modify, and Modify Content	PACKAGE CREATOR
ManagedCollectionImpl	All	Create, Create By Move, Read, and Modify	PACKAGE CREATOR
DeliveryRecord	All	Create, Read, Modify, Modify Content, Download, and Change Permissions	PACKAGE CREATOR
DeliveryRecord	All	Create, Read, Modify, Modify Content, Download, and Change Permissions	REPLICATION PACKAGE ADMINISTRATOR
ExportRecord	All	Create, Read, Modify, and Delete	PACKAGE CREATOR
ExportRecord	All	Create, Read, Modify, and Delete	REPLICATION PACKAGE ADMINISTRATORS
ReceivedDelivery	All	Create, Read, Modify, Modify Content, Download, Set State, Delete, Change Permissions, Administrative	RECEIVED DELIVERY MANAGER
ReplicationPackage	All	Create, Read, and Download	REPLICATION PACKAGE ADMINISTRATORS
ReplicationPackage	In Work	Modify, Modify Content, Modify Identity, Administrative,	REPLICATION PACKAGE ADMINISTRATORS

Object Type	State	Permissions	Participant
		and Revise	
ReplicationPackage	Released	Modify Identity, Modify, Administrative, and Revise	REPLICATION PACKAGE ADMINISTRATORS
ReplicationPackage	All	All <sup>1</sup>	REPLICATION PACKAGE ADMINISTRATORS <sup>2</sup>

1. This permission is Absolutely Denied to the specified participant. All other permissions listed in this table are Granted to the specified participant.

2. This permission is applied to all participants who are not part of the Replication Package Administrators group.

### System Domain Rules

The following table lists the combination of object type, life cycle state, and granted permissions that the System domain out-of-the-box rules define for the organization.

Object Type	State	Permissions	Participant
WObject	All	Full Control (All)	ORG ADMIN
WDocument	All	Read and Download	All Participating Members
WPart	All	Read and Download	All Participating Members
FilteredDynamic EnumSet	All	Read	All Participating Members
Notebook Template	All	Read	All Participating Members
Notebook Template	All	Read	This Org
Cabinet	All	Read	All Participating Members
SubFolder	All	Read	All Participating Members
TeamTemplate	All	Read	All Participating Members
WfTemplateObject	All	Read	All Participating Members
LifeCycleTemplate	All	Read	All Participating Members
EPMDocument	All	Read and	All Participating



<b>Object Type</b>	<b>State</b>	<b>Permissions</b>	<b>Participant</b>
		Download	Members
Project2	All	Create	PROJECT CREATOR
WTLibrary	All	Create	LIBRARY CREATOR
TypeBasedRule	All	Read	All Participating Members
PDMLinkProduct	All	Create	PRODUCT CREATOR
TableViewDescriptor	All	Read	All Participating Members
WTGroup	All	Read and Delete	SHARED TEAM CREATOR
ContainerTeam	All	Read	PROJECT CREATOR
ContainerTeam	All	Read, Modify, Create, and Delete	SHARED TEAM CREATOR
ContainerTeam	All	Read	PRODUCT CREATOR
ContainerTeam	All	Read	LIBRARY CREATOR
Report Template	All	Read	All Participating Members
WTPartAlternateRep	All	Read and Download	All Participating Members
ContainerTeam	All	Read	PROGRAM CREATOR
Project2	All	Create	PROGRAM CREATOR

The following table lists the combination of object type, life cycle state, and granted permissions that the System domain out-of-the-box rules define for organizations created with the General organization template.

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>	<b>Participant</b>
WTVariance	All	Read and Download	All Participating Members
WTChangeIssue	All	Read and Download	All Participating Members
WTChangeRequest2	All	Read and Download	All Participating Members
WTChangeOrder2	All	Read and Download	All Participating Members
WTChangeActivity2	All	Read and Download	All Participating Members

## Private Domain Rules

The following table lists the combination of object type, life cycle state, and permissions that the Default domain out-of-the-box rules define for the organization.

Object Type	State	Permissions	Participant
WTVariance	All	Read and Download	All Participating Members
WTChangeIssue	All	Read and Download	All Participating Members
WTChangeRequest2	All	Read and Download	All Participating Members
WTChangeOrder2	All	Read and Download	All Participating Members
WTChangeActivity2	All	Read and Download	All Participating Members

## Organization-specific User Domain Rules

The following table lists out-of-the-box rules that are defined for the organization. The descriptions show the combination of object type, life cycle state, and granted permissions that are present in the organization organization-specific user domain out-of-the-box rules define for (the one with the same name as the organization):

Object Type	State	Permissions	Participant
WTOBJECT	All	Full Control (All)	ORG ADMIN (Organization Administrator group)
ReplicationPackage	All	Full Control (All) <sup>1</sup>	REPLICATION PACKAGE ADMINISTRATOR <sup>2</sup>

1. This permission is Absolutely Denied to the specified participant. All other permissions listed in this table are Granted to the specified participant.
2. This permission is applied to all participants who are not part of the Replication Package Administrators group.

## /Default/PDM Domain Rules for General (PDM) Template

The following table lists the combination of object type, life cycle state, and granted permissions that the out-of-the-box rules define for the General (PDM) organization template:

Object Type	State	Permissions	Participant
WTOBJECT	Released	Read	This Org

---

## Default/PDM Domain Rules

The following table lists the combination of object type, life cycle state, and granted permissions that the Default/PDM domain out-of-the-box rules define for the organization:

Object Type	State	Permissions	Participant
WTLibrary	All	Create	LIBRARY CREATOR
PDMLinkProduct	All	Create	PRODUCT CREATOR

## Default/Project Domain Rules

The following table lists the combination of object type, life cycle state, and granted permissions that the Default/Project domain out-of-the-box rules define for the organization:

Object Type	State	Permissions	Participant
Project2	All	Create	PROJECT CREATOR



## Context Data

For organization contexts created using the General or Enterprise organization templates, document types are inherited from the site.

For organization contexts created using the Customer or Supplier organization templates, document types include those defined in the template as well as the ones inherited from the site. The Customer and Supplier organization templates define the following document types: Analysis, Contract, Design, Drawing, Issues, Memo, Proposal, Report, Requirements, Schedule, Specification, and Statement of Work.

For all organization contexts, document attributes, part attributes, and project types are inherited from the site.

## Creating an Organization Context

Only site administrators have the permissions to create organization contexts. Organization contexts are created from the **Organizations** page (visible only to site administrators), accessed by clicking the **View All** link under **Organizations** . Click the new organization icon  at the top of the **Organizations** table.

The **New Organization** window that opens is similar to the following:

**New Organization** ?

**Attributes**

\* Organization Name:  Search...

Description:

Postal Address:

Web Site:

\* Template: General ▾

Subscriber - organization can host libraries, products, and projects:  Yes  No

Allow all organization members to create projects:  Yes  No

Restricted Directory Search:  Yes  No

Allow sourcing administrators to create organizations:  Yes  No

Conferencing ID:

Conferencing URL:

\* Indicates required fields.

To associate an existing organization participant to the organization context, click **Search**, next to the **Context Name** field, and search for existing organization participants. You can also type in a new organization name (one that does not match an existing organization participant); in this case, a new organization participant is created along with the organization context.

---

 **Note**

Associating a new organization context with an existing organization participant may change the domain association of the organization participant. For more information, see [Organization Domain Algorithm on page 97](#).

---

 **Note**

The internet domain defined on the organization participant is important when creating new subtypes. The internet domain is used to distinguish which organization participant owns the type. During the installation process, the initial organization participant that was created included an internet domain. This organization participant is associated with the site context; any types defined at the site context are available to all organizations. In a multiple organization environment, PTC strongly recommends that the internet domains of new organizations be distinct from the internet domain for the site. Do not use underscores ( \_ ) in the internet domain.

---

By default, the **Subscriber** option is selected. This means the organization can host products and libraries (for Windchill PDMLink, Arbortext Content Manager, and Pro/INTRALINK), and projects and programs (for Windchill ProjectLink). Members of a subscribing organization who belong to the appropriate application context creators group can create application contexts (products, libraries, projects, or programs) within the organization.

For Windchill ProjectLink, the **Allow all organization members to create projects** option shows on the window and is set to **Yes** by default.

By default, users cannot search for users and organizations outside of their own organization. When creating or editing an organization context, you can turn off the **Restricted Directory Search** option to provide users with the ability to search for all users and organizations. Regardless of whether **Restricted Directory Search** is selected, a site administrator can search for all users and organizations from any context.

For Windchill Supplier Management, the **Allow sourcing administrators to create organizations** option displays, and is set to **No** by default.

For additional information on creating an organization context, see the help available from the **New Organization** window.

---

## Note

The site administrator user who created the organization is owner of the organization and is the user identified in the **Owner** attribute on the organization information page. (The organization owner of the initial organization created during installation is the administrator user that was identified during installation, by default wadmin.) The organization owner can be changed to another user by editing the organization.

---

For a description of the contents of the templates, see [Out-of-the-box Organization Templates on page 147](#).

## Owning Organization Participants

Parts or documents created within an organization context are automatically owned by the organization participant associated with the organization context. However, the site can choose to allow users to specify a different organization participant, such as one associated with an external vendor or supplier, as the owner of an object. For example, if a part used in a part structure is acquired from a vendor, you can create an organization participant for that vendor, and select that vendor's organization participant as the owning organization for the part.

To change the out-of-the-box functionality so that a user who creates a part or document can specify which organization participant owns the part or document, you must do the following things:

- Set up domains for use with owning organizations. For more information, see [Setting Up Domains for Use with Owning Organization Participants on page 159](#).
- Create or update organization participants to be used as owning organizations, sometimes referred to as internal organizations. For more information, see [Creating and Updating Owning Organization Participants on page 159](#).
- Enable the appropriate preferences to display the owning organization on objects, using the **Preference Management** utility:
  - **Expose Organization** – Displays the organization for all objects except change objects.
  - **Expose Organization for Change Management Objects** – Displays the organization for change objects. The **Expose Organization** preference must also be enabled.
- Configure the context where the parts or documents will reside so that the user enters the part or document number (rather than having the numbers auto-generated). How to turn off autonumbering is described in the *PTC Windchill Specialized Administration Guide*.

---

For information about creating object initialization rules, see the help available from the **Object Initialization Rules Administration** utility.

An alternative to having the user enter the part of document number is to set up object initialization rules for parts and documents that automatically set different numbers depending on the owning organization.

For an example of the XML elements that can be used in an object initialization rule to set this up, see the *PTC Windchill Specialized Administration Guide*.

## Setting Up Domains for Use with Owing Organization Participants

To allow users to identify the ownership of parts and documents that are created in the solution with external vendors and suppliers, the organization participants created for vendors and suppliers must be in a domain that allows the users read access to the organization participant.

A simple approach to setting this up is the following:

1. Create a domain that will be used specifically for this purpose. For example create the /Vendors domain using the **Policy Administration** utility from the site context.
2. Create the access control rule in the Vendors domain that grants READ permission on WTOrganization objects to ALL users.
3. When creating the organization participants that represent external vendors and suppliers using the **Participant Administration** utility, select the /Vendors domain for the **Windchill Domain** field.

For more information on domains, see [Managing User Access to Data on page 34](#).

## Creating and Updating Owing Organization Participants

Use the **Participant Administration** utility to create a new organization participant or update an existing organization participant for use as an owning organization by including the following attributes on the participant:

- The **Organization ID** attribute indicates the type and value that is specified for the globally unique organization identifier under which the organization is registered. Select the type from the drop-down list. By default, the drop-down list contains **CAGE Code**, **DUNS Number**, and **ISO 6523**.

---

 **Note**

The organization identifier, such as a CAGE code or DUNS number, is an internationally coded number that is assigned when the organization registers with a specific site. For site registration information, see the [Registration Authority](#).

---

If the drop-down list does not contain the type required, you can specify a new list by adding the `wt.org.organizationTypes` property to the `wt.properties` file. The `wt.org.organizationTypes` property value is a comma-separated list of coding systems, where each coding system has two parts in the following format:

```
<ICD_number>/<coding_system_name>
```

where:

`<ICD_number>` is the international code designator number assigned to the coding system. For example, the CAGE ICD number is 0141. For a list of ICD numbers, see the [Registration Authority](#).

`<coding_system_name>` is the name of the coding system.

If the `wt.org.organizationTypes` property does not exist in the `wt.properties` file, then the following `wt.org.organizationTypes` property value is used:

```
0141/CAGE Code,0060/DUNS Number,0026/ISO 6523
```

If you add the `wt.org.organizationTypes` property, be sure to include all coding systems that you want to appear in the drop-down list. For example, to include CAGE Code, DUNS Number, and GTE/OSI Network, set the `wt.org.organizationTypes` property by entering the following `xconfmanager` command from a windchill shell:

```
xconfmanager -s wt.org.organizationTypes="0141/CAGE Code,0060/DUNS Number,  
0126/GTE/OSI Network" -t codebase/wt.properties -p
```

---

 **Note**

After restarting the method server with the above property set, the **Organization ID** drop-down list contains CAGE Code, DUNS Number, and GTE/OSI Network, but not ISO 6523.

---



---

Windchill does no checking to ensure that the international code designator numbers and coding system names set are valid. It is your responsibility to ensure the use of valid coding systems.

Use the `xconfmanager` utility to add the `wt.org.organizationTypes` property. For more information, see the *PTC Windchill Specialized Administration Guide*.

- The **Windchill Domain** attribute identifies the administrative area where the organization object resides. The domain selected must have access control rules set for the `WTOrganization` object type so that the users who create part and documents have read access to the organization objects that you want to use as internal organizations. For information on how to set up a domain for this use, see [Setting Up Domains for Use with Owning Organization Participants on page 159](#).

If you enter a type and value for **Organization ID** in an organization participant, then Windchill combines the organization ID type number and ID and stores the resulting value in the `organizationIdentifier` attribute of the organization directory entry. The format of the attribute is:


```
<ICD_number>${<org_ID>
```

where:

`<ICD_number>` is the international code designator number assigned to the organization ID type. For example, the CAGE ICD number is 0141. For a list of ICD numbers, see the [Registration Authority](#).

`<org_ID>` is the organization identification number assigned when the organization was registered.

## Using the Organization Utilities Page

The utilities listed on **Organizations**  **Utilities** allow you to perform administrative actions at an organization level. Some of these utilities also appear in other locations. The difference is the context from which the utility is launched.

The utilities are grouped according to whether they are system administration utilities or business administration utilities. Many of links provided on the page give you access to the utilities that you need to use to perform the duties described in [Typical Duties of Organization Administrators on page 139](#).

To explore the use of each utility, click the corresponding link on the page and then click the help icon in the window that opens.

---

## Changing an Established Internet Domain

If the internet domain associated with an organization context is changed by modifying the organization participant using the **Participant Administration** utility, the previous internet domain is no longer recognized as being associated with the organization context. Any types associated with the organization context's previous internet domain are no longer recognized as mapping to the organization.

If the internet domain name of the organization is changed, each type associated with the organization context's previous internet domain must be edited in the **Manage Types** window of the **Type and Attribute Management** utility so that the type internal name contains the new internet domain reversed.

For example, the World Wide Tractors organization participant has an internet domain of worldwidetractors.com. A subtype of Engine created in that organization has the internal name of com.worldwidetractors.Engine.

If the internet domain is later changed using the **Participant Administration** utility to wwtractor.com, then the com.worldwidetractors.Engine subtype is no longer associated with the organization's internet domain.

To associate the com.worldwidetractors.Engine subtype with the organization's new internet domain name, the type's internal name must be edited from com.worldwidetractors.Engine to com.wwtractor.Engine.

For more information on assigning domains to organization contexts, see [Participants \(Users, Groups, and Organizations\) on page 251](#). For more information on types, see the help available from the **Type and Attribute Management** utility.

## Using the OrganizationSync Utility for User Organization Changes

When a user is moved from one organization to another by using a third party tool that allows your site to modify user entries in your directory service, the domains of the user and of the user's personal cabinet are not automatically changed. As the site administrator, you can use the OrganizationSync command-line utility to update organization-related information for users who have changed organizations. After changing the user's organization through a third party tool, run the OrganizationSync utility to change the other organization-related information for the user. Using the utility ensures that properties of a user or set of users are in sync with their current organization.

---

 **Note**

If you use the **Participant Administration** utility (and not a third party tool) to update user information in your directory service, then the OrganizationSync utility is automatically run as a result of changing a user's organization from the **Edit User** window.

---

The OrganizationSync utility does the following:

- Assigns a set of user-related business objects to the administrative domain of the user's current organization. If a user does not have an organization, these objects are assigned to the Unaffiliated domain. The objects reassigned include the WTUser object, the user's personal cabinet and content of that personal cabinet, and the user's notebook.
- Removes the user from the administrators and creators groups of their previous organization context, if necessary. The utility determines the previous context by extracting the context of the user's previous administrative domain.
- Updates the organization groups of any teams, in which the user was a member, to reflect the user's current organizational membership.

---

 **Note**

It is safe to run the OrganizationSync utility on a user that was not actually updated.

---

The syntax of the OrganizationSync command is as follows:

```
java wt.inf.container.OrganizationSync [--users <user_list>] [--domains <domain_list>]
[--domain-hierarchies <domain_list>] [--organizations <organization_list>]
```

The brackets ({} ) in the syntax indicate optional parameters and indicate parameters that you specify together. Parameter names are case-sensitive; enter the names using the case shown in the syntax and the following table.

Parameter Value	Description
<user_list>	A space-separated list of user names.
<domain_list>	A space-separated list of domain paths.
<organization_list>	A space-separated list of organization names.

When <domain\_list> is used with the --domains parameter, all users in the domain are synchronized. When <domain\_list> is used with the --domain-hierarchies parameter, all the users in each domain and in all descendent domains are synchronized.

---

## Note

Always run the OrganizationSync utility from a windchill shell. For details on using the windchill shell, see the *PTC Windchill Specialized Administration Guide*.

---

### Examples:

```
//Update the foo and bar users
java wt.inf.container.OrganizationSync --users foo bar

// Update all users in the site-level Unaffiliated domain
// and the "PTC Inc" domain in the "PTC Inc" org container
java wt.inf.container.OrganizationSync --domains []/User/Unaffiliated
"/wt.inf.container.OrgContainer=PTC Inc]/PTC Inc"

// Update all users in the site-level User domain, and in
// all of its child domains
java wt.inf.container.OrganizationSync --domain-hierarchies []/User

// Update all members of the "Acme Inc." and
// "Widget Intl." organizations
java wt.inf.container.OrganizationSync --organizations "Acme Inc."
"Widget Intl."
```

In the above examples, the container path is enclosed in brackets to separate it from the domain path. [/] is the Site (root) container.

## Best Practices

The following best practices are recommended by PTC.

### For All Windchill Solutions


The following best practices are recommended for all Windchill solutions.

#### Email Addresses

Ensure that users have an email address; many features in Windchill require that users have an email address. If users do not have the email attribute set in their user directory server entry, they cannot participate in the features that require an email address.

---

## Synchronizing Team Membership with Updated User-defined Groups

The recommended practice for defining groups is to define them at the organization level whenever possible and then use the user-defined groups in product, library, program, and project teams. The **Organizations**  **Groups** page can be used for this purpose.

Over the life of a product, library, project, or program, the members of user-defined groups referenced in teams may change. If group membership is modified from within Windchill, the membership of the teams in which the group is a member is automatically updated and you do not need to do anything additional; however, if the membership of one or more groups is modified using a third-party LDAP tool, you need to put together a plan for how to remove the updated groups from the participant cache and synchronize the teams on a regular basis.


For details on your options, see the Teams help.

## Displaying Alias Attribute Information for a Workflow Primary Business Object on the My Tasks Table

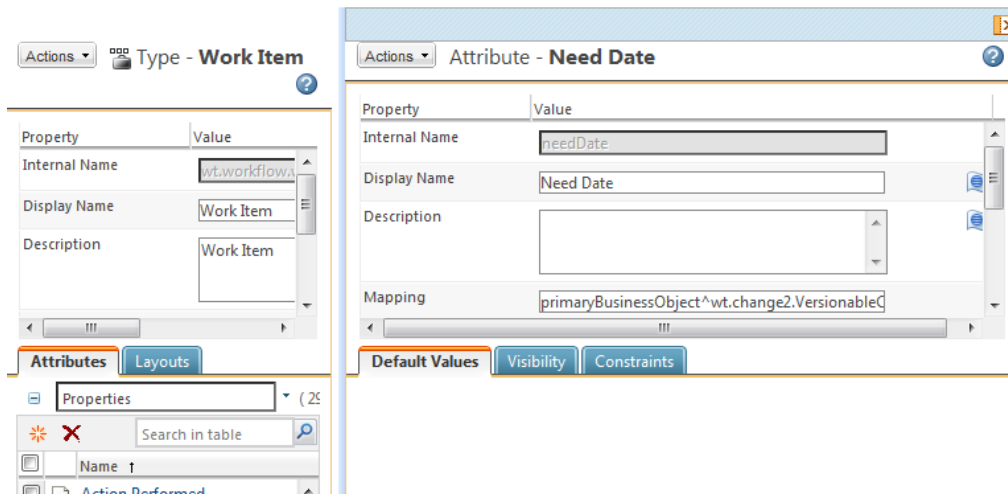
A workflow process is typically launched in the context of a primary business object (PBO), such as a change notice, change request, change task, or promotion request. Site and organization administrators can choose to display attributes from the primary business object on a work item as columns in the **My Tasks** table for a user by:


1. Mapping an alias attribute on the **Work Item** type to the desired attribute on the primary business object. For more information, see the *Creating a New Attribute and Alias Attribute Mapping* help topics in the PTC Windchill Help Center.
2. Creating or editing a table view on the **My Tasks** table to include the alias attribute mapped in step 1. For more information, see the *Creating and Editing New Table Views* help topic in the PTC Windchill Help Center.
3. Share this table view with all users in your site or organization. For more information, see the *Administering Table Views for the Site or Administering Table Views for the Organization* topic in the PTC Windchill Help Center.

For example, to display the **Need Date** attribute of a change task on the assigned work item on a user's **My Tasks** table:

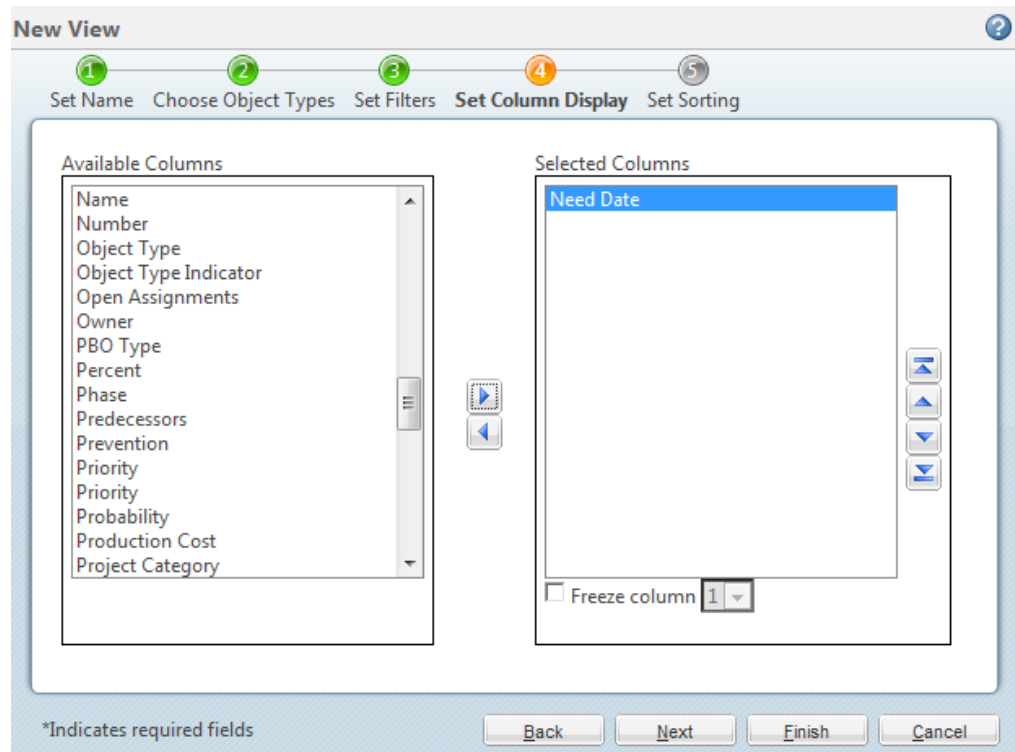
1. In the **Type and Attribute Management** utility, view the **Work Item** type.
2. Select **Edit** from the **Actions** menu to enter edit mode.
3. Click the new attribute icon .
4. On the **Define Attributes** step, specify the **Internal Name** for the attribute as "needDate", and select the **Alias** type for the attribute.
5. On the **Choose Data Type** step, select **Date and Time**.

6. On the **Set Properties** step, specify the following mapping syntax for the **Mapping** property: *primaryBusinessObject^wt.change2.VersionableChangeItem~needDate*
7. Click **Save** to finish creating the attribute.



8. From the **My Tasks** table on the **Home**  page, select **Customize** from the view drop-down list, and create or edit a view.
9. (Optional) On the **Set Name** step of the **New View** or **Edit View** window, ensure that the **Share with all users** checkbox is selected, if you want to make this table view available to all users.

10. On the **Set Column Display** step, select the **Need Date** attribute.



11. Click **OK**.

When users select the table view, the **Need Date** attribute will now display as a column in the **My Tasks** table.

## For Windchill Solutions with Products and Libraries

The following best practices are recommended for Windchill solutions which use products and libraries.

### Setting Object Initialization Rules

The object initialization rules include the ability to set default values and display characteristics for the following attributes:

- Folder paths
- Default life cycle template
- Default team template
- Default numbering scheme
- Default version scheme

---

Additionally, rules can be used to set the following:

- Available life cycle templates
- Attribute values
- Display characteristics for other attributes

Although these rules can be set for individual product and library contexts, PTC recommends that you set them at either the organization or site level so that an entire organization or site is using the same set of rules. This promotes reuse and reduces unnecessary duplication at lower context levels.

For more information, see the Object Initialization Rules chapter of the *PTC Windchill Specialized Administration Guide*.

## Setting Up Enhanced Life Cycle Templates

The out-of-the-box Product Design template includes object initialization rules that set different default life cycle templates and versioning schemes for parts, documents, and CAD documents than what is set out-of-the-box at the site level. This template demonstrates the use of simplified life cycles and state-based versioning. Unless you have overriding business practices that require unique rules, PTC recommends that to use these features, you modify the site object initialization rules and remove them from the Product Design template.

## For Windchill Solutions with Projects and Programs

The following best practices are recommended for Windchill solutions which use projects and programs.

### Allowing All Organization Members Read Access to Project or Program Content

To allow all organization members access to project or program content, even if they are not a member of the project or program, you must update the access control policies.

To update an existing organization, navigate to the **Policy Administration** utility on the **Utilities** page of the organization. Select the /Default/Project domain, and create a new access control rule granting the This Org group Read access to the WLObject type in all states. By creating this new access control rule, all organization members will have read access by default to all business objects within all project or programs that are created by selecting an **Access Group** option other than **Project Members Only**. (This access control rule will not affect access to objects within projects or programs created with the Members Only access group.)

For more information on the **Policy Administration** utility, see [Using the Policy Administration Utility on page 93](#).



---

Alternatively, the site administrator can update the organization template so that all organizations subsequently created include this access control policy by default.

Add the following XML to the organization template:

```
<AccessControlRule>
  <domainName>/Default/Project</domainName>
  <externalTypeId>WCTYPE|wt.fc.WTObject</externalTypeId>
  <lifecycleState>ALL</lifecycleState>
  <WTPrincipalReference isInternal="true">
    <groupName>This Org</groupName>
    <groupType>This Org</groupType>
  </WTPrincipalReference>
  <grantPermissionSet>
    <AccessPermissionSet>
      <permissionField name="Read"/>
    </AccessPermissionSet>
  </grantPermissionSet>
</AccessControlRule>
```



# 7

## Understanding Products and Libraries

Overview .....	172
Typical Duties of Product and Library Administrators .....	172
Creating a Product .....	179
Creating a Library .....	179
Administering Teams .....	180
Using the Product and Library Utilities Page .....	182
Out-of-the-box Product and Library Context Templates .....	182
Configuring Products or Libraries for Dynamic Documents .....	224
Configuring Part and Document Relationships .....	225
Best Practices for Object Initialization Rules .....	231

This section provides an overview for administering product and libraries and describes the typical duties that an administrator does. It also provides additional information about some of the main administrative tasks for products and libraries.

For more information, see the [Product and Library Administration help](#).

---

## Overview

Product and library administrators (also known as product and library managers) are responsible for managing product and library contexts. The capabilities of product and library administrators are nearly identical.

Product and library administrators control the product and library configuration, and the membership in their product and library teams within the confines of a specific product or library application context. They control access to product and library information. They define the specific life cycles, templates and processes, and they monitor and manage the product and library activities.

Product application contexts are used to define new product models or instances and collect all the information associated with the product. Product contexts are defined by product creators who are authorized by the parent organization under which a product is created. Products inherit templates, roles, user-defined groups, and policies from their parent organization context. In addition, the administrator can define product-specific templates, roles, and policies.

Library application contexts are used to manage standard parts and documents that are used across products and projects in an organization. Library contexts are defined and managed by authorized library creators in the parent organization under which a library is created. Libraries inherit templates, roles, user-defined groups, and policies from their parent organization context. In addition, the administrator can define library-specific templates, user-defined groups, roles, and policies.

If Arbortext products are installed in your environment, product and library contexts can be used to manage dynamic documents and the published documents created from dynamic documents.

For more information about context contents and how to create contexts, see [Contexts – Distributed and Hierarchical Administration on page 59](#).

## Typical Duties of Product and Library Administrators

Product and library administrators are responsible for managing the content of products and libraries. The capabilities of product and library administrators are nearly identical.

The typical duties of product and library administrators include the following:

- Managing team members and roles
- Managing folders
- Managing templates
- Managing object initialization rules
- Managing access policies

- 
- Configuring numbering and versioning schemes
  - Managing the life cycle of parts, documents, CAD documents, and dynamic documents
  - Managing viewable publishing
  - Managing preferences
  - Undoing a user checkout
  - Viewing and managing access control rules for objects
  - Importing and exporting information
  - Configuring external vaults or replication sites

The following sections describe some of these duties in more detail.

## Managing Team Members and Roles

Product and library managers can add members and team roles to a local team.

If the team includes a shared team, the shared team is managed from the organization context, and not the product or library context.

For more information about local and shared teams, see [Teams and Team Template Administration on page 297](#).

The team membership in a product or library can change or the current members can take on different responsibilities. To accommodate these types of changes, product and library managers have the ability to reassign tasks from one member to another.

## Establishing Roles

A product or library inherits the roles defined by its parent organization and the site. Additionally, roles can be defined in the context template used to create the product or library. You can then use these roles in the product or library, or you can add product or library-specific roles to product and library teams.

Each local team contains two fixed roles that cannot be removed: Product or Library Manager and Guest. The Guest role is designed to include user-defined groups and users that are not active team members and need only read access to product or library information.

It is possible to hide the Guest role for product and libraries. For more information, see the teams help.

The products and libraries in which a user is a guest can be seen by selecting the **Guest Member** view from the **Full Product List** and **Full Library List** that is available from the **Product** and **Library** tabs.

---

You define the team members and roles for the product and library local teams that you manage. Each product team has a product manager group and each library team has a library manager group. Any individual that is a member of one of these managers groups has the rights to administer the product or library after it has been created. The creator of a library or product is automatically defined as a member of the product or library managers group, and is identified as the product or library owner, by default.

## Controlling the Visibility of Actions

As the product or library manager, you can control visibility to information and actions within the product or library based on the roles in the product or library local team.

For more information, see the teams help.

## Overriding Profiles

As the product or library manager, you can override profile settings that are established at the site and organization contexts. For more information about profiles, see [Profile Management on page 291](#).

The site or organization administrator determines whether the various user interface elements and actions are configurable from an application context. You can override an action or user interface element in a context instance using Configure Actions for Roles which is accessed from the Team page. For more information, see the teams help.

## Moving Objects

Moving objects to a new folder requires different permissions depending on the move being performed. For more information on the permissions required to move an object, see the *PTC Windchill Specialized Administration Guide*.

## Additional Product and Library Team Information

For more information about teams, see [Administering Teams on page 180](#).

## Managing Folders

You can define folders and links within products and libraries.

By default, only product or library managers can define folders and subfolders in a product or library. This is typically a good policy because it prevents members from adopting a multitude of folder organization models, thereby creating folder chaos.

---

By default, a folder inherits the domain of the parent folder. You can change this behavior as described in [Assigning Domains to Folders in Solutions with Products and Libraries](#) on page 96.

## Managing Templates

You can define the document, CAD document, life cycle, team, option filter, and workflow templates that you want used in the context of a product or library. Each product or library inherits the templates defined by its parent organization context and the site. Additionally, you can create new product- or library-specific templates. If the name you specify is the name of an inherited template, then the new template overrides the inherited template that has the same name. You can restrict which templates are made available within your product or library by choosing to hide certain templates. For more information about templates, see [Templates](#) on page 75.

## Managing Object Initialization Rules

The use of object initialization rules provides a way to specify the following:

- Default values for the attributes of a specific object type. The default values are then used when a Windchill solution creates objects of that type and the user interface does not set a value. For example, you can set the default values for numbering and versioning.
- Display characteristics that constrain attribute values. If the user interface checks for the constraints, they are then used when the attribute value is displayed in the user interface. For example, the constraints for numbering, and versioning are honored in the user interface.

By default, the object initialization rules established by the site are inherited by each organization context and then inherited by the product or library. However, they can be overridden by an organization or overridden in a product or library. The rules are defined in an XML format and can be viewed and edited by a product or library manager. For PTC recommendations in this area, see [Best Practices for Object Initialization Rules](#) on page 231.

For more information about object initialization rules, see the Object Initialization Rules chapter of the *PTC Windchill Specialized Administration Guide*.

## Viewing and Managing Access Policies

You can view and manage the access control rules for objects (such as folders, parts, and documents) in your product or library. Navigate to the object, and select the **Edit Access Control** action, depending on your configuration. Using this action you can view and set the access control to the object for roles within your product or library team.

---

For more information, see the *PTC Windchill Specialized Administration Guide* and the “About Security Management” topic in the PTC Windchill Help Center.

You can define policies that control the level of access to information in a product or library. When defining a policy, the object types and user-defined groups defined in the parent organization can be used as well as the system groups representing the team roles in a product or library. For example, you could create a policy that provides read access to all documents of type “Quality Assessment” to the product team role/group called “Testers”. You can also choose to extend read access to this document type to an organizational user-defined group with the name “Quality Assurance” (if such a policy is not already granted at the parent organization level).

For more information about domains and policies, see [Administering Domains and Policies on page 86](#).

For more information about creating or updating access control rule policies, see the Access Control chapter of the *PTC Windchill Specialized Administration Guide*.

## Configuring Numbering and Versioning Schemes

You can configure the number and versioning scheme used to uniquely identify parts, documents and other objects in the product or library. The numbering and versioning schemes defined at the site and organization level are inherited by products and libraries by default, but each product or library can optionally define its own schemes. Use the Object Initialization Rules Administrator to configure the number and versioning schemes.

In general, when a company is hosting Windchill for its internal use, the numbering and versioning schemes should all be defined in the Site context and should not be overridden by an organization or in a product or library. The Product Design template demonstrates how to set up versioning (and other required functionality) for use in a basic life cycle management environment, where multiple life cycle templates are in use and state-based versioning is set up. If you choose to use this type of environment, consider defining the versioning (and other initialization rules) in the Site context rather than in individual product or library contexts so that all of your products and libraries use the same set of rules.

For more information, see [Administering the Numbering of Parts, Documents, CAD Documents, Managed Baselines, and Change Objects on page 104](#) and [Administering the Versioning of Parts, Documents, and CAD Documents on page 105](#).



---

## Managing the Life Cycle of Parts, Documents, CAD Documents, and Dynamic Documents

Within your Windchill solution, you have the choice of using a variety of out-of-the-box life cycle templates to help manage the life cycle of parts, documents, CAD documents, and dynamic documents. You can also create your own life cycle template or modify one of the existing templates. The options available to you range from the ability to fully automate the process of promoting a business object through maturity levels with the use of workflow processes to providing manual transition process where users in specified roles can promote objects to new states explicitly through the promote action. Default life cycle templates are established for object types through the use of object initialization rules and a default set of Site rules is loaded during the installation process.



For more information, see the *PTC Windchill Specialized Administration Guide* and [Understanding Life Cycles on page 299](#).

## Managing Viewable Publishing

You can monitor and manage the publishing of viewable files that are optionally generated when CAD models are checked into products and libraries. You can also configure and update the watermarks used by the visualization tool when viewing document and part content from the product or library.

For more information, see *PTC Windchill Visualization Services Administrator's Guide*.

## Managing Preferences

Using the **Preference Management** utility from **Products**  **► Utilities** or **Libraries**  **► Utilities**, you can manage preferences at the product or library level. Preferences set at the product or library level affect the product or library for which they are set. Different preferences can be set for different products or libraries.

For example, a number of preferences are available which allow you to determine the types of content allowed for documents. These preferences are found in the **Attachments** category of the **Preference Management** utility.

## Undoing a User Checkout

If a user in your product or library has an object checked out, you can undo the checkout, reverting to the last modified version or iteration of the object. This is useful in situations where the user who had the object checked out has left the company, or if they are out of the office when the checked out object is needed.

---

If you know the object or objects for which you want to undo the checkout, you can perform the undo checkout action on an object from either the **Folders** page of your product or library, or from the information page for the checked out object.

## Importing and Exporting Information

You can import information into a product or library, and export information to a local file system. The import/export facilities support information exchange with another Windchill server or non-Windchill system. These utilities read and write system information in an XML format. For more information about import and export, see the Export and Import chapter of the *PTC Windchill Enterprise Administration Guide*.

The workflow and life cycle administration utilities accessible to the site and organization administrator integrate the import and export functions with administering workflows and life cycles.

For more information about life cycle import and export, see [Importing and Exporting Life Cycle Templates on page 326](#).

For more information about workflow import and export, see Life Cycles and Workflow help.

## Configuring External Vaults or Replication Sites to Optimize Performance

You can configure the vaulting and replication rules for the external file and replica sites established by the site administrator.

When external vaults are configured, document and part content is stored on a file system rather than in the database. This configuration can provide significant upload performance improvements and is appropriate when the site is frequently used to exchange large files (such as CAD model files).

By default, external storage rules are based on individual domains in each context. You can launch the **Vaulting Rules** utility from the **Utilities ► File Server Administration** page in the context of a product or library. The utility allows you to create vaulting rules for the domains - /System and /Default - associated with the context in which the client is launched.

---

### Note

The rules needed for setting up an external file vault for a product or library are not inherited from the site.

---

---




If the increased number of vaults and file vault rules becomes unmanageable, the site administrator can force vaulting to be accomplished through a single vault by setting the `wt.fv.forceContentToVault` property to true. For how to set external file vault rules or set up a single vault, see the External File Vaults chapter in the *PTC Windchill Enterprise Administration Guide*.

Site administrators typically define the replica site and the replication schedule, and the product or library managers configure the replication rules for a particular product or library. Product and library managers can access the **File Server Administration** utility, but can only work on setting the replication and file vaulting rules. For how to set replication rules, see the help available from the **Content Replication Rules** window.

## Creating a Product

A product context provides the space in which a team of people can create and manage all of the information that is relevant to the design, manufacture, and support of a customer product. This information includes the following:

- A defined data storage area for the business objects associated with a customer product.
- A set of rules that control the access to the product and optionally set the numbering scheme, versioning scheme, life cycles, and workflows that are used with the objects that are associated with a product.
- The team of users who have access to the product.

Product contexts are created within an organization by members of the product creators group that is defined in the organization or by the organization administrator. The organization administrator can add users who are members of the organization to the product creators group from **Organizations**  **► Creators**. The new product icon  appears on the **Products** table (accessed by selecting **Products**  **► View All**) only for members of the product creators group.




For detailed instructions, see the help available from the **New Product** window.

## Creating a Library

A library context provides the space in which you can store and provide access to business information. For example, all documents owned by a department can be stored in a department library.

Libraries can also hold objects that are not related to a single product. For example, parts that are related to more than one product could be stored in a common parts library (such as a Commodity Parts or Engineered Parts library), from which you allow multiple product teams access to those parts.

---

Libraries are created under an organization by members of the library creators group or by the organization administrator. The organization administrator can add users who are members of the organization to the library creators group from **Organizations**  ► **Creators**. The new library icon  appears on the **Libraries** table (accessed by selecting **Libraries**  ► **View All**) only for members of the library creators group. For detailed instructions, see the help available from the **New Library** window.

## Administering Teams

One of the main activities that a product or library manager has is to administer the local team associated with the product or library.

---

### Note

If the context team created in a product or library includes a shared team or is exclusively made up of a shared team, the shared team is managed from the organization context and is not managed by the product or library manager.

---

When a product or library that uses a local team is first created, a base set of roles for the local team is established from the context template that is used in the creation. For more information about these roles and the access control rules that are set for the roles that are in the out-of-the-box templates, see [Out-of-the-box Context Access Control Policies on page 187](#).

To administer a product or library local team, perform the following activities:

- Establish the roles that you want used in the team. You can add, remove, or create new roles.

The base set of roles that are established through the out-of-the-box templates is the minimal set of roles that you should have for a team. (See [Out-of-the-box Context Participation on page 212](#)) Before removing any of these roles, consider the consequences of the removal. For example in a product team, you should not remove the Product Manager role because this role defines who can administer the product.

The roles you can add are roles inherited from your organization. For additional information about these roles, see [Installed Site Templates on page 76](#).

---

You can also create roles specifically for your product or library local team. In addition to creating a new role through the **Team** page, you must define the access control rules for the role by using the **Policy Administration** utility. As part of this activity, create the rules against the system group that is created for the team role. This group has the same name as the role that you create.

---

 **Note**

Any new roles that you create are not available for life cycle, workflow, or team templates.

---

- Add users to the team by adding the users in the specific roles.

You can add users by selecting individual users or by selecting the user-defined groups or organizations that are available. For example, if the organization administrator has created groups for the organization context, you can select one or more of these groups to be a member of a role.

---



 **Note**

When the organization context is created, the site administrator has the option of restricting user access. By default, users are restricted so that they see only users or user-defined groups that belong to the organization. Selecting the **Restricted Directory Search** checkbox when the organization context is created provides the ability to search for all users or user-defined groups. If this checkbox was not selected when the organization was created, the site or organization administrator can update the organization context to select it. Only site administrators can search for other organization participants regardless of the checkbox selection.

---

- Change task assignments for members of a team.

As the membership of a team changes or members change responsibilities, you can manage the ownership of the tasks assigned to team members.

From **Products**  or **Libraries** , click the **Team** link to access the **Members** table. From this table, you can administer a product or library local team. For more information about teams, see [Teams and Team Template Administration on page 297](#).

Click the **Assignments** link to access a table of assignments with the following views: **All**, **Open**, **Overdue**, **Assigned to Me**, **Completed**, and **Uncompleted**. From this table you can manage the tasks assigned to your team.

---

## Using the Product and Library Utilities Page

The utilities listed on the **Utilities** page that is accessible from the **Product** and **Library** tabs allow you to perform administrative actions at a product and library level. The same set of utilities appears on both the **Product** and **Library** tabs. The difference is the context from which each utility is launched:

- Clicking a link from a product **Utilities** page launches the utility within the context of the current product.
- Clicking a link from a library **Utilities** page launches the utility within the context of the current library.

The utilities are grouped according to whether they are system administration utilities or business administration utilities. Many of the links provided on the page give you access to the utilities that you need to use to perform the duties described in [Typical Duties of Product and Library Administrators on page 172](#).

To explore the use of each utility, click the corresponding link on the page and then click the help icon in the window that opens.

## Out-of-the-box Product and Library Context Templates

When Windchill PDMLink is installed, the following product and library templates are loaded:

- Product Design – This template provides a demonstration of how to setup a product context for use with the One Phase Development and Two Phase Development life cycle templates and state-based versioning. As described in detail later in this section, the default set of roles defined is Members, Promotion Reviewers, Promotion Approvers, Collaboration Manager, Variance Approvers, Marketing, Procurement Engineer, Designer, Quality Engineer, Manufacturing Engineer, Design Team Leader, Option Administrator, Package Creator, Change Review Board, Change Admin I, Change Admin II, Change Admin III, and Received Delivery Manager. Also, the Guests and Product Manager roles are created automatically. Some basic information about these roles is as follows:
  - The Members role is used as a basic role to grant context team membership. A set of access rules are defined for confirmed members of the context team.
  - The Designer and Design Team Leader roles are unique to this template and identify the people who are responsible for creating and maintaining the business objects used to design a product.

- 
- Additionally, there are marketing and engineering roles that are unique to this template that can be used to delineate those functions in the design process.
  - Access policies defined for Change Objects have been setup to work in conjunction with the closed-loop change process.
  - Members of the Guest role are granted Read access to all objects.
  - General Product and General Library – These templates provide examples of how to setup basic access control for a general product or library context. As described in detail later in this section, the default set of roles defined is Members, Promotion Reviewers, Collaboration Manager, Variance Approvers, Promotion Approvers, Option Administrator, Package Creator, Change Review Board, Change Admin I, Change Admin II, Change Admin III, and Received Delivery Manager. Also, the Guests and Product/Library Manager roles are created automatically. Some basic information about these roles is as follows:
    - The Members role is used as a basic role to grant context team membership. A set of access rules are defined for confirmed members of the context team.
    - Access policies defined for Change Objects have been setup to work in conjunction with the closed-loop change process.
    - Members of the Guest role are granted Read access to all objects.

The product and library templates can define the same basic information that is discussed in [Context Administrative Items on page 61](#). If you want to create a new product or library template, see [Understanding Context Templates on page 393](#).

When users are working primarily with dynamic documents, you can start with the context template that is closest to your business model and modify the product or library that you create to meet your needs. For some general guidelines on administrative activities that you should consider doing, see [Configuring Products or Libraries for Dynamic Documents on page 224](#).

## Product Design Template

The Product Design out-of-the-box template defines the following context administrative items:

- Promotion Requests subfolder in the Default domain
- Context participation
- Context access control policies
- Object initialization rules for the following objects:
  - wt.maturity.PromotionNotice
  - wt.part.WTPart

- wt.epm.EPMDocument
- wt.doc.WTDocument

Through the object initialization rules, the following life cycle templates are set as defaults in the Design Product template:

- Two Phase Development life cycle template - default template for parts and functional specifications. It has the following states:



- One Phase Development life cycle template - default template for documents and CAD documents. It has the following states:

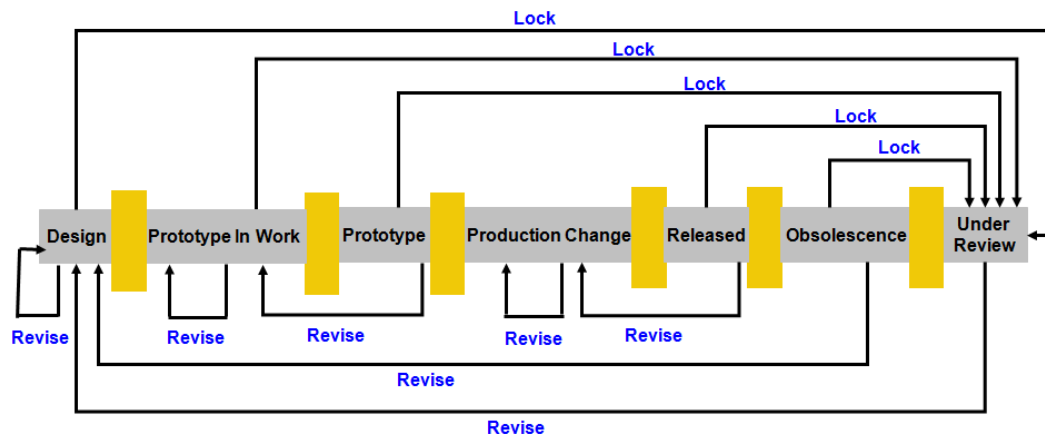


#### Note

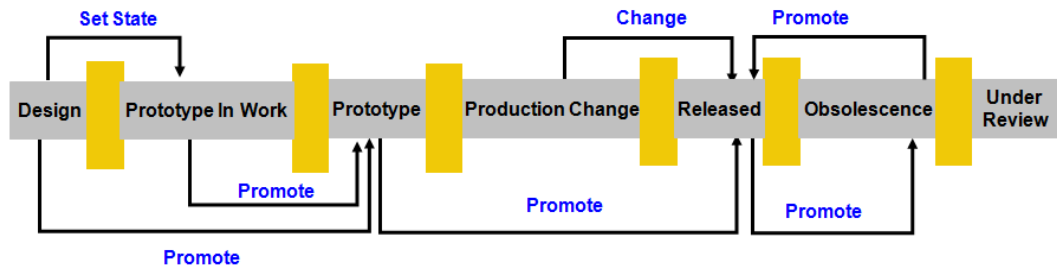
Although you can use multiple life cycle templates within a product context as is done with the demonstration Product Design template, PTC recommends that you become familiar with the functionality available through these life cycle templates and select one of the out-of-the-box templates (or create your own template) to use for all life-cycle managed objects in a product context.

The Two Phase Development and One Phase Development life cycle templates have the following transitions defined: Lock, Revise, Promote, Change, and Set State. Each template establishes different transition rules out of the box.

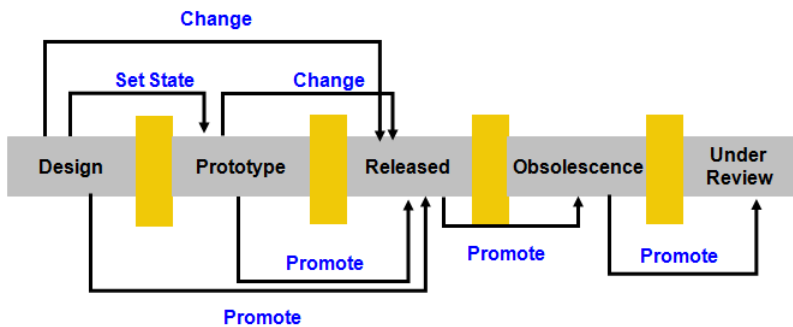
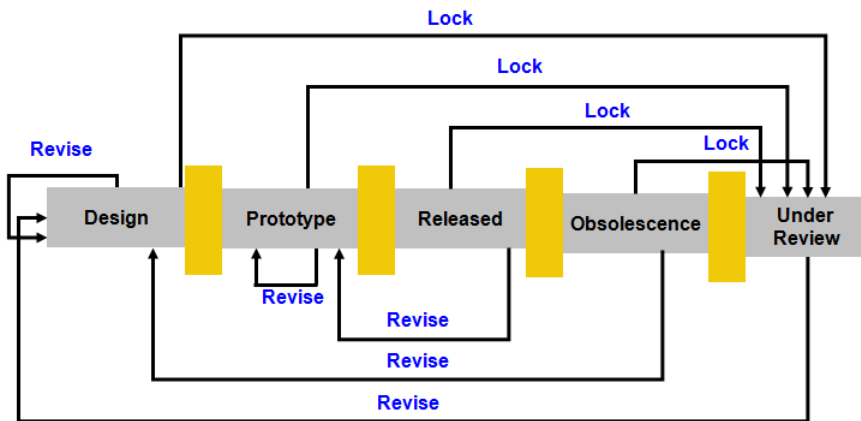
The following diagrams show the out-of-the-box transition rules for the Two Phase Development life cycle:







The following diagrams show the out-of-the-box transition rules for the One Phase Development life cycle:



For additional information about modifying or creating life cycle templates, see [Understanding Life Cycles on page 299](#). The out-of-the-box workflows that are used with the default life cycle templates are:

- Promotion Request Approval Process
- Promotion Request Review Process

For additional information about these workflows, see [Managing Promotion Processes in Windchill PDMLink on page 333](#).

The following sections describe the items that are defined in the Product Design template.

---

## Out-of-the-box Subfolder for wt.maturity.PromotionNotice Objects

In the Default cabinet and Default domain, the Product Design template creates the Promotion Requests subfolder. This folder is then defined as the default folder for the wt.maturity.PromotionNotice object type. Creating and using this folder is not required, but provides a useful folder for promotion requests.

## Out-of-the-box Context Participation

The Product Design template defines roles that are automatically included in product teams. These roles are the roles that automatically appear on the **Members** table. Additionally, roles available through the organization context can be added manually to the team.

The following roles are automatically included in the team:

- Product Manager
- Guest, which is the role to use for users who you do not want as a member of the team, but you do want them to have limited access to the product.

The out-of-the-box Product Design template adds the following roles to the team:

- Members, which is a role that can be used for team members who do not belong in other roles on the team.
- Change Admin I, which is the change administrator I change management role.
- Change Admin II, which is the change administrator II change management role.
- Change Admin III, which is the change administrator III change management role.
- Promotion Reviewers, which are the team members for reviewing promotion requests.
- Promotion Approvers, which are the team members for approving promotion requests.
- Change Review Board, which are the team members of the Change Review Board.
- Design Team Leader, which is the Design Team Leader role. This role is unique to this template.
- Designer, which is the role used to create, edit and manage business objects within the system. This role is unique to this template.
- Manufacturing Engineer, which is the Workflow Manufacturing Engineer role. This role is unique to this template.
- Marketing, which is the Marketing role. This role is unique to this template.

- 
- Procurement Engineer, which is the Procurement Engineer role. This role is unique to this template.
  - Quality Engineer, which is the Workflow Quality Engineer role. This role is unique to this template.
  - Collaboration Manager, which provides users in the Collaboration Manager role with some of the access rights needed for sharing objects across application contexts. If the **Access Permission Configuration (PDM)** security preference is configured to allow permissions to be modified, users in this role can also manage the ad hoc access control rights of others using the **Edit Access Control** action.
  - Variance Approvers
  - Option Administrator
  - Package Creator, which is a role that can be used to manage packages. This role is added to products created using this template, but no access control rules are specified in this template. Instead, all access control rules for this role are inherited from the organization under which the product was created.
  - Received Delivery Manager, which is a role that can be used to manage received deliveries. This role is added to products created using this template, but no access control rules are specified in this template. Instead, all access control rules for this role are inherited from the organization under which the product was created.

## Out-of-the-box Context Access Control Policies

When you create a product context using the out-of-the-box Product Design template, domain-based access control rules are defined in the System and Default domains of a product context. The rules that are created use the system groups that correspond to the out-of-the-box roles established for the team.

The following section lists the roles and their corresponding groups. Additional sections provide the out-of-the-box rules generated that reference the groups listed in the next section. All rules are generated as a result of administrative policy items that are in the out-of-the-box template.

---

### **Caution**

PTC recommends that you use caution when modifying the access control rules that are set when contexts are created. Modifying rules can cause problems with access to data and administrative functionality.

---

---

 **Note**

There are no out-of-the-box rules set for the Members or Change Admin III roles.

---

### Team Roles and Groups

The following table lists the out-of-the-box Product Design template team roles and system groups, and identifies which group that is associated with each role:

<b>Team Role</b>	<b>Corresponding System Group</b>
Change Admin I	CHANGE ADMINISTRATOR I
Change Admin II	CHANGE ADMINISTRATOR II
Change Admin III	CHANGE ADMINISTRATOR III
Change Review Board	CHANGE REQUEST REVIEW BOARD
Promotion Approvers	PROMOTION APPROVERS
Promotion Reviewers	PROMOTION REVIEWERS
Design Team Leader	DESIGN TEAM LEADER
Designer	DESIGNER
Manufacturing Engineer	MANUFACTURING ENGINEER
Marketing	MARKETING
Procurement Engineer	PROCUREMENT ENGINEER
Quality Engineer	QUALITY ENGINEER
Guests	GUEST
Members	MEMBERS
Product Manager	PRODUCT MANAGER
Collaboration Manager	COLLABORATION MANAGER
Variance Approvers	VARIANCE APPROVERS
Option Administrator	OPTION ADMINISTRATOR
Package Creator	PACKAGE CREATOR
Received Delivery Manager	RECEIVED DELIVERY MANAGER

---

 **Note**

As shown in the Generation Method column, the rules for Cabinet and SubFolder object types are defined programmatically when a product context is created; they are not defined through the template that is used. All other rules are defined through the template.

---

### Rules for the GUEST Group

Out-of-the-box Product Design access control rules for the GUEST group (Guest role) are described in the following sections.

#### Default Domain Rules for the GUEST Group

The following table lists the combination of object type, life cycle state, and granted permissions that the System domain out-of-the-box rules define for guests of a product:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
Cabinet	All	Read
SubFolder	All	Read
WTOBJECT	All	Read and Download
DiscreteActionItem	All	Read

#### System Domain Rules for the GUEST Group

The following table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for guests of a product:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
WTOBJECT	All	Read and Download

## Rules in Default Domain for the MARKETING Group

Out-of-the-box Product Design access control rules that are defined for the MARKETING group are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for the MARKETING group:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
EPMDocument	Prototype In Work	Read and Download
EPMDocument	Production Change	Read and Download
WTDocument	Design	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Prototype In Work	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Prototype	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Production Change	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Released	Revise
WTPart	Prototype In Work	Read and Download
WTPart	Prototype	Read and Download
WTPart	Production Change	Read and Download
WTPart	Released	Read and Download
WTPart	Obsolescence	Read and Download
WTPart	Under Review	Read and Download
WTPartAlternateRep	Prototype In Work	Read and Download
WTPartAlternateRep	Prototype	Read and Download

Object Type	State	Permissions
WTPartAlternateRep	Production Change	Read and Download
WTPartAlternateRep	Released	Read and Download
WTPartAlternateRep	Obsolescence	Read and Download
WTPartAlternateRep	Under Review	Read and Download

 **Note**

No rules are defined in the System domain for the MARKETING group.

Rules in Default Domain for the PROCUREMENT ENGINEER Group

Out-of-the-box Product Design access control rules that are defined for the PROCUREMENT ENGINEER group are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for the PROCUREMENT ENGINEER group:

Object Type	State	Permissions
EPMDocument	Prototype In Work	Read and Download
EPMDocument	Production Change	Read and Download
WTDocument	Design	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Prototype In Work	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Prototype	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Production Change	Read, Modify, Create, Delete, Revise, Download, Modify

Object Type	State	Permissions
		Content, Change Domain, Create by Move, and Change Context
WTDocument	Released	Revise
WTPart	Prototype In Work	Read and Download
WTPart	Prototype	Read and Download
WTPart	Production Change	Read and Download
WTPart	Released	Read and Download
WTPart	Obsolescence	Read and Download
WTPart	Under Review	Read and Download
WTPartAlternateRep	Prototype In Work	Read and Download
WTPartAlternateRep	Prototype	Read and Download
WTPartAlternateRep	Production Change	Read and Download
WTPartAlternateRep	Released	Read and Download
WTPartAlternateRep	Obsolescence	Read and Download
WTPartAlternateRep	Under Review	Read and Download

 **Note**

No rules are defined in the System domain for the PROCUREMENT ENGINEER group.

### Rules in Default Domain for the QUALITY ENGINEER Group

Out-of-the-box Product Design access control rules that are defined for the QUALITY ENGINEER group are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for the QUALITY ENGINEER group:

Object Type	State	Permissions
EPMDocument	Prototype In Work	Read and Download
EPMDocument	Production Change	Read and Download
WTDocument	Design	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Prototype In Work	Read, Modify, Create,



Object Type	State	Permissions
		Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Prototype	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Production Change	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Released	Revise
WTPart	Prototype In Work	Read and Download
WTPart	Prototype	Read and Download
WTPart	Production Change	Read and Download
WTPart	Released	Read and Download
WTPart	Obsolescence	Read and Download
WTPart	Under Review	Read and Download
WTPartAlternateRep	Prototype In Work	Read and Download
WTPartAlternateRep	Prototype	Read and Download
WTPartAlternateRep	Production Change	Read and Download
WTPartAlternateRep	Released	Read and Download
WTPartAlternateRep	Obsolescence	Read and Download
WTPartAlternateRep	Under Review	Read and Download

 **Note**

No rules are defined in the System domain for the QUALITY ENGINEER group.

## Rules in Default Domain for the DESIGNER Group

Out-of-the-box Product Design access control rules that are defined for the DESIGNER group are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for the DESIGNER group:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
EPMDocument	Design	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, Change Context, and Set State
EPMDocument	Prototype In Work	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
EPMDocument	Prototype	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
EPMDocument	Production Change	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
EPMDocument	Released	Read, Revise, and Download
EPMDocument	Obsolescence	Read and Download
EPMDocument	Under Review	Read and Download
WTDocument	Design	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context, and Set State
WTDocument	Prototype In Work	Read, Modify, Create, Delete, Revise,

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
		Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Prototype	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Production Change	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Released	Revise
WTPart	Design	Read, Modify, Create, Delete, Revise, New View Version, Download, Modify Content, Change Domain, Create by Move, Change Context, and Set State
WTPart	Prototype In Work	Read, Modify, Create, Delete, Revise, New View Version, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTPart	Prototype	Read, Modify, Create, Delete, Revise, New View Version, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTPart	Production Change	Read, Modify, Create, Delete, Revise, New View Version, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTPart	Released	Read, Revise, New View

Object Type	State	Permissions
		Version, and Download
WTPart	Obsolescence	Read and Download
WTPart	Under Review	Read and Download
WTPartAlternateRep	Design	Read, Download, Modify, Create, Delete, Revise, Modify Content, Change Domain, Create by Move, Change Context, and Set State
WTPartAlternateRep	Prototype In Work	Read, Download, Modify, Create, Delete, Revise, Modify Content, Change Domain, Create by Move, and Change Context
WTPartAlternateRep	Prototype	Read, Download, Modify, Create, Delete, Revise, Modify Content, Change Domain, Create by Move, and Change Context
WTPartAlternateRep	Production Change	Read, Download, Modify, Create, Delete, Revise, Modify Content, Change Domain, Create by Move, and Change Context
WTPartAlternateRep	Released	Read, Download, and Revise
WTPartAlternateRep	Obsolescence	Read and Download
WTPartAlternateRep	Under Review	Read and Download

 **Note**

No rules are defined in the System domain for the DESIGNER group.

## Rules in Default Domain for the MANUFACTURING ENGINEER Group

Out-of-the-box Product Design access control rules that are defined for the MANUFACTURING ENGINEER group are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for the MANUFACTURING ENGINEER group:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
EPMDocument	Design	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, Change Context, and Set State
EPMDocument	Prototype In Work	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
EPMDocument	Prototype	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
EPMDocument	Production Change	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
EPMDocument	Released	Read, Revise, and Download
EPMDocument	Obsolescence	Read and Download
EPMDocument	Under Review	Read and Download
WTDocument	Design	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, Change Context, and Set State
WTDocument	Prototype In Work	Read, Modify, Create, Delete, Revise,

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
		Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Prototype	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Production Change	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Released	Revise
WTPart	Design	Read, Modify, Create, Delete, Revise, New View Version, Download, Modify Content, Change Domain, Create by Move, Change Context, and Set State
WTPart	Prototype In Work	Read, Modify, Create, Delete, Revise, New View Version, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTPart	Prototype	Read, Modify, Create, Delete, Revise, New View Version, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTPart	Production Change	Read, Modify, Create, Delete, Revise, New View Version, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTPart	Released	Read, Revise, New View

Object Type	State	Permissions
		Version, and Download
WTPart	Obsolescence	Read and Download
WTPart	Under Review	Read and Download
WTPartAlternateRep	Design	Read, Download, Modify, Create, Delete, Revise, Modify Content, Change Domain, Create by Move, Change Context, and Set State
WTPartAlternateRep	Prototype In Work	Read, Download, Modify, Create, Delete, Revise, Modify Content, Change Domain, Create by Move, and Change Context
WTPartAlternateRep	Prototype	Read, Download, Modify, Create, Delete, Revise, Modify Content, Change Domain, Create by Move, and Change Context
WTPartAlternateRep	Production Change	Read, Download, Modify, Create, Delete, Revise, Modify Content, Change Domain, Create by Move, and Change Context
WTPartAlternateRep	Released	Read, Download, and Revise
WTPartAlternateRep	Obsolescence	Read and Download
WTPartAlternateRep	Under Review	Read and Download

 **Note**

No rules are defined in the System domain for the MANUFACTURING ENGINEER group.

## Rules in Default Domain for the DESIGN TEAM LEADER Group

Out-of-the-box Product Design access control rules that are defined for the DESIGN TEAM LEADER group are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for the DESIGN TEAM LEADER group:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
EPMDocument	Design	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, Change Context, and Set State
EPMDocument	Prototype In Work	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
EPMDocument	Prototype	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
EPMDocument	Production Change	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
EPMDocument	Released	Read, Revise, and Download
EPMDocument	Obsolescence	Read and Download
EPMDocument	Under Review	Read and Download
WTDocument	Design	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, Change Context, and Set State
WTDocument	Prototype In Work	Read, Modify, Create, Delete, Revise,



<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
		Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Prototype	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Production Change	Read, Modify, Create, Delete, Revise, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Released	Revise
WTPart	Design	Read, Modify, Create, Delete, Revise, New View Version, Download, Modify Content, Change Domain, Create by Move, Change Context, and Set State
WTPart	Prototype In Work	Read, Modify, Create, Delete, Revise, New View Version, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTPart	Prototype	Read, Modify, Create, Delete, Revise, New View Version, Download, Modify Content, Change Domain, Change Context, and Create by Move
WTPart	Production Change	Read, Modify, Create, Delete, Revise, New View Version, Download, Modify Content, Change Domain, Create by Move, and Change Context
WTPart	Released	Read, Revise, New View

Object Type	State	Permissions
		Version, and Download
WTPart	Obsolescence	Read and Download
WTPart	Under Review	Read and Download
WTPartAlternateRep	Design	Read, Download, Modify, Create, Delete, Revise, Modify Content, Change Domain, Create by Move, Change Context, and Set State
WTPartAlternateRep	Prototype In Work	Read, Download, Modify, Create, Delete, Revise, Modify Content, Change Domain, Create by Move, and Change Context
WTPartAlternateRep	Prototype	Read, Download, Modify, Create, Delete, Revise, Modify Content, Change Domain, Create by Move, and Change Context
WTPartAlternateRep	Production Change	Read, Download, Modify, Create, Delete, Revise, Modify Content, Change Domain, Create by Move, and Change Context
WTPartAlternateRep	Released	Read, Download, and Revise
WTPartAlternateRep	Obsolescence	Read and Download
WTPartAlternateRep	Under Review	Read and Download

 **Note**

No rules are defined in the System domain for the DESIGN TEAM LEADER group.

---

### Rules in Default Domain for PROMOTION REVIEWERS Group

Out-of-the-box Product Design access control rule for the PROMOTION REVIEWERS group is described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
PromotionNotice	Under Review	Read and Download

---

#### **Note**

No rules are defined in the System domain for the PROMOTION REVIEWERS group.

---

### Rules in Default Domain for CHANGE REQUEST REVIEW BOARD Group

Out-of-the-box Product Design access control rules for the CHANGE REQUEST REVIEW BOARD group are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
WTChangeRequest2	Under Review	Read and Download
WTChangeOrder2	Under Review	Read and Download

---

#### **Note**

No rules are defined in the System domain for the CHANGE REQUEST REVIEW BOARD group.

---

### Rules in Default Domain for PROMOTION APPROVERS Group

Out-of-the-box Product Design access control rule for the PROMOTION APPROVERS group is described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
PromotionNotice	Under Review	Read and Download

---

 **Note**

No rules are defined in the System domain for the PROMOTION APPROVERS group.

---

### Rules for PRODUCT MANAGER Group

Out-of-the-box Product Design access control rules for the PRODUCT MANAGER group (Product Manager role) are described in the following sections.

#### Default Domain Rule for PRODUCT MANAGER Group

The following table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for the Product Manager:

Object Type	State	Permissions
WObject	All	Full control (All)

#### System Domain Rule for PRODUCT MANAGER Group

The following table lists the combination of object type, life cycle state, and granted permissions that the System domain out-of-the-box rules define for the Product Manager:

Object Type	State	Permissions
WObject	All	Full control (All)

### Rules in Default Domain for CHANGE ADMINISTRATOR I Group

Out-of-the-box Product Design access control rules for the CHANGE ADMINISTRATOR I group (Change Admin I role) are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
WTChangeActivity2	All	Full Control (All)
WTChangeIssue	All	Full Control (All)
WTChangeOrder2	All	Full Control (All)
WTChangeProposal	All	Full Control (All)
WTChangeRequest2	All	Full Control (All)
WTVariance	All	Full Control (All)

---

 **Note**

No rules are defined in the System domain for the CHANGE ADMINISTRATOR I group.

---

Rules in Default Domain for CHANGE ADMINISTRATOR II Group

Out-of-the-box Product Design access control rules for the CHANGE ADMINISTRATOR II group (Change Admin II role) are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
WTChangeActivity2	All	Full Control (All)
WTChangeOrder2	All	Full Control (All)
WTChangeProposal	All	Read and Download

---

 **Note**

No rules are defined in the System domain for the CHANGE ADMINISTRATOR II group.

---

Rules in Default Domain for TEAMMEMBERS Group

Out-of-the-box Product Design access control rule for the TEAMMEMBERS group is described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
WTPart	All	Read and Download
WTPart	Prototype	Read and Download
WTPart	Released	Read and Download
WTPart	Obsolescence	Read and Download
WTPart	Under Review	Read and Download
WTPartSubstituteLink	All	Read, Modify, Create, Delete, Change Domain, and Create by Move
WTPartAlternateLink	All	Read, Modify, Create, Delete, Change Domain, and Create by Move

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
WTDocument	All	Read and Download
WTDocument	Prototype	Read and Download
WTDocument	Released	Read and Download
WTDocument	Obsolescence	Read and Download
WTDocument	Under Review	Read and Download
EPMDocument	All	Read and Download
EPMDocument	Prototype	Read and Download
EPMDocument	Released	Read and Download
EPMDocument	Obsolescence	Read and Download
EPMDocument	Under Review	Read and Download
ManagedBaseline	All	Read
ManagedBaseline	In Work	Read, Modify, Create, Delete, Change Domain, Create by Move, Change Context, and Modify Identity
StructuredAnnotationSet	All	Read
StructuredAnnotationSet	In Work	Read, Modify, Create, Delete, Change Domain, Create by Move, and Change Context
WTProductConfiguration	All	Read
WTProductConfiguration	In Work	Read, Modify, Create, Delete, Change Domain, Create by Move, and Change Context
WTProductInstance2	All	Read
WTProductInstance2	In Work	Read, Modify, Create, Delete, Change Domain, Create by Move, and Change Context
WTProductInstance2	Released	Read and Revise
WTChangeIssue	All	Read and Download
WTChangeIssue	Open	Read, Modify, Create, Modify Content, Download, and Create by Move
WTChangeRequest2	All	Read and Download
WTChangeRequest2	Open	Read, Modify, Create, Modify Content, Download, and Create by Move
WTChangeProposal	Open	Read, Modify, Create, Modify Content, Download, and Create by Move
WTChangeOrder2	All	Read and Download

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
WTChangeOrder2	Open	Read, Modify, Modify Content, and Download
WTChangeOrder2	Implementation	Read, Modify, Modify Content, and Download
WTChangeActivity2	All	Read and Download
WTChangeActivity2	Open	Read, Modify, Modify Content, and Download
WTChangeActivity2	Implementation	Read, Modify, Modify Content, and Download
PromotionNotice	All	Read and Download
PromotionNotice	Open	Read, Modify, Create, Modify Content, Delete, Download, Change Domain, Create by Move, and Change Context
WTVariance	All	Read and Download
WTVariance	Open	Read, Modify, Create, Modify Content, Download, and Modify Identity
WTObject	All	Read
WfExecutionObject	All	Read, Modify, Create, Download, and Modify Content
Cabinet	All	Read and Modify
SubFolder	All	Read and Modify
DiscreteActionItem	All	Read
WTPartAlternateRep	All	Read and Download
WTPartAlternateRep	In Work	Modify, Create, Delete, Modify Content, Change Domain, Create by Move, and Change Context
WTPartAlternateRep	Prototype	Read and Download
WTPartAlternateRep	Released	Read and Download
WTPartAlternateRep	Obsolescence	Read and Download
WTPartAlternateRep	Under Review	Read and Download
WTPartAlternateRep	Released	Revise
OptionSet	All	Read
Option	All	Read
Choice	All	Read

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
ChoiceRule	All	Read
Group	All	Read

#### Rules in System Domain for TEAMMEMBERS Group

Out-of-the-box Product Design access control rule for the TEAMMEMBERS group is described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the System domain out-of-the-box rules:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
WtObject	All	Read
WfExecutionObject	All	Read, Modify, Create, Download, and Modify Content

#### Rules in Default Domain for COLLABORATION MANAGER Group

Out-of-the-box Product Design access control rules for the COLLABORATION MANAGER group are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
WtDocument	All	Change Permissions
WtPart	All	Change Permissions
EPMDocument	All	Change Permissions
WtChangeIssue	All	Change Permissions
WtChangeProposal	All	Change Permissions
WtChangeRequest2	All	Change Permissions
WtChangeOrder2	All	Change Permissions
WtChangeActivity2	All	Change Permissions
WtVariance	All	Change Permissions
VariantSpec	All	Change Permissions
SubFolder	All	Change Permissions
WtPartAlternateRep	All	Change Permissions



---

 **Note**

No rules are defined in the System domain for the COLLABORATION MANAGER group.

---

#### Rules in Default Domain for VARIANCE APPROVERS Group

Out-of-the-box Product Design access control rule for the VARIANCE APPROVERS group is described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
WTVariance	Under Review	Read and Download

---

 **Note**

No rules are defined in the System domain for the VARIANCE APPROVERS group.

---

#### Rules for SHARED TEAM MANAGER Group

Out-of-the-box Product Design access control rules for the SHARED TEAM MANAGER group (Shared Team Manager role) are described in the following sections.

##### Default Domain Rule for SHARED TEAM MANAGER Group

The following table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for the Shared Team Manager:

Object Type	State	Permissions
WTObject	All	Full control (All)

##### System Domain Rule for SHARED TEAM MANAGER Group

The following table lists the combination of object type, life cycle state, and granted permissions that the System domain out-of-the-box rules define for the Shared Team Manager:

Object Type	State	Permissions
WTObject	All	Full control (All)

---

## Rules for OPTION ADMINISTRATOR Group

Out-of-the-box Product Design access control rules for the OPTION ADMINISTRATOR group are described in the following sections.

### Default Domain Rules for OPTION ADMINISTRATOR Group

The following table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for the Option Administrator:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
OptionSet	All	Full control (All)
Option	All	Full control (All)
Choice	All	Full control (All)
ChoiceRule	All	Full control (All)
Group	All	Full control (All)

### System Domain Rules for OPTION ADMINISTRATOR Group

The following table lists the combination of object type, life cycle state, and granted permissions that the System domain out-of-the-box rules define for the Option Administrator:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
Cabinet	All	Full control (All)
OptionSet	All	Full control (All)
Option	All	Full control (All)
Choice	All	Full control (All)
ChoiceRule	All	Full control (All)
Group	All	Full control (All)

### Rules in Default Domain for OWNER

OWNER is a pseudo role that is used by Windchill to represent the object owner. Out-of-the-box Product Design access control rule for the OWNER pseudo role is described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
DiscreteActionItem	All	Modify
PromotionNotice	Open	Read, Delete, Download, Change Domain, and Change Context

Object Type	State	Permissions
PromotionNotice	Under Review	Read, Delete, Download, Change Domain, and Change Context
PromotionNotice	Rejected	Read, Delete, Download, Change Domain, and Change Context

## Out-of-the-box Object Initialization Rules

The Product Design template sets object initialization rules for the following object types:

- wt.maturity.PromotionNotice
- wt.part.WTPart
- wt.epm.EPMDocument
- wt.doc.WTDocument

The following table lists the object types, attributes, and default values set by the object initialization rules that are in the template:

Object Type	Attribute	Default Value
PromotionNotice	folder.id	/Default/Promotion Requests
WTPart	folder.id	/Default
WTPart	lifeCycle.id	Two Phase Development
WTPart	teamTemaplate.id	Default
WTPart	MBA versionInfo	wt.series.HarvardSeries.StateBased
EPMDocument	folder.id	/Default
EPMDocument	lifeCycle.id	One Phase Development
EPMDocument	teamTemaplate.id	Default
EPMDocument	MBA versionInfo	wt.series.HarvardSeries.StateBased
WTDocument	folder.id	/Default
WTDocument	lifeCycle.id	One Phase Development
WTDocument	teamTemaplate.id	Default
WTDocument	MBA versionInfo	wt.series.HarvardSeries.StateBased

---

## Note

Setting object initialization rules in a product template means that the rules are different than those set for the organization or site. This is the case with this template and the out-of-the-box object initialization rules that are set in the site context. PTC recommends that you only use this template as a demonstration template and consider setting those rules that you want to use for parts, documents, and CAD documents in either the organization or site context.

For additional information, see the Object Initialization Rules chapter of the *PTC Windchill Specialized Administration Guide*.

## General Product and General Library Templates

The General Product and General Library out-of-the-box templates define only the following context administrative items:

- Context participation
- Context access control policies

The following sections describe the items that are defined in these templates.

### Out-of-the-box Context Participation

The General Product and General Library templates define roles that are automatically included in product and library teams. These roles are the roles that automatically appear on the **Members** table. Additionally, roles available through the organization context can be added to the team.

The following roles are automatically included in the team:

- Product Manager (for products) and Library Manager (for libraries)
- Guest, which is the role to use for users who you do not want as a member of the team, but you do want them to have limited access to the product or library. Users who are guests will not see the product or library on their Product List or Library List. They would need to search for the product or library to locate it. Out of the box, guests have only read access to product or library data.

The out-of-the-box General Product and General Library templates add the following roles to the team:

- Members, which is a role that can be used for team members who do not belong in other roles on the team.
- Change Admin I, which is the change administrator I change management role

- 
- Change Admin II, which is the change administrator II change management role
  - Change Admin III, which is the change administrator III change management role
  - Promotion Reviewers, which are the team members for reviewing Promotion Requests
  - Promotion Approvers, which are the team members for approving Promotion Requests
  - Change Review Board, which are the team members of the Change Review Board
  - Collaboration Manager, which provides team members in this role with some of the access rights needed for sharing objects across application contexts.
  - Variance Approvers
  - Option Administrator
  - Package Creator, which is a role that can be used to manage packages. This role is added to products and libraries created using one of these templates, but no access control rules are specified in these templates. Instead, all access control rules for this role are inherited from the organization under which the product or library was created.
  - Received Delivery Manager, which is a role that can be used to manage received deliveries. This role is added to products and libraries created using one of these templates, but no access control rules are specified in these templates. Instead, all access control rules for this role are inherited from the organization under which the product or library was created.

## **Out-of-the-box Context Access Control Policies**

When you create a product or library context using the out-of-the-box General Product and General Library templates, domain-based access control rules are defined in the System and Default domains of a product or library context. The rules that are created reference the groups that correspond to the out-of-the-box roles established for the team.

The following section lists the roles and their corresponding groups. Additional sections provide the out-of-the-box rules that reference the groups listed in the next section. All rules are generated as a result of administrative policy items that are in the out-of-the-box templates.

---

**⚠ Caution**

PTC recommends that you use caution when modifying the access control rules that are set when contexts are created. Modifying rules can cause problems with access to data and administrative functionality.

---

**🗨 Note**

There are no out-of-the-box rules set for the Members or Change Admin III roles.

---

### Team Roles and Groups

The following table lists the out-of-the-box General Product and General Library team roles and groups, and identifies which group that is associated with each role:

<b>Team Role</b>	<b>Corresponding Group</b>
Change Admin I	CHANGE ADMINISTRATOR I
Change Admin II	CHANGE ADMINISTRATOR II
Change Admin III	CHANGE ADMINISTRATOR III
Change Review Board	CHANGE REQUEST REVIEW BOARD
Promotion Approvers	PROMOTION APPROVERS
Promotion Reviewers	PROMOTION REVIEWERS
Guests	GUEST
Members	MEMBERS
Product Manager (products only)	PRODUCT MANAGER
Library Manager (libraries only)	LIBRARY MANAGER
Collaboration Manager	COLLABORATION MANAGER
Variance Approvers	VARIANCE APPROVERS
Option Administrator	OPTION ADMINISTRATOR
Package Creator	PACKAGE CREATOR
Received Delivery Manager	RECEIVED DELIVERY MANAGER

### Rules for the GUEST Group

Out-of-the-box General Product and General Library access control rules for the GUEST group (Guest role) are described in the following sections.

---

### Default Domain Rules for the GUEST Group

The following table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for guests of a product or library:

Object Type	State	Permissions
Cabinet	All	Read
DiscreteActionItem	All	Read
SubFolder	All	Read
WTOBJECT	All	Read and Download

### System Domain Rules for the GUEST Group

The following table lists the combination of object type, life cycle state, and granted permissions that the System domain out-of-the-box rules define for the guests of a product or library:

Object Type	State	Permissions
WTOBJECT	All	Read and Download

### Rules in Default Domain for CHANGE REQUEST REVIEW BOARD Group

Out-of-the-box General Product and General Library access control rules for the CHANGE REQUEST REVIEW BOARD group are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
WTChangeRequest2	Under Review	Read and Download
WTChangeOrder2	Under Review	Read and Download

---

#### **Note**

No rules are defined in the System domain for the CHANGE REQUEST REVIEW BOARD group.

---

---

### Rules in Default Domain for PROMOTION APPROVERS Group

Out-of-the-box General Product and General Library access control rule for the PROMOTION APPROVERS group is described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
PromotionNotice	Under Review	Read and Download

---

 **Note**

No rules are defined in the System domain for the PROMOTION APPROVERS group.

---

### Rules in Default Domain for PROMOTION REVIEWERS Group

Out-of-the-box General Product and General Library access control rule for the PROMOTION REVIEWERS group is described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
PromotionNotice	Under Review	Read and Download

---

 **Note**

No rules are defined in the System domain for the PROMOTION REVIEWERS group.

---

### Rules for PRODUCT MANAGER and LIBRARY MANAGER Groups

Out-of-the-box General Product and General Library access control rules for the PRODUCT MANAGER group (Product Manager role) and LIBRARY MANAGER group (Library Manager role) are described in the following sections.



---

### Default Domain Rule for PRODUCT MANAGER and LIBRARY MANAGER Groups

The following table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for the Product Manager or Library Manager:

Object Type	State	Permissions
WTOBJECT	All	Full control (All)

### System Domain Rule for PRODUCT MANAGER and LIBRARY MANAGER Groups

The following table lists the combination of object type, life cycle state, and granted permissions that the System domain out-of-the-box rules define for the Product Manager or Library Manager:

Object Type	State	Permissions
WTOBJECT	All	Full control (All)

### Rules in Default Domain for CHANGE ADMINISTRATOR I Group

Out-of-the-box General Product and General Library access control rules for the CHANGE ADMINISTRATOR I group (Change Admin I role) are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
WTChangeActivity2	All	Full Control (All)
WTChangeIssue	All	Full Control (All)
WTChangeOrder2	All	Full Control (All)
WTChangeProposal	All	Full Control (All)
WTChangeRequest2	All	Full Control (All)
WTVariance	All	Full Control (All)

---

#### **Note**

No rules are defined in the System domain for the CHANGE ADMINISTRATOR I group.

---

---

## Rules in Default Domain for CHANGE ADMINISTRATOR II Group

Out-of-the-box General Product and General Library access control rules for the CHANGE ADMINISTRATOR II group (Change Admin II role) are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
WTChangeActivity2	All	Full Control (All)
WTChangeOrder2	All	Full Control (All)
WTChangeProposal	All	Read and Download

---

### Note

No rules are defined in the System domain for the CHANGE ADMINISTRATOR II group.

---

## Rules in Default Domain for TEAMMEMBERS Group

Out-of-the-box General Product and General Library access control rules for the TEAMMEMBERS group is described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
WTDocument	All	Read and Download
WTDocument	In Work	Modify, Create, Delete, Modify Content, Change Domain, Create by Move, and Change Context
WTDocument	Released	Revise
WTPart	All	Read and Download
WTPart	In Work	Modify, Create, Delete, Modify Content, Change Domain, Create by Move, and Change Context
WTPart	Released	Revise and New View Version
WTPartSubstituteLink	All	Read, Modify, Create, and Delete
WTPartAlternateLink	All	Read, Modify, Create, and Delete
EPMDocument	All	Read and Download

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
EPMDocument	In Work	Modify, Create, Delete, Modify Content, Change Domain, Create by Move, and Change Context
EPMDocument	Released	Revise
ManagedBaseline	All	Read
ManagedBaseline	In Work	Modify, Create, Delete, Change Domain, Create by Move, and Change Context
StructuredAnnotationSet	All	Read
StructuredAnnotationSet	In Work	Modify, Create, and Delete
WTProductConfiguration	All	Read
WTProductConfiguration	In Work	Modify, Create, and Delete
WTProductInstance2	All	Read
WTProductInstance2	In Work	Modify, Create, and Delete
WTProductInstance2	Released	Revise
WTChangeIssue	All	Read and Download
WTChangeIssue	Open	Modify, Create, and Modify Content
WTChangeRequest2	All	Read and Download
WTChangeRequest2	Open	Modify, Create, and Modify Content
WTChangeProposal	Open	Modify, Create, and Modify Content
WTChangeOrder2	All	Read and Download
WTChangeOrder2	Open	Modify and Modify Content
WTChangeOrder2	Implementation	Modify and Modify Content
WTChangeActivity2	All	Read and Download
WTChangeActivity2	Open	Modify and Modify Content
WTChangeActivity2	Implementation	Modify and Modify Content
PromotionNotice	All	Read and Download
PromotionNotice	Open	Modify, Create, and Modify Content

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
WTVariance	All	Read and Download
WTVariance	Open	Modify, Create, and Modify Content
WTOBJECT	All	Read
WfExecutionObject	All	Read, Modify, Create, Download, and Modify Content
Cabinet	All	Read and Modify
SubFolder	All	Read and Modify
DiscreteActionItem	All	Read
WTPartAlternateRep	All	Read and Download
WTPartAlternateRep	In Work	Modify, Create, Delete, Modify Content, Change Domain, Create by Move, and Change Context
WTPartAlternateRep	Released	Revise
OptionSet	All	Read
Option	All	Read
Choice	All	Read
ChoiceRule	All	Read
Group	All	Read
VariantSpec	All	Read and Download
VariantSpec	In Work	Modify, Create, Modify Content, Delete, Create by Move, Change Domain, and Change Context

#### Rules in System Domain for TEAMMEMBERS Group

Out-of-the-box General Product and General Library access control rules for the TEAMMEMBERS group is described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the System domain out-of-the-box rules:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
WTOBJECT	All	Read
WfExecutionObject	All	Read, Modify, Create, Download, and Modify Content

---

### Rules in Default Domain for COLLABORATION MANAGER Group

Out-of-the-box Product Design access control rules for the COLLABORATION MANAGER group are described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
WTDocument	All	Change Permissions
WTPart	All	Change Permissions
EPMDocument	All	Change Permissions
WTChangeIssue	All	Change Permissions
WTChangeProposal	All	Change Permissions
WTChangeRequest2	All	Change Permissions
WTChangeOrder2	All	Change Permissions
WTChangeActivity2	All	Change Permissions
WTVariance	All	Change Permissions
VariantSpec	All	Change Permissions
SubFolder	All	Change Permissions
WTPartAlternateRep	All	Change Permissions

---

#### Note

No rules are defined in the System domain for the COLLABORATION MANAGER group.

---

### Rules in Default Domain for VARIANCE APPROVERS Group

Out-of-the-box Product Design access control rule for the VARIANCE APPROVERS group is described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
WTVariance	Under Review	Read and Download

### Rules for SHARED TEAM MANAGER Group

Out-of-the-box Product Design access control rules for the SHARED TEAM MANAGER group (Shared Team Manager role) are described in the following sections.

---

### Default Domain Rule for SHARED TEAM MANAGER Group

The following table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for the Shared Team Manager:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
WObject	All	Full control (All)

### System Domain Rule for SHARED TEAM MANAGER Group

The following table lists the combination of object type, life cycle state, and granted permissions that the System domain out-of-the-box rules define for the Shared Team Manager:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
WObject	All	Full control (All)

### Rules for OPTION ADMINISTRATOR Group

Out-of-the-box Product Design access control rules for the OPTION ADMINISTRATOR group are described in the following sections.

### Default Domain Rules for OPTION ADMINISTRATOR Group

The following table lists the combination of object type, life cycle state, and granted permissions that the Default domain out-of-the-box rules define for the Option Administrator:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
OptionSet	All	Full control (All)
Option	All	Full control (All)
Choice	All	Full control (All)
ChoiceRule	All	Full control (All)
Group	All	Full control (All)

### System Domain Rules for OPTION ADMINISTRATOR Group

The following table lists the combination of object type, life cycle state, and granted permissions that the System domain out-of-the-box rules define for the Option Administrator:

<b>Object Type</b>	<b>State</b>	<b>Permissions</b>
Cabinet	All	Full control (All)
OptionSet	All	Full control (All)
Option	All	Full control (All)

Object Type	State	Permissions
Choice	All	Full control (All)
ChoiceRule	All	Full control (All)
Group	All	Full control (All)

#### Rules in Default Domain for OWNER

OWNER is a pseudo role that is used by Windchill to represent the object owner. Out-of-the-box Product Design access control rule for the OWNER pseudo role is described in the following table. The table lists the combination of object type, life cycle state, and granted permissions that are defined in the Default domain out-of-the-box rules:

Object Type	State	Permissions
DiscreteActionItem	All	Modify
PromotionNotice	Under Review	Read, Download, and Delete
PromotionNotice	Rejected	Read, Download, and Delete

## Updating Access Control Rules

### Caution

PTC recommends that you use caution when modifying the access control rules that are set when contexts are created. Modifying rules can cause problems with access to data and administrative functionality.

To adjust the access control rules that are defined, you can use the **Policy Administration** utility. Navigate to the product or library and click the **Policy Administration** link from the **Utilities** page. Select the /Default domain and click **Update**. From the **Administrative Domain** window, click the **Access Control** tab to view the access control rules for the domain. From this tab, you can create new rules and update or delete existing rules. When creating or updating rules, the **Groups** tab shows the groups available from in the current context. These groups include the groups that map to the roles being used in the product or library team.

For more information about creating or updating access control rules, see the Access Control chapter of the *PTC Windchill Specialized Administration Guide*.

---

## Configuring Products or Libraries for Dynamic Documents

Products and libraries that will be used primarily for managing dynamic documents are generally no different from products and libraries used for managing parts. When setting up a product or library for this purpose, review all of the activities described in [Typical Duties of Product and Library Administrators on page 172](#), keeping in mind that the main business object type being managed is the Dynamic Document object type.

Since the out-of-the-box context templates do not have anything specifically set up for this object type, you may want to look closely at the following administration activities as they relate to managing this type of object:

- Create folders for use in organizing the dynamic documents that are checked into your Windchill solution.
- Create additional subtypes and attributes for dynamic documents. The subtypes and attributes correspond with Arbortext document types and attributes that are set up for use with the Arbortext Editor.

For more information, see the *PTC Windchill Specialized Administration Guide*.

- Set up specific teams, life cycle templates, and workflow templates for use with dynamic documents. For more information about these topics, see the teams help, [Understanding Life Cycles on page 299](#), and [Understanding Workflow on page 337](#).
- Review and set object initialization rules for Dynamic Document subtypes. for more information on setting object initialization rules, see the *PTC Windchill Specialized Administration Guide*



---

### Note

Autonumbering must be turned on for the Dynamic Document subtype and its subtypes. By default, autonumbering is turned on for the wt.epm.EPMDocument type and all of its subtypes through an object initialization rule in the site context. Since dynamic documents are subtypes of the wt.epm.EPMDocument type, the rule automatically applies dynamic documents unless additional rules have been set up that override the site context rule.

For more information about numbering objects, see the *PTC Windchill Specialized Administration Guide*.

- Set access control policies on the Dynamic Document subtypes. For more information on setting access control policies, see [Administering Domains and Policies on page 86](#).

Additionally, there are activities unique to using the Arbortext Editor and the Arbortext Publishing Engine with product and libraries that need to be performed. These include the following:

- Establish the configuration settings used by the Windchill connection to Arbortext Editor. For more information, see the Windchill connection online help accessible from the Arbortext Editor.
- Manage the bursting rules used when a dynamic document is stored in Windchill. For more information on bursting rules, see the Arbortext Editor online help.
- Manage additional attributes for WTDocument object type that are used by the publishing agent when publishing dynamic documents. For more information on specifying publishing rules, including specifying rules for the resulting documents, see the *PTC Windchill Visualization Services Administrator's Guide*.

For more information about using product and libraries with Arbortext products to manage dynamic documents, see the *Getting Started Authoring PTC Arbortext Documents* guide.

## Configuring Part and Document Relationships

The relationships between a part and a document, two parts, or two documents vary depending upon how the two objects are linked. This section briefly describes the different types of links that form these relationships and then describes the configuration options that are available.

---

## Part to Document Relationships

### Note

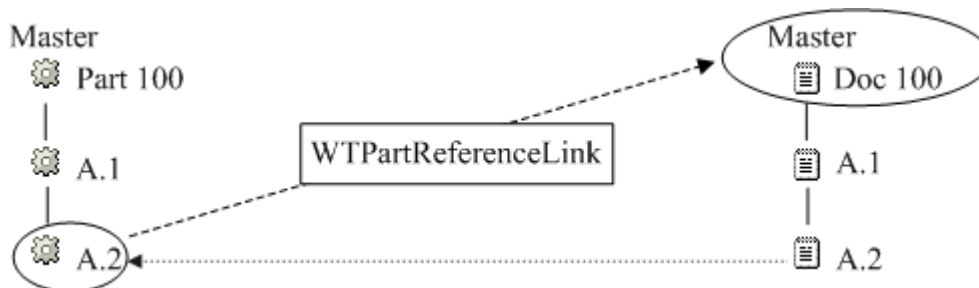
Part to document relationships do not apply to Arbortext Content Manager or Pro/INTRALINK 10.1.

---

The association between a part and a document is created from the part information page, document information page, or Product Structure Explorer. Associations can be viewed from the **Related Objects** tab on the part information page. These same relationships can be viewed from the **Related Objects** tab of the document information page.

There are two types of links that can be established:

- A **Part Reference Link** (WTPartReferenceLink)—Using this type of link always links the part to the master document. Regardless of the version of the document the user selects, the part will always link to the master document when this link type is used. This is true even when the system has been configured to allow the user to select the link type and the document type.



Reference links always display a document version of the master based on life cycle state rules. For example, when a user clicks the reference link for Part 100 version A.1, Windchill searches for the latest released version of Doc 100 to display. If no version of the document has been released, it displays the latest working version (in this case, Doc 100 version A.2).

How to configure the life cycle state rules is described later in this section.

- A **Part Describe Link** (WTPartDescribeLink)—Using this type of link links the part to the latest iteration of a document and vice versa.



For example, when the user clicks a describe link for Part 100 version A.2, Windchill searches for the latest iteration of Doc 100 to display (in this case, Doc 100 version A.2).



You can create part to document relationships in the following ways:

- From the **Related Objects** tab on the part information page, the user creates the link using the actions from the **References Documents** or **Described By Documents** tables.
- From the **Related Objects** tab on the document information page, the user creates the link using the actions from the **Describes Parts** or **Referenced By Parts** tables.
- From the **Structure** tab on the part information page, the user creates the link using the **Add Related Information** ► **Add Described By Document** or **Add Related Information** ► **Add References Document** actions from the right-click action menu for a part.

Relationship constraints can be created for the **Part Reference Link** and **Part Describe Link** types, to specify which document types can be related to which part types for those relationships. Once relationship constraints have been created, only documents of the types specified in the relationship constraint appear when adding an existing document or creating a new document and adding it to a part as a described by or references document. For more information, see “Relationship Constraints Tab” in the PTC Windchill Help Center.

#### **Note**

Special link types, known as configurable links, can be used to configure and display additional relationship tables on document and part information pages. For information, see “Using Configurable Links” in the PTC Windchill Help Center.

To allow the user to select the link type regardless of the document subtype, set the **Part to Document Association Logic** preference to Yes from the **Preference Management** utility on **Site**  ► **Utilities** or **Organizations**  ► **Utilities**. You might create relationship constraints in the **Type and Attribute Management** utility that do not carry forward to the end-user user interface until you modify this preference.

---

For more information on using the **Preference Management** utility, see the help available from the **Preference Management** utility.

---

 **Note**

In addition, setting this preference allows you to associate more than one version of a described by document to a part. For reference documents, the part is associated to the document master.

---

Additional configuration options are described in the following sections.

## Revised or Saved Part to Related Document

When a user revises a part using the **Revise** action or saves the part using the **Save As** action, the new version of the part carries forward the link to the document by default. While the **Revise** action always carries the link forward, you can choose to prevent the link from being carried forward during a **Save As** action by removing the Relationship copy rules related to this operation from wt.properties.

For example, assume the following properties are set in wt.properties:

```
wt.enterprise.copyRuleDelimiter=,  
  
wt.enterprise.copyRulesN=wt.part.WTPart,Relationship,  
wt.part.WTPartReferenceLink-references
```

The first property sets the delimiter for the copy rules to the comma (,).

The wt.enterprise.copyRulesN property is the Relationship copy rule for wt.part.WTPart. This rule copies the references forward when the type of link is WTPartReferenceLink.

If you remove the wt.enterprise.copyRulesN property, then reference links are not carried forward.

---

 **Note**

As a best practice, there should be no gaps in the sequence of copy rules. If you remove a copy rule, renumber those rules that follow. For example if there are six copy rules and you remove copyRules5, then you should renumber copyRules6 so that it is copyRules5.

Duplicate numbers should never be used in the copy rules sequence.

---

---

Use the `xconfmanager` utility when modifying the `wt.properties` file. For more information on using this utility, see the *PTC Windchill Specialized Administration Guide*. For more information about the properties used for copy rules, see the description of `wt.enterprise.copyRules` in the `properties.html` file.

---

 **Caution**

PTC recommends that you do not change the value of the `wt.enterprise.copyServiceRules` property. The property is used by internal services.

---

## Document Version Used with Reference Link

As described earlier, **Part Reference Link** links (`WTPartReferenceLink`) link to a document master, but display a document version of the master based on the life cycle state rules for the document.

The default behavior is that Windchill searches for the latest released version of the document to display. If no version of the document has been released, it displays the latest working version of the document.

To change the default behavior, change the value set for the **List of comma separated life cycle states of documents used to display associated Reference documents to part.** in the **Preference Management** utility.

---

 **Note**

The states must be valid life cycle states. The states are defined as key value pairs in `StateRb.rbinfo` and can be viewed in the life cycle template associated with the object. States are always specified using uppercase characters.

---

For example, to change the search to include the Released, Approved, and then Completed states of a document, set the preference value to:

```
RELEASED, APPROVED, COMPLETED
```

After this preference is set, Windchill searches for the latest Released version first. If none is found, it searches for the latest Approved version. If none is found, it searches for the latest Completed version. So, if a part is linked to Reference Document 4 which has three versions (A, B, and C), where A = Released, B = Approved, and C = In Work, based on the state settings in `wt.properties`, Windchill displays the latest iteration of version A which was released and ignores the rest.

---

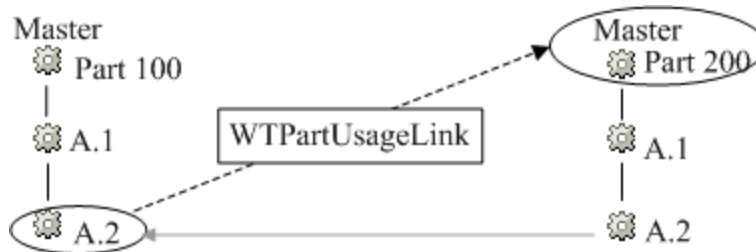
## Part to Part Relationships

### Note

Part to part relationships are available only in Windchill PDMLink, and do not apply to Arbortext Content Manager or Pro/INTRALINK 10.1.

---

A user associates one part with another by using the **Structure** tab on a part information page. When a user makes the association, a **Part Usage** link (WTPartUsageLink) is created, forming a "uses part" relationship between a part and a part master.



The only configuration option for part to part relationships is described in the next section.

### Revised or Saved Parent Part to Child Part

When a user revises a parent part using the **Revise** action or saves the part using the **Save As** action, the new version of the part carries forward the usage link.

To prevent a link from being copied forward on a **Revise** or **Save As** action, you must remove copy rules from wt.properties. For example, assume the following properties are set in wt.properties:

```
wt.enterprise.copyRuleDelimiter=,

wt.enterprise.copyRulesN=wt.part.WTPart,Relationship,
wt.part.WTPartUsageLink-uses
```

The first property sets the delimiter for the copy rules to the comma (,).

The wt.enterprise.copyRulesN property is the Relationship copy rule for wt.part.WTPart. This rule copies the references forward when the type of link is WTPartUsageLink.

If you remove the wt.enterprise.copyRulesN property, then the usage links are not carried forward.

---

### **Note**

There can be no gaps in the sequence of copy rules. If you remove a copy rule, you must renumber those rules that follow. For example, if there are six copy rules and you remove `copyRules4`, then you must renumber `copyRules5` and `copyRules6` so that `copyRules5` becomes `copyRules4` and `copyRules6` becomes `copyRules5`.

---

Use the `xconfmanager` utility when modifying the `wt.properties` file. For more information on using this utility, see the *PTC Windchill Specialized Administration Guide*. For more information about the properties used for copy rules, see the description of `wt.enterprise.copyRules` in the `properties.html` file.

---

### **Caution**

PTC recommends that you do not change the value of the `wt.enterprise.copyServiceRules` property. The property is used by internal services.

## Document to Document Relationships

There are several different types of document to document relationships in your Windchill solution:

- A document can reference another document from the **Related Objects** tab on the document information page. This relationship creates a link of type `WTDocumentDependencyLink`.
- A document can serve as the parent to a second child document from the **Structure** tab on the document information page. This relationship creates a link of type **Document Usage** (`WTDocumentUsageLink`).

There are no configuration options available for document to document relationships.

## Best Practices for Object Initialization Rules

Although you can set object initialization rules for individual product and library contexts, consider the consequences of doing this.

For most sites, the recommended approach is to set the rules at either the organization or site level so that an entire organization or site is using the same set of rules.

---

If you choose to set different rules in a product or library context, be aware that the ability to move objects between contexts may be restricted. Specifically, if you create a life cycle template in a specific product or library and the template is not available in other products or libraries, then you cannot move any object that uses the life cycle template. The same is true if the team template is unique to a product or library; objects using the team template cannot be moved. Similarly, the versioning scheme used for an object must match the scheme set in the destination product or library or the object cannot be moved.

---

 **Note**

For demonstration purposes, the Product Design template (available by default when you create a product) includes object initialization rules that sets different default life cycle templates and versioning schemes for parts, documents, and CAD documents than is set out-of-the-box at the site level. This template demonstrates the used of simplified life cycles and state-based versioning. Unless you have overriding business practices that require unique rules, PTC recommends that if you want to use these features, you modify the organization or site object initialization rules and remove them from the Product Design template.

---



# 8

## Understanding Projects and Programs

Project and Program Administration Overview .....	234
Typical Duties of Project and Program Managers .....	235
Out-of-the-box Project and Program Templates .....	241
Configuring Part and Document Relationships .....	244

This section provides an overview for administering projects and programs and describes the typical duties that an administrator performs. It also provides additional information about some of the main administrative tasks for projects and programs.

For more information, see the Project and Program Administration help topics.

---

# Project and Program Administration Overview

Project and program managers (also known as project and program administrators) are responsible for creating and managing projects and programs hosted by a parent organization. The capabilities of project and program managers are nearly identical.


Project and program managers control the project and program configuration, and control the membership in their project and program teams within the confines of a specific project or program application context. They control access to project and program information; they define the schedule, resources, and plan details, and monitor and manage the project and program activities.

Project application contexts are online work areas used to collect information that teams need to track, collaborate, and manage as well as plan work activities to meet a specific objective. Project contexts are defined by project creators who are authorized by the parent organization. Projects inherit templates, roles, user-defined groups, and policies from their parent organization context. The project manager can also define project-specific templates, roles, and policies.

Program application contexts provide a central area to link together information, people, and plans for a series of projects. Program contexts are defined by program creators who are authorized by the parent organization. Programs inherit templates, roles, user-defined groups, and policies from their parent organization context. The program manager can also define program-specific templates, roles, and policies.

---

## Note

By default, programs are hidden. To make programs visible and available for use in your Windchill solution, a site administrator can set the value of the **Display ► Hide Program** preference to “No”. This preference is available from the **Preference Management** utility on **Site**  ► **Utilities**. For more information on using the **Preference Management** utility, see help available from the **Preference Management** utility.

---

For general information about context contents and how to create contexts, see [Contexts – Distributed and Hierarchical Administration on page 59](#).

---

## Typical Duties of Project and Program Managers

Project and program managers are responsible for creating and managing the content of projects and programs. The capabilities of project and program managers are nearly identical. Your typical duties include the following:

- Creating and editing the project or program
- Overriding user profiles
- Managing team members and roles
- Creating, editing, and managing documents and folders
- Creating, editing, and managing activities, deliverables, resources, and action items
- Limiting edit privileges for all action items
- Managing document templates
- Managing preferences
- Importing and exporting information
- Undoing a user checkout
- Viewing and managing access control rules for objects
- Managing utilities

The following sections describe some of the duties in more detail.

### Creating and Editing Projects and Programs

When you create a project or program, you can choose the project or program template on which the project or program is based, define the key project or program attributes, define the project or program properties and select the configuration options. You can also update the project or program attributes as work progresses. These attributes include the project or program description, scope, project or program number, and so forth.

Only members of the project creators group and the organization administrator in an organization are allowed to create projects. By default, organizations allow all members to create projects, but the organization or site administrator may update an organization restricting project creation privileges to identified creators.

Only members of the program creators group and the organization administrator in an organization are allowed to create programs. By default, only the organization administrator can create programs. The organization administrator must manually add users to the program creators group to allow users to create programs.

For information about creating projects and programs, see the help available from the **New Project** or **New Program** windows.

---

## Note

If you use a shared team that is not extended locally when creating a program or project, and you are not a member of the shared team, you may not have access to the program or project that is created.

---

## Managing Team Members and Roles

Project and program managers can add members and team roles to a local team, as well as override profiles.

If the team includes a shared team, the shared team is managed from the organization context, and not the project or program context.

For more information about local and shared teams, see [Teams and Team Template Administration on page 297](#).

For more information about profiles, see [Profile Management on page 291](#).

## Controlling the Visibility of Actions

As the project or program manager, you can control visibility to information and actions within the project or program based on the roles in the project or program local team.

For more information, see the teams help.

## Establishing Roles

Each project team contains two fixed roles that cannot be removed: Project Manager and Guest. Each program team contains two fixed roles that cannot be removed: Program Manager and Guest. Additionally, you can select team roles from the list of roles inherited from the parent organization, or you can create new roles.

The Guest role is designed to include user-defined groups and users that are not active team members and need only read access to project or program information. It is possible to hide the Guest role for projects and programs. For more information, see the teams help.

The creator of the project or program is automatically established as both a project or program manager and as the project or program owner. The project or program manager can change the owner and can add members to the project or program managers role. All members of the project or program managers role have the same privileges.

---

You can invite groups to the project or program roles from the user-defined groups defined in the parent organization.

## Overriding Profiles

As the project or program manager, you can override profile settings that are established at the site and organization contexts. For more information about profiles, see [Profile Management on page 291](#).

The site or organization administrator determines whether the various user interface elements and actions are configurable from an application context. You can override an action or user interface element in a context instance using Configure Actions for Roles which is accessed from the Team page. For more information, see the teams help.

## Moving Objects

Moving objects to a new folder requires different permissions depending on the move being performed.

For more information on the permissions required to move an object, see the *PTC Windchill Specialized Administration Guide*.

## Creating, Editing, and Managing Documents and Folders

You can create documents for the project or program, and you can define a folder structure. By default, any member of the project or program can define folders and subfolders in the folder structure.

If you are using the out-of-the-box project and program templates, you have full control over all documents created in the project or program; no member can prevent you from reading, editing, or deleting any object. You can also modify the access rules on any folder or any document.

You can delete discussion topics and postings. Non-project or program managers can only post to discussion topics; they cannot delete postings or topics, even if they created them.

## Creating, Editing, and Managing Activities, Deliverables, Resources, and Action Items

You alone can create activities, mark activities as milestones, deliverables, and resources in the project or program. The owner of an activity, milestone, or deliverable can edit and complete the item, but only project or program managers can create plan items.

---

## Managing Routing

While routing an object to a group, you have the option of displaying the group as a whole or exploding a group into individual members. By exploding a group into members, you can decide if you want the entire group to be participants in a particular role. For example, if only a select number of users within the group need to be approvers, the other users within the group can be deleted from the role. The exploding of groups into members is defined in the following property in the wt.properties file:



```
com.ptc.netmarkets.workflow.routeExplodeGroups
```

The default value for this property is FALSE. To enable the exploding of groups into members, set the property to TRUE using the xconfmanager. For more information, see the *PTC Windchill Specialized Administration Guide*.

## Limiting Edit Privileges for All Action Items

You can limit the edit privileges on all action items, preventing the action item assignee from updating the following fields:

- Name
- Description
- Assignee
- Due Date
- Priority

To limit the edit privileges for all action items, a site or organization administrator can set the **Create and Edit ► Restrict Action Item Updates** preference to **Yes** using the **Preference Management** utility from either the **Site**  ► **Utilities** page or the **Organizations**  ► **Utilities** page for your organization. Assignees will not be allowed to update the fields listed above for any action items.

## Managing Templates

You control the document templates available to a project or program. You can:



- Add to the list of document templates inherited from the parent organization or the site, by creating a new document template within your project or program.
- Override the inherited template by creating a project- or program-specific template of the same name.
- Disable a document template that was created within the context of the project or program.
- Choose to hide or show inherited document templates for use in your project or program.

---

Document templates that are enabled and shown are available to users when creating a new document from a template on the project or program **Folders** page; document templates that are hidden or disabled are not available.

For more information, see the help available from the **Templates** table.

## Managing Preferences

Using the **Preference Management** utility from the **Projects**  ► **Utilities** or **Programs**  ► **Utilities** page, you can manage preferences at the project or program level. Preferences set at the project or program level affect the project or program for which they are set. Different preferences can be set for different projects or programs.

For example, a number of preferences are available which allow you to determine the types of content allowed for documents. These preferences are found in the **Attachments** category of the **Preference Management** utility.

For more information, see the help available from the **Preference Management** utility.

## Importing and Exporting Information

You can export information from one project and import it into another project, or export information from one program and import it into another program on the same system or a different Windchill system. Generally, you can only import into a system at the same or higher release version as the system from which the data was exported. You can export project or program information as a template. A site or organization administrator can then create a template from that information that can be reused by the organization.

You can also save an existing project or program as a new project or program as a means of quickly starting a similar project or program.

You can also import a Microsoft Project plan into the system and export project and program information from Windchill into the Microsoft Project format.

---

### **Note**

By default, milestones that have resources assigned in Microsoft Project are converted to activities in Windchill ProjectLink. To change this behavior so that milestones that have resources assigned in Microsoft Project are converted to milestones in Windchill ProjectLink and the resources are dropped, set the following property to TRUE in the wt.properties file:

```
wt.projmgmt.msproject.dropMilestoneResource
```

---

---

## Undoing a User Checkout

If a user in your project or program has an object checked out, you can undo the checkout, reverting to the last modified iteration of the object. This is useful in situations where the user who had the object checked out has left the company, or if they are out of the office when the checked out object is needed.

If you know the object or objects for which you want to undo the checkout, you can perform the undo checkout action on an object from either the **Folders** page of your project or program, or from the information page for the checked out object.

## Viewing and Managing Access Policies

You can view and manage the access control rules for objects (such as folders, and documents) in your project or program. Navigate to the object, and select the **Edit Access Control** action, depending on your configuration. Using this action you can view and set the access control to the object for roles within your project or program team.



For more information, see the “About Security Management” topic in the PTC Windchill Help Center.


You can define policies that control the level of access to information in a program or project. When defining a policy, the object types and user-defined groups defined in the parent organization can be used as well as the system groups representing the team roles in a program or project. For example, you could create a policy that provides Write access to all documents of type “Agenda” to the project team role/group called “Scheduler”.

For more information about domains and policies, see [Administering Domains and Policies on page 86](#).

For more information about creating or updating access control rule policies, see the *PTC Windchill Specialized Administration Guide*.

## Managing Utilities

A number of administrative utilities are available through **Projects**  **Utilities** and **Programs**  **Utilities**.

By default, only site and organization administrators can access **Projects**  **Utilities** and must act on behalf of the project manager. Access is restricted by default because these utilities are complex and require a level of training that is not expected for typical project managers. The site or organization administrator can set the **Display** **Project Utilities Page** preference to grant all project managers access to the project utilities functions.

For more information, see the help available from the **Utilities** page.



# Out-of-the-box Project and Program Templates

When Windchill ProjectLink is installed, the following templates are loaded:

Template Name	Description
General	Sample templates that can be used to create a general project or program.
Design	A sample template that can be used to create a design project.
Manufacturing	A sample template that can be used to create a manufacturing project.
Custom	A sample template that can be used to create a custom project.

The project and program templates can define the same basic information that is discussed in [Context Administrative Items on page 61](#). However, the out-of-the-box templates define only the following:

- Context structure
- Context environment
- Context participation

The following tables describe the items that are defined in the templates.

## Note

Project and program plan definition information is included in each template.

Context Structure				
	General	Design	Manufacturing	Custom
Folder structure	General	Analysis Contracts Designs General Plans Prototypes Specifications Standards	Analysis Contracts Designs General Plans Specifications	Changes Contracts Designs General Installation Plans Prototypes Specifications

<b>Context Environment</b>				
	<b>General</b>	<b>Design</b>	<b>Manufacturing</b>	<b>Custom</b>
Discussion topics	General	Analysis Design General Manufacturing Specifications	Design General Manufacturing Quality Specifications	Changes Contract Design General Manufacturing Quality Specifications
Notebook template	Documents General Links Parts	Documents General Links Parts	Documents General Links Parts	Documents General Links Parts

<b>Context Participation</b>				
	<b>General</b>	<b>Design</b>	<b>Manufacturing</b>	<b>Custom</b>
Project or program team roles	Guest Members Project or Program Manager Collaboration Manager	Consultant Designer Guest Manufacturer Members Project Manager Collaboration Manager	Engineer Guest Manufacturer Members Production Planner Project Manager Purchasing Agent Quality Engineer Supplier Collaboration Manager	Customer Engineer Guest Members Project Manager Quality Engineer Supplier Collaboration Manager

<b>Template Plan Objects</b>				
	<b>General</b>	<b>Design</b>	<b>Manufacturing</b>	<b>Custom</b>
Milestones	Project or Program Start Project or Program Finish	Project Start Contract Signed Specifications Approved Design Approved Prototype Approved Design Released Project Finish	Project Start Contract Signed Specifications Approved Design Approved Testing Complete Prototype Approved Production Part Approved Production Initiated Project Finish	Project Start Contract Signed Specifications Approved Design Approved Testing Complete Prototype Approved Production Part Approved Production Initiated Project Finish
Deliverables	Project or Program Start Project or Program Finish Scope Post Mortem	Project Start Contract Signed Specifications Approved Design Approved Prototype Approved Design Released Project Finish Scope Contract Specification DraftDesign Prototype Final Design Post Mortem	Project Start Contract Signed Specifications Approved Design Approved Testing Complete Prototype Approved Production Part Approved Production Initiated Project Finished Scope Contract Specification Draft Design	Project Start Contract Signed Specifications Approved Design Approved Testing Complete Prototype Approved Production Part Approved Production Initiated Project Finish Scope Contract Specification Draft Design

---

# Configuring Part and Document Relationships

The relationships between a part and a document, two parts, or two documents vary depending upon how the two objects are linked. This section briefly describes the different types of links that form these relationships and then describes the configuration options that are available.

## Part to Document Relationships

---

### Note

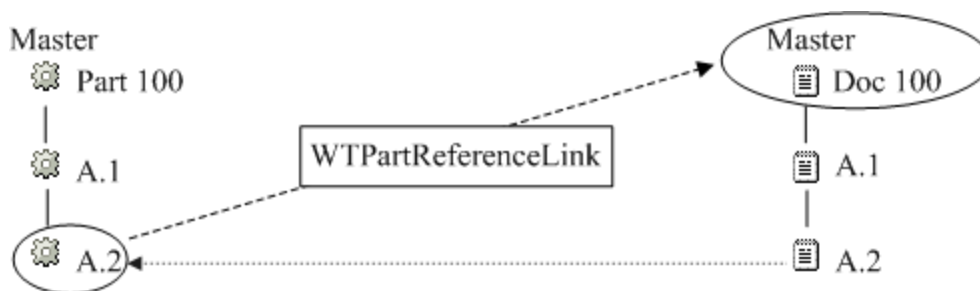
Part to document relationships apply to projects only; parts are not used within programs.

---

The association between a part and a document is created from the part information page or document information page. Associations can be viewed from the **Related Objects** tab on the part information page. These same relationships can be viewed from the **Related Objects** tab of the document information page.

There are two types of links that can be established:

- A **Part Reference Link** (WTPartReferenceLink)—Using this type of link always links the part to the master document. Regardless of the version of the document the user selects, the part will always link to the master document when this link type is used. This is true even when the system has been configured to allow the user to select the link type and the document type.



Reference links always display a document version of the master based on life cycle state rules. For example, when a user clicks the reference link for Part 100 version A.1, Windchill searches for the latest released version of Doc 100 to display. If no version of the document has been released, it displays the latest working version (in this case, Doc 100 version A.2).

---

How to configure the life cycle state rules is described later in this section.

- A **Part Describe Link** (WTPartDescribeLink)—Using this type of link links the part to the latest iteration of a document and vice versa.



For example, when the user clicks a describe link for Part 100 version A.2, Windchill searches for the latest iteration of Doc 100 to display (in this case, Doc 100 version A.2).

You can create part to document relationships in the following ways:

- From the **Related Objects** tab on the part information page, the user creates the link using the actions from the **References Documents** or **Described By Documents** tables.
- From the **Related Objects** tab on the document information page, the user creates the link using the actions from the **Describes Parts** or **Referenced By Parts** tables.
- From the **Structure** tab on the part information page, the user creates the link using the **Add Related Information** ► **Add Described By Document** or **Add Related Information** ► **Add References Document** actions from the right-click action menu for a part.

Relationship constraints can be created for the **Part Reference Link** and **Part Describe Link** types, to specify which document types can be related to which part types for those relationships. Once relationship constraints have been created, only documents of the types specified in the relationship constraint appear when adding an existing document or creating a new document and adding it to a part as a described by or references document. For more information, see “Relationship Constraints Tab” in the PTC Windchill Help Center.



---

#### **Note**

Special link types, known as configurable links, can be used to configure and display additional relationship tables on document and part information pages. For information, see “Using Configurable Links” in the PTC Windchill Help Center.

---

---

To allow the user to select the link type regardless of the document subtype, set the **Part to Document Association Logic** preference to Yes from the **Preference Management** utility on **Site**  **Utilities** or **Organizations**  **Utilities**. You might create relationship constraints in the **Type and Attribute Management** utility that do not carry forward to the end-user user interface until you modify this preference.

For more information on using the **Preference Management** utility, see the help available from the **Preference Management** utility.

Additional configuration options are described in the following sections.

## Revised or Saved Part to Related Document

When a user revises a part using the **Revise** action or saves the part using the **Save As** action, the new version of the part carries forward the link to the document by default. While the **Revise** action always carries the link forward, you can choose to prevent the link from being carried forward during a **Save As** action by removing the Relationship copy rules related to this operation from wt.properties.

For example, assume the following properties are set in wt.properties:

```
wt.enterprise.copyRuleDelimiter=,  
  
wt.enterprise.copyRulesN=wt.part.WTPart,Relationship,  
wt.part.WTPartReferenceLink-references
```

The first property sets the delimiter for the copy rules to the comma (,).

The wt.enterprise.copyRulesN property is the Relationship copy rule for wt.part.WTPart. This rule copies the references forward when the type of link is WTPartReferenceLink.

If you remove the wt.enterprise.copyRulesN property, then reference links are not carried forward.

---

### Note

As a best practice, there should be no gaps in the sequence of copy rules. If you remove a copy rule, renumber those rules that follow. For example if there are six copy rules and you remove copyRules5, then you should renumber copyRules6 so that it is copyRules5.

Duplicate numbers should never be used in the copy rules sequence.

---

Use the xconfmanager utility when modifying the wt.properties file. For more information on using this utility, see the *PTC Windchill Specialized Administration Guide*. For more information about the properties used for copy rules, see the description of wt.enterprise.copyRules in the properties.html file.

---

### **Caution**

PTC recommends that you do not change the value of the `wt.enterprise.copyServiceRules` property. The property is used by internal services.

---

## Document Version Used with Reference Link

As described earlier, **Part Reference Link** links (`WTPartReferenceLink`) link to a document master, but display a document version of the master based on the life cycle state rules for the document.

The default behavior is that Windchill searches for the latest released version of the document to display. If no version of the document has been released, it displays the latest working version of the document.

To change the default behavior, change the value set for the **List of comma separated life cycle states of documents used to display associated Reference documents to part.** preference in the **Preference Management** utility.

---

### **Note**

The states must be valid life cycle states. The states are defined as key value pairs in `StateRb.rbinfo` and can be viewed in the life cycle template associated with the object. States are always specified using uppercase characters.

---

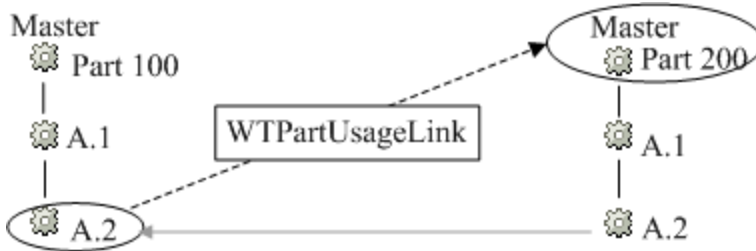
For example, to change the search to include the Released, Approved, and then Completed states of a document, set the preference value to:

```
RELEASED, APPROVED, COMPLETED
```

After this preference is set, Windchill searches for the latest Released version first. If none is found, it searches for the latest Approved version. If none is found, it searches for the latest Completed version. So, if a part is linked to Reference Document 4 which has three versions (A, B, and C), where A = Released, B = Approved, and C = In Work, based on the state settings in `wt.properties`, Windchill displays the latest iteration of version A which was released and ignores the rest.

## Part to Part Relationships (Projects Only)

A user associates one part with another by using the **Structure** tab on a part information page. When a user makes the association, a **Part Usage** link (`WTPartUsageLink`) is created, forming a "uses part" relationship between a part and a part master.



The only configuration option for part to part relationships is described in the next section.

## Revised or Saved Parent Part to Child Part

When a user revises a parent part using the **Revise** action or saves the part using the **Save As** action, the new version of the part carries forward the usage link.

To prevent a link from being copied forward on a **Revise** or **Save As** action, you must remove copy rules from wt.properties. For example, assume the following properties are set in wt.properties:

```
wt.enterprise.copyRuleDelimiter=,

wt.enterprise.copyRulesN=wt.part.WTPart,Relationship,
wt.part.WTPartUsageLink-uses
```

The first property sets the delimiter for the copy rules to the comma (,).

The wt.enterprise.copyRulesN property is the Relationship copy rule for wt.part.WTPart. This rule copies the references forward when the type of link is WTPartUsageLink.

If you remove the wt.enterprise.copyRulesN property, then the usage links are not carried forward.

### Note

There can be no gaps in the sequence of copy rules. If you remove a copy rule, you must renumber those rules that follow. For example if there are six copy rules and you remove copyRules4, then you must renumber copyRules5 and copyRules6 so that copyRules5 becomes copyRules4 and copyRules6 becomes copyRules5.

Use the xconfmanager utility when modifying the wt.properties file. For more information on using this utility, see the *PTC Windchill Specialized Administration Guide*. For more information about the properties used for copy rules, see the description of wt.enterprise.copyRules in the properties.html file.



---

 **Caution**

PTC recommends that you do not change the value of the wt.enterprise.copyServiceRules property. The property is used by internal services.

---

## Document to Document Relationships

There are multiple types of document to document relationships in Windchill ProjectLink:

- A document can reference another document from the **Related Objects** tab on the document information page. This relationship creates a link of type WTDocumentDependencyLink.
- A document can serve as the parent to a second child document from the **Structure** tab on the document information page. This relationship creates a link of type **Document Usage** link (WTDocumentUsageLink).

There are no configuration options available for document to document relationships.



# 9

## Understanding Participants (Users, Groups, and Organizations)

Overview of Windchill Participants .....	252
Working with LDAP Directory Services .....	255
Using the Participant Administration Utility .....	265
Windchill Participant Status .....	282
Participant (Users, Groups, and Organizations) Identification .....	285
Best Practices for Assigning Domains to Participants .....	285
Receiving Administrative Notifications .....	287
Managing the Participant Cache .....	287
Maintaining the Connections between Participant Objects and their Directory Server Entries .....	289
Registering a non-Windchill User .....	290
Profile Management .....	291

This section describes the LDAP nodes, participants (user, group, and organization objects) that are used in your Windchill solution, and details about managing the participants. It also provides information about profile management for dynamic control of visibility to actions.

For more information, access help available in the **Participant Administration** utility.

---

## Overview of Windchill Participants

Windchill uses the term participant to mean a user, group, or an organization; it includes any combination of users, groups, or organizations.

As the Windchill system administrator for any Windchill solution, you can create and update Windchill user, group, and organization objects through the **Participant Administration** utility. As an Organization Administrator, you can update the Windchill user, group, and organization objects that are in your organization context.

---

### Note

When a Windchill solution is installed, the system administrative user (Administrator), the system administrative group (Administrators), and the initial organization object are always created. By default, the user Administrator (for example, wadmin) belongs to the Administrators group. This user does not have an organization affiliation (as defined by the LDAP organization attribute, which is "o" by default).

---

Windchill uses both the Windchill database and a directory service when creating participants. For each participant, there is an entry in a directory service and a Windchill object stored in the database:

- The directory service entry contains attributes specific to the type of participant. For example, user entries have attributes for the user's full name, email address, and organization.

The Windchill Directory Server is set up when your Windchill solution is installed. Other directory services can be established by setting up JNDI adapter entries through the Info\*Engine Property Administrator and adding the adapter entries to the wt.federation.org.directoryServices property value.

For additional information, see the *PTC Windchill Installation and Configuration Guide*.

- The Windchill object contains information that is relevant to Windchill (such as the associated domain) and the Unique Federation Identifier (UFID) associated with participant.

The UFID contains the distinguished name of the participant and identifies the directory service where the participant entry resides.

---

 **Note**

If the LDAP directory server is read-only, edit and create actions are not available for participants and Windchill uses existing LDAP entries as participants.

---

The following sections provide additional details about Windchill participants.

## Windchill Users

A Windchill user object identifies a user and is used when establishing group membership and policy rules for that user. It is stored in the Windchill database and holds user information for those users who have access to Windchill. This information includes the user name, the UFID associated with the user, the Windchill domain of the user, and administrative flags that are set if the object needs to be repaired or is disabled.

A Windchill user object is automatically created and persisted in the Windchill database the first time the user is selected from a search or the first time the user logs on to Windchill. In both of these cases, the corresponding directory service entry for the user already exists and is then referenced in the object that is created. As an administrator, you can also create, update, and delete users through the Participant Administration utility.

Windchill does not rely on the user object to authenticate users. Rather, the web server authenticates users and passes the authenticated user name to Windchill. The user's web server ID is then mapped directly to the user object that has a matching user name.

Windchill users are usually affiliated with an organization that is set through the directory service organization attribute (by default, "o"). If the organization attribute is not set, then the user is an unaffiliated user and cannot create products, libraries, projects, or programs. However, that user can be invited to a team by email or by selecting the **Restricted Directory Search** checkbox when creating or editing the organization. Users that have been invited to the team through one of these methods can do the same things within the product, library, project, or program as any other member.

---

 **Note**

If your site does not use the organization attribute in the directory service entry, users can be assigned to an organization by specifying the `usersOrganizationName` property in a JNDI adapter. For more information on using this property, see the *PTC Windchill Installation and Configuration Guide*.

---

## Windchill Groups

Windchill has two types of groups:

- User-defined groups are those groups created and managed by the users of a Windchill solution. These groups can be created through the Participant Administration utility or can be created through a third party LDAP tool and have a corresponding UFID that is maintained in an LDAP database.
- System groups are created and managed internally by the system and do not have a corresponding UFID. Windchill uses system groups for managing context team membership and other system activities.

Additionally, dynamic roles represent the system groups that are used in managing context team membership. Dynamic roles can be participants in access control policy rules. For additional information, see the *PTC Windchill Specialized Administration Guide*.

Organizing users into user-defined groups provides you with a more efficient way to apply policies for access control and event notification, to populate participants in team and life cycle roles, and to populate recipients of workflow tasks. Each user-defined group object identifies selected users, organizations, and possibly other groups, under one name. You can create user-defined groups so that you can efficiently apply administrative tasks to groups of users, rather than to each user individually.

User-defined groups are associated with the context in which they are created. Some Windchill solutions also create and manage system groups that are used to manage team role membership. These groups are not accessible from the Participant Administration utility. For more information on accessing groups from the Participant Administration utility, see [Using the Participant Administration Utility on page 265](#).

A Windchill user-defined group object holds the group name, the UFID associated with the group, the Windchill domain of the group, and administrative flags that are set if the object needs to be repaired or is disabled. The UFID contains the distinguished name of the user-defined group and identifies the directory service where user-defined group entry resides.

---

## Windchill Organizations

Categorizing users by organization provides an additional way in which you can identify a set of participants by name. Windchill manages Windchill objects within each organization context and users affiliated with an organization can be given access to objects created from within an organization context.

An organization can be a company, company division, university, or some other list of people. Organization membership is defined by user directory entries that include the organization name defined for the organization object. For example, if the organization name is DIV1, then all users in the configured directory services who have their organization attribute (o, by default) set to DIV1 are members of the DIV1 organization.

Organization participants are associated with the context in which they are created. From the Participant Administration utility, you only have access to the organization participants created in the current context or in the site context. Organization participants are used to define organization identifiers (such as CAGE codes or DUNS numbers), context ownership, and suppliers for supplier management activities.

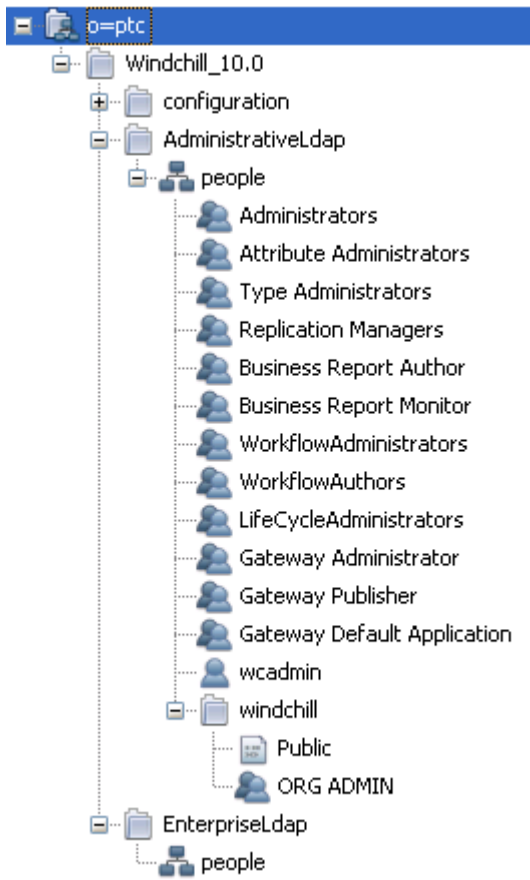
Each Windchill organization participant holds the organization name, the UFID associated with the organization, the Windchill domain of the organization, and administrative flags that are set if the participant needs to be repaired or is disabled. The UFID also contains the distinguished name of the organization and identifies the directory service where the organization entry resides.

## Working with LDAP Directory Services

When your Windchill solution was installed, two LDAP directory services were configured:

- **Administrative LDAP** – This LDAP is intended to be used for your administrative users and any user-defined groups that you want to have administrative access. The display name for this service uses the reverse of the site domain and ends in .Ldap.
- **Enterprise LDAP** – This LDAP is intended to contain your end users and any user-defined groups that you do not want to have administrative access. The display name for this service uses the reverse of the site domain and ends in .EnterpriseLdap.

For example, if your site has a domain of ptcnet.ptc.com, if you supplied "windchill" as your organization name during installation, and if you accepted the default LDAP directory service options during installation, your directory service structure is similar to the following.



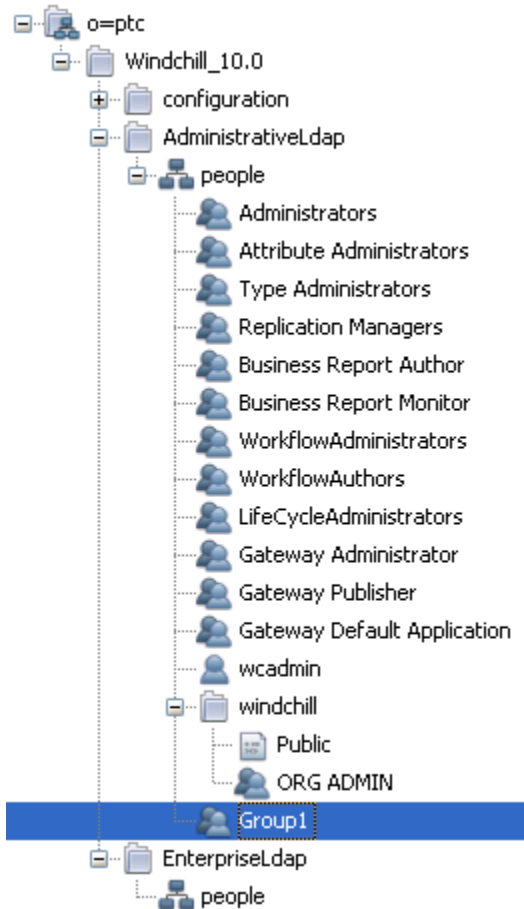
The Administrative LDAP includes the system-defined administrative groups.

When you create a new group using the Participant Administration utility, you can select which LDAP it is created under by selecting the desired directory service as shown below:

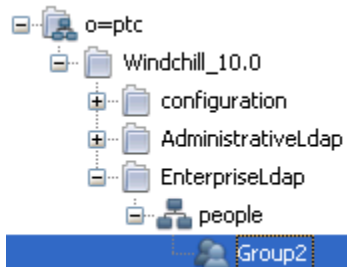




For example, if you use the Participant Administration utility to create a new group from the site context, and you choose the Administrative LDAP as the **Directory Service**, the group is added as shown below:

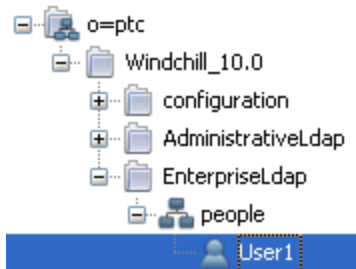


If you use the Administrator to create a new group from the site context and select the Enterprise LDAP, the group is added as shown below:

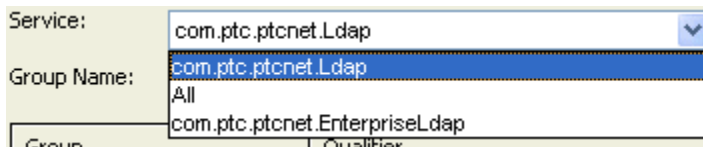


---

If you use the Participant Administration utility to create a new user and select the Enterprise LDAP, the user is added as shown below:



When creating an access control rule for a group using the **Policy Administration** utility, select the directory in which the group resides to find the group, as shown below:



For more information on the **Policy Administration** utility, see [Using the Policy Administration utility on page 93](#).

By default, the Windchill search for groups uses a one level search scope in the selected directory service. This means that for Windchill to find the groups, you must store them at the top level established in the service. The Participant Administration utility automatically does this.

If you add groups through a third party tool and the following things are true:

- You do not store the groups in the default search base associated with the service
- You do not want to create a new directory service to map to this additional search base

then you must add the search base to the **Additional search bases which need to be queried** preference so the search base is included when Windchill searches for groups.

Change the preference value using the site-level Preference Management utility.

For more information on the Preference Management utility, see the help available from the utility.

---

#### **Note**

If your site requires changes in your established directory service structure, you should contact PTC Technical Support for assistance.

---

---

## Searching for Participants in Administrative Clients

The following administrative clients use a common interface when searching for participants (users, groups, and organizations):

- **Policy Administration** – When working with policy rules, you select participants against which the rules are applied.
- **Life Cycle Template Administration** – When defining an advanced life cycle template, you can select participants as constituents for any of the roles defined for that life cycle template.
- **Team Administration** – When defining team in a team template, you can select participants as constituents for roles.
- **Workflow Template Administration** – When defining activities, you can select participants to complete each assigned activity.

In these administrative clients, the ability to locate users, groups, and organizations is determined by the administrator's access permissions and by the search scope used within each of the services searched. The administrator who is performing the search must have Read permission for participants to appear in the search result.


The service's default search scope is used to locate users and organizations (that is, the search scope configured in the service's JNDI adapter).


In the administrative clients, user-defined groups can be displayed. The search scope of the selected directory service determines which groups are displayed. For more information, see [Working with LDAP Directory Services on page 255](#).

The methods used to display users, groups, or organizations within a participant search window are determined by setting participant search properties. Properties narrow the search and return participants with specific characteristics in the search results. By setting the following property values in the `wt.properties` file, you can change the behavior of the interface so that when the participants search window appears, it is automatically populated with all groups or organizations that are available.


For information about add, remove, and modify the properties in the Windchill property files, see the *PTC Windchill Specialized Administration Guide*.

Search properties include:

Property Name	Properties.html	Search Property Function	Description
Max Count	com.ptc.net markets. userSearch. maxCount	Defines the maximum results count	<p>Controls how many results are returned from the search. The default is set to 50, limiting results to 50 returned participants.</p> <p> <b>Note</b></p> <p>If you have a large number of groups or organizations, then automatically populating the participants window with them may take a long period of time. PTC recommends that you use the default setting for the Max Count property unless you have a small number of groups and organizations.</p>
LDAP Query Limit	wt.org.Ldap QueryLimit	Defines the maximum result size that can be requested by Windchill using an LDAP query.	Controls how many results LDAP sends to Windchill. If the property is set to zero, the internally configured LDAP value is used (typically 20000).

Property Name	Properties.html	Search Property Function	Description
			<p>If set to a lower value than the LDAP value, the value of this property is used. If set to a higher value than LDAP, then the LDAP configured value is used. The actual results returned to the user could be impacted by the <code>com.ptc.netmarkets.userSearch.maxCount</code> property.</p> <p> <b>Note</b></p> <p>If your organization needs to limit communication with LDAP or if you will need to search on wide criteria that could return many results, PTC recommends that you use a value other than the default of zero (0).</p>

<b>Property Name</b>	<b>Properties.html</b>	<b>Search Property Function</b>	<b>Description</b>
Required Character Search	com.ptc.net markets. participant Picker. requiredChar acter Search	Defines the minimum required characters	Specifies the quantity of characters required before a search will begin. For example, by setting the property to '3', the search requires three characters in at least one field. The characters limit the search results to return participants named with the specified characters. The default is set to '0'; allowing any quantity of characters to be used in a search.
Invalid Characters	com.ptc.net markets. participant Picker. invalidChar acters	Defines invalid characters	Specifies which characters are not counted towards the Required Character Search property. Special characters, such as asterisk (*), colon (:), and comma (,) are good candidates to be specified as invalid characters.  For example, with Required Character Search set at a minimum quantity of 3, and defining (*) as an Invalid Character, the search string



Property Name	Properties.html	Search Property Function	Description
			<p>(ma*) would not be allowed because the asterisk is not counted as a character. However, the search string (mat*) would allow a search to run because the search string has at least 3 valid characters.</p> <p>The default setting defines the space character ( ) as invalid for use in a search.</p> <p> <b>Note</b></p> <p>The Required Character Search property must be set to 1 or higher in order to use Invalid Characters property settings.</p>



<b>Property Name</b>	<b>Properties.html</b>	<b>Search Property Function</b>	<b>Description</b>
Leading Wildcard Allowed	com.ptc.net markets. participant Picker. leadingWild card Allowed	Allows or prohibits leading wildcards	Controls whether a leading wildcard character (*) is allowed in a search field. The default is set to true; a leading wildcard character is allowed as a search parameter.  Setting this property to false may help increase search performance.
Principal Wildcard Search	com.ptc.net markets. user.princi pal Wildcard Search	Enhances search to find search content within participant names	Adds wildcards on either side of the specified search characters to return any result that contains those characters anywhere in the participant name. The default is set to true; wildcards are automatically added to search characters.  Setting this property to false may help increase search performance.



---

## Using the Participant Administration Utility

You can access the Participant Administrator utility from **Site**  ► **Utilities** or from **Organizations**  ► **Utilities**:



- The **Participant Administration** utility link from **Site**  ► **Utilities** provides the site administrator with access to users and to the user-defined groups and organizations created in the site context.
- The link from **Organizations**  ► **Utilities** provides access to only those participants that belong to the organization context from which you launched the **Participant Administration** utility and to those that belong to the site context (which is its ancestor context). If the organization was set up so that it allows entire user and user-defined group directory selection, then you can see all users and groups (except for the system groups maintained by your solution). However, access control rules may be set to prohibit you from seeing some users and user-defined groups.

## Best Practices for Windchill PDMLink and Windchill ProjectLink

The Participant Administration utility creates only organization objects (also referred to as the organization ) and not organization contexts.

---

### Note

Creating an organization participant in the Participant Administration utility does not create an organization context. Both the organization participant and its context can be created the **Organizations** page (visible only to site administrators), accessed by clicking the **View All** link under **Organizations** . Click the new organization icon  at the top of the **Organizations** table. For more information about organization contexts, see [Getting Started with Windchill Administration on page 11](#).

---

Ensure that users have an email address, as many features in Windchill require users to have an email address. If users do not have the email attribute set in their user directory service entry, they cannot participate in the features that require an email address.

---

## Searching for Users and Groups

by default, users cannot search for users and organizations outside of their own organization. When creating or editing an organization context, you can turn off the **Restricted Directory Search** option to provide the ability to search for all users and organizations.


Regardless of whether **Restricted Directory Search** is selected, a site administrator can search for all users and organizations from any organization context.

## Best Practices When Maintaining a Directory Service Outside of Windchill

Because your Windchill solution may be connected to a corporate LDAP server rather than a Windchill-owned LDAP, you may not be creating users through the Participant Administration utility; instead, users are automatically created in the Windchill database when the users become active in the solution. As users are removed or changed in the user directory service through an external tool, you will need to manage the Windchill user objects by doing the following:

- Deleting Windchill user objects that no longer have valid user directory service entries (see [Maintaining the Connections between Participant Objects and their Directory Service Entries on page 289](#)).
- Cleaning up after deleted users (see [Deleting Users on page 270](#)).
- Managing the participant cache so that changes in a user directory service are available in Windchill (see [Managing the Participant Cache on page 287](#)).

## Managing Users

Users can be managed from the **Participant Administration** table. See help available in the Participant Administration utility for information about locating existing users and adding them to the table. Clicking the new user icon  allows you to create a new user.





There are some restrictions for the user name you enter for a new user:

- User names cannot include the following characters: #, /, >, \, and <.
- Because of known problems with the Apache and Sun ONE web servers, user logon names cannot contain multi-byte characters nor extended ASCII characters such as ä, ê, ì, ò, ù, æ, and so on.

---

 **Note**

Although the Participant Administration utility does not require that users have an email address, the following features in Windchill require that users have an email address:

- Giving the site administrator privileges through the **Site**  ► **Administrators** window
- Giving the organization administrator privileges through the **Organizations**  ► **Administrators** window
- Enabling the user to create products, libraries, or projects through the **Organizations**  ► **Creator** window
- Adding the user as a member of a project through the **Team** window in the **Project**  context

---


After a user is added to the table, you can manage the user.

Managing users includes performing the following activities:

- Creating users
- Searching for users
- Editing and deleting users

When deleting users, you can delete them from just the Windchill database or delete them from both the database and the user directory service.

- Creating users from existing users
- Associating users with profiles
- Editing the domain and personal cabinet of a user
- Viewing information about users
- Defining electronic signatures for users
- Assigning pictures for users
- Managing personal cabinet names

From Windchill PDMLink and Windchill ProjectLink, you can administer personal cabinets from **Site**  ► **Utilities** ► **Personal Cabinets Administration**.

- Purging users from the cache
- Synchronizing the teams' membership with updated user-defined groups

For more information, see [Synchronizing Team Membership for Users and User-defined Groups on page 273](#).

---

For more information on performing these activities, see the help available from within the Participant Administration utility.

## Changing User Passwords

When editing a user from the Participant Administration utility, you can change the user password along with changing other user information if you have the rights needed to make changes in the directory service.

---

### Note

In Windchill your password cannot begin or end with a blank space.

---

When you change the password for a user, the old password may still be active for a period of time. This is the case if the web server you are using caches user information, as is true with the Apache web server. If a user password is changed in LDAP, there may be a short period of time where the new password will not work, or where the old password and the new password will both work due to the cache. This is only temporary and will resolve itself when the web server cache expires and the web server refreshes the LDAP information. Generally, the time to live for cache entries is short. For example, the default for Apache is 10 minutes.

Additionally, you can configure your Windchill solution so that users can change their own passwords.

For more information on configuring password management, see the help available in the **Participant Administration** utility.

## Naming a User's Personal Cabinet

Windchill uses the `wt.folder.personalCabinetNamingAttribute` property in the `wt.properties` file to determine what the initial personal cabinet name should be for a given user. The `wt.folder.personalCabinetNamingAttribute` property contains the following default ordered list of attributes:

- name – The cabinet name used is the user's name.
- eMail – The cabinet name used is the user's email address.
- fullName – The cabinet name used is the user's full name.

For the cabinet name, Windchill uses the value of the first attribute in the list that produces a unique name. In most cases, the name of the personal cabinet is the user's name. If there is already a personal cabinet with that name, the user's email address is used for the personal cabinet name. If the email address is already being used as a cabinet name, then the full name is used. If the full name is already being used, the object identifier for the user (OID) is used as the cabinet name. The OID is a unique string that identifies each object in Windchill. If the OID is

---

already in use, Windchill appends an underscore and an integer, starting with 1, to the object identifier (<oid>\_1, <oid>\_2, and so on) until a unique cabinet name is discovered.

You can change the attributes used in creating the personal cabinet name or the order of these attributes by modifying the list of attributes in the wt.folder.personalCabinetNamingAttribute property using the xconfmanager utility. Valid values are those attributes used in user directory service entries. For example, to use the full name before using an email address, you could specify the following xconfmanager command from a windchill shell:

```
xconfmanager -s wt.folder.personalCabinetNamingAttribute=name,fullName,eMail,oid  
-t <Windchill>/codebase/wt.properties -p
```

Where <Windchill> is the location where your Windchill solution is installed.

To use a user's telephone number instead of the email address, you could specify the following property and value pair:

```
wt.folder.personalCabinetNamingAttribute=name,fullName,  
telephoneNumber,oid
```

If the attribute list for wt.folder.personalCabinetNamingAttribute has been modified and no personal cabinet name is discovered using the modified list, then Windchill derives the cabinet name from the user's name with the OID appended (as discussed earlier in this section).

For more information about using the xconfmanager utility, see help available in the **Participant Administration** utility.



## Associating Users with Profiles

Profiles define which parts of the user interface (for example, actions, tabs, and attributes) should be visible to a participant (such as a user, group of users, or the users of an organization). By associating participants with profiles, the user interface reflects the settings in the profile for that participant.

---

### Note

If the directory service your users are stored in is "read-only", then you cannot associate users with profiles using the Participant Administration utility.

Instead, manage user profiles from the **Profiles** page in the **Organization**  or **Site**  contexts.

---

When creating a new user or editing an existing user you can associate that user with a profile. On the **Profiles** step, specify the profile to which the user should be added as a member. You will need to create a profile prior to associating a user to a profile.

---

 **Note**

Users can be added to a profile on the **New User** window and the **Edit User** window in all Windchill solutions except Pro/INTRALINK 9.1.

---

For more information about profiles, see [Profile Management on page 291](#).

## Editing the Domain of a User

A domain is an administrative area that defines a set of administrative policies, such as access control, indexing, and notification. Objects associated with a domain are subject to its policies.

A user's domain can be edited on the **Edit User** window. Click **Find** next to the **Domain of User** field. The **Find Domain** window opens and you can search for and select a domain. You can also type the name of an existing domain into the **Context** field.

## Deleting Users

---

 **Caution**

Do not delete a user unless you understand how it affects the system, as described in this section.

---

These two actions result in deleting a user:

- Delete from Windchill 
- Delete from Windchill and Windchill Directory Server 

The first action has the effect of deleting the user from the Windchill database. The second action deletes the user from both the Windchill database and the user directory service. To use the second action, you must have the required permissions to be able to delete users from the directory service as well as the database.

---

 **Note**

You cannot delete users that are owned by a read-only directory server.

---

---

 **Note**

You cannot delete the Administrator or the Administrators group. You also cannot delete your own user object.

---

The results of deleting a user from the Windchill database are:

- The user is removed from all groups.
- All access control policy rules that specifically identify the user are removed.
- The user is removed from all notification lists within notification policy rules and, if deleting the user from the list results in an empty list, then the rule is also deleted.
- If the user was a member of a local or shared team, the user row in the **Members** table includes **(Deleted)** after the user name to inform the team that the user has been deleted. The deleted user can then be replaced or removed from the team.
- A user can be created with an identical user name as a user that was previously deleted, but if the original user's personal cabinet was not deleted, the new personal cabinet will have a different name. For more information, see [Naming a User's Personal Cabinet on page 268](#).
- If a deleted user is specified as the user of a collection defined in the index properties, a stack trace prints in the method server log when an attempt is made to index an object.

The following rules govern tasks associated with a workflow process when a user is deleted from the Windchill database:

- If a user is deleted after a workflow process has been initiated, but prior to assignment of a task, the user is removed from the list of participants and no task is assigned. The value of the wt.property called ignoreUnresolvedRoles decides if the task should be completed or assigned to the responsible role.
- If the user is deleted after a workflow process has been initiated, and a task has been assigned, that task must be manually reassigned. The task will be reassigned to a context creator.

For more information, see help available from the **Participant Administration** utility.

- A deleted user continues to appear in iteration history, object properties pages, and so on, but the name is not displayed as an email link.
- When a user is deleted, the user is automatically removed from the list of participants in any workflow process template. The user is also removed from any role mappings created as part of a life cycle or team definition. The change does not result in an iteration to the workflow or life cycle templates.


- 
- If a user is identified as a participant in a workflow template definition and that user is deleted from the system after the workflow has been initiated, any task that would have been assigned to the user is assigned to the Responsible Role which is generally the user who initiated the process.
  - If both the template creator and a user identified in a workflow process template are deleted after the workflow process is initiated, the workflow process stops until the tasks assigned to the deleted user are manually reassigned.

The results of deleting a user from both the Windchill database and the directory service include all results described earlier for deleting a user from the Windchill database and additionally include the following:

- A user is not authenticated when attempting to log into Windchill.
- The user's name is not included in search results.

If a user is not removed from the user directory service, a new user object is created in Windchill database when the user tries to log on or when the user is selected from a search. This new user object is not the same object that was deleted, and all of the results of the earlier deletion are still true. For example, the user is no longer a member of the groups to which the user had been a member.

After deleting a user from the Windchill database, you must perform the following clean-up steps:

- Reassign any items in the user's list of tasks.
- Unlock any objects the user has checked out of the Windchill database.
- Remove the user's personal cabinet and any folders or objects within it. From Windchill PDMLink, use **Site**  **► Utilities ► Personal Cabinets Administration**.

## Changing the Organization to which a User Belongs

You can change the organization attribute for users using the **Participant Administration** utility (if you have write permission to the directory service) or by using a third party tool that allows your site to modify user entries in your directory service. Changing the organization attribute by using the **Participant Administration** utility automatically changes the other organization-related information for users. However, changing this attribute by using a third party tool does not change the other organization-related information for users.

If you change the organization affiliation of a user, the domain and personal cabinet of the user are automatically updated to reflect the change (by default). When the site preference named **Synchronize Domains for User Organization Changes** is set to true and the organization of a user changes, the user domain and the domain of the user's personal cabinet are reassigned to the new organization root domain. Additionally, the organization groups that are associated with the



---

context teams for which the user is a member, are updated. The user is removed from the group for the old organization and added to the group for the new organization.


If this preference is set to false, the site administrator will have to manually execute the OrgSync command line utility to perform the update after using a third party tool to change a user's organization. For more information on using this utility, see [Using the OrganizationSync Utility for User Organization Changes on page 162](#).

You can turn off this automatic update through the **Synchronize Domains for User Organization Changes** preference that is under the **Display** category.

For more information about preferences, see help available in the **Participant Administration** utility.


## Synchronizing Team Membership for Users and User-defined Groups

Users and user-defined groups can be members of teams. If group membership is modified from within Windchill, the membership of the teams in which the group is a member is automatically updated.

If the membership of one or more groups is modified using a third-party LDAP tool, then you can manually synchronize team membership by clicking the recompute group icon  that is available from the right-click action menu for the group in the **Participant Administration** table.

---

### Note

If the groups that have been updated using a third-party LDAP tool are not used in any context or shared teams, you do not need to recompute group membership; however, you should remove the groups from the participant cache by using the Remove from Cache icon  that is available from the right-click action menu for the group in the **Participant Administration** table.

---

## Synchronizing Users with LDAP

Enabling the **Synchronize Name with LDAP** option for a user allows the full name, last name, or email address of the user to be automatically synchronized between LDAP and the database. This prevents problems that can occur when user attributes are changed in LDAP.

---

Updates to user data are made on a periodic basis rather than as soon as the update in LDAP occurs. By default, user data is updated weekly. The interval between synchronization is determined by the `wt.org.userSyncTime` property. Synchronization is checked when a user logs on to Windchill if the time specified in the property has been exceeded since the last update.

User data synchronization can be done by an administrator using the following process:

1. Update the necessary attributes in the LDAP entry for the user.
2. Ensure that the user is not logged on to Windchill and that all browser sessions have been closed.
3. Run the following SQL command from the database command prompt:  
`Select lastSyncTime from WTUser where name='<userid>';`
4. Confirm that the value displayed is larger than the value of the `wt.org.userSyncTime` property.
5. In Windchill, navigate to the **Participant Administration** utility.
6. Add the user to the **Participant Administration** table.
7. Right-click the user in the table and select the **Remove from Cache** action.

The user data should be updated the next time the user logs on to Windchill.

---

 **Note**

Depending on your settings for the `wt.session.sessionUsers.timeout` property, a wait time of up to 30 minutes may be required to clear the active session of the user.






---

## Managing User-defined Groups

Groups created using the Participant Administration utility are used in Windchill utilities that allow administrators to select participants as part of setting up context teams, access control, indexing, and notification policies or as part of setting up workflow processes or life cycle templates.

---

 **Note**

Administrators can create and manage the groups used with context teams using the **Groups** link from the **Organizations**  context and the **Team** page from the **Products** , **Libraries** , **Programs**  or **Projects**  contexts.

---

---

Groups can be members of other groups, and groups are associated with the context in which they are created. After you have created a group, you can edit the group but you cannot change the context associated with the group.

Creating a new Windchill group involves creating both a group object in the Windchill database and a group entry in a directory service. For more information, see help available in the **Participant Administration** utility.

---

 **Note**

To create a new group, you must have write permission to the directory service in which you want the group directory entry to reside.

---

Managing user-defined groups from the Participant Administration utility includes performing the following activities:

- Creating user-defined groups
- Searching for user-defined groups
- Editing and deleting user-defined groups

When deleting user-defined groups, you can delete them from just the Windchill database or delete them from both the database and the directory server.

- Assigning profiles
- Viewing information about user-defined groups
- Purging user-defined groups from the cache
- Synchronizing the teams' membership with updated user-defined groups. For additional information, see [Synchronizing Team Membership for Users and User-defined Groups on page 273](#).

From within an organization, you can also add or update user-defined groups that are defined in the organization context.

---

 **Note**

The groups that can be managed from the Participant Administration utility do not include system groups. These system groups (also referred to as internal groups) are automatically created and used by Windchill. For example, the system groups created for the context team roles can only be managed from the **Teams** page; they are not visible through the Participant Administration utility.

---

---

For specific instructions on how to perform these activities, access the help from within the Participant Administration utility.

The following sections provide additional information about working with groups and deleting groups.

## **Working with User-defined Groups that are Maintained in a Directory Server**

Any groups created in a node of a directory server that can be searched by Windchill solution are automatically added to the Windchill database when the node is searched. The name of each Windchill user-defined group object is taken from the `cn` attribute of the LDAP group entry distinguished name (unless the mapping done in the JNDI adapter specifies a different attribute). This allows you to create groups using the editing tool available through a directory service rather than using the interfaces available in Windchill.

Adding and removing members from a user-defined group can also be accomplished using the editing tool available through a directory service. After updating group membership in the directory service, you can synchronize the team membership with the updated groups as described in help available in the **Participant Administration** utility.

When access to Windchill is limited, you can rename a group using the editing tool available through a directory service while maintaining the association of the directory server group with an existing Windchill group; however, the name of the group in the Windchill database cannot be changed to match the name stored in the directory server unless the user has write permission to both the database and the directory server. PTC recommends that you do not rename groups outside of the Participant Administration utility.

Use the following steps to re-establish the connection between an existing Windchill group to an LDAP entry for a user-defined group that has been renamed in your directory server:

1. Limit access to Windchill before renaming the user-defined group.

---

 **Caution**

If you do not limit access and someone searches and finds the renamed group or updates the user information for any member of the group, then a new Windchill group object is automatically created for the group. After a new Windchill group is associated with the LDAP entry, you cannot reconnect the renamed group to another Windchill group.

2. Rename the user-defined group using the editing tool available through a directory server.
3. From the main **Participant Administration** table, use **Search Disconnected Participants** and **Reconnect Disconnected Participant** actions.

For specific instructions on how to perform these activities, access the help from within the Participant Administration utility.

## Deleting User-defined Groups

---

 **Caution**

Do not delete a user-defined group unless you understand how it affects the system, as described in this section.

There two actions result in deleting a user-defined group:

- Delete from Windchill 
- Delete from Windchill and Windchill Directory Server 

The first action has the effect of deleting the user-defined group from the Windchill database. The second action deletes the group from both the Windchill database and the directory server. To use the second action, you must have the required permissions to be able to delete user-defined groups from the directory server as well as the database.

---

 **Note**

You cannot delete groups that are owned by a read-only directory server.

---

---

The results of deleting a user-defined group from the Windchill database are as follows:

- Users who were members of the user-defined group no longer belong to the group.
- All access control rules that specifically refer to this user-defined group are removed. If any users had access permissions derived solely from membership in the deleted group, it may be necessary to create new rules to restore the lost permissions.
- The user-defined group is removed from all notification lists within notification policy rules; if deleting the group from the list results in an empty list, then the rule is also deleted.
- If the user-defined group had been added to a local or shared team, the team membership shows the group as deleted, and if a user was a member of the team only because he or she is a member of the deleted group, then the user is no longer a member of the team. The deleted group remains on the **Members** table so that anyone managing a team is aware of the deletion. The deleted group row can then be removed from the **Members** table since the group is no longer a member of the team.

The following rules govern tasks associated with a workflow process when a user-defined group is deleted from the Windchill database:

- If a user-defined group is deleted after a workflow process has been initiated, but prior to assignment of a task, the group is removed from the list of participants.

If removing the group leaves no participants for a role, then the role resolution is determined by the settings in the wt.properties file:

- If the wt.workflow.engine.ignoreUnresolvedRole property is set to true and if the ignoreUnresolvedRole event configuration is set for this activity; then there will be no task created and the WfAssignment object completes so the workflow does not hang.
- If the wt.workflow.engine.ignoreUnresolvedRole property is set to false, one task is created that goes to the Responsible Role defined in the activity template. The default for the Responsible Role is the process creator. When the workflow process is started through a life cycle, the process creator is the creator of the business object.

For more information, see [Activity Flags on page 379](#).



- If the user-defined group is deleted after a workflow process has been initiated and tasks are assigned, deleting the group has no effect on the process because the group itself is no longer being referenced. Tasks are assigned to the individual users that were in the group.

- 
- When a user-defined group is deleted, it is automatically removed from the list of participants in any workflow process template. The group is also removed from any role mappings created as part of a life cycle or team definition.
  - If a user-defined group is identified as a participant in a workflow template definition, and that group is deleted from the system after the workflow has been initiated, any task that would have been assigned to the group is reassigned to the responsible role. Generally, the responsible role is the user who initiated the workflow process.

By deleting a user-defined group from both the Windchill database and the directory service, the user-defined group is not included in search results and all results described earlier for deleting a group from the Windchill database also apply.



If a user-defined group is not removed from the directory service, a new group object is created in Windchill database when the group is selected from a search. This new group object is not the same object that was deleted and all of the results of the earlier deletion are still true. For example, the users who had been members of the group are no longer members.

## Managing Organizations

Manage organization objects, also known as organization participants, from the **Participant Administration** table. Clicking the add participants to the table icon  allows you to search for existing organization participants and add them to the **Participant Administration** table. Clicking the new organization icon  allows you to create a new organization participant.

---

### Note

Creating an organization participant in the Participant Administration utility does not create an organization context, it only creates the participant. Both the organization participant and its context can be created from the **Organizations** page (visible only to site administrators), accessed by clicking the **View All** link under **Organizations** . Click the new organization icon  at the top of the **Organizations** table. When creating an organization context, you can associate the context with either an existing organization (that is not already associated with a context) or you can create a new organization.

---

Organization participants created using the Participant Administration utility are considered restricted organizations. This means that no access control rules are automatically added to allow users in one organization to see users and groups from other organizations. When you create an organization context, you can select

---

a checkbox that allows users in the organization to see all users and groups. This adds the organization to the Unrestricted Organizations group, which has the access control rules set to allow users to see other users and groups.

Organization participants can be used to identify an organization as the owner of specific parts and documents. By default, Windchill solutions are not set up to allow organization ownership selection. The organization under which the parts and documents are created automatically own them. There are multiple steps involved in enabling organization ownership selection, one of which is creating the organization participants.

For more information on enabling organization ownership selection, see [Owning Organization Participants on page 158](#).

Managing organizations includes performing the following activities:

- Creating organization participants
- Searching for organization participants
- Editing and deleting organization participants

When deleting organization participants, you can delete them from just the Windchill database or delete them from both the database and the directory service.

- Viewing information about organization participants
- Adding profiles for organization participants
- Purging organization participants from the cache

For specific instructions on how to perform these activities, access the help available from the Participant Administration utility.

---

 **Note**

When specifying the internet domain name of an organization, the name you enter can contain only alphanumeric characters and the hyphen (-) character. Do not enter any other types of characters in the name.

---

The following section provides additional information about deleting organization participants.



---

## Deleting Organizations

---

### **Caution**

Do not delete an organization participant unless you understand how it affects the system, as described in this section.



---

### **Note**

You cannot delete an organization participant that is associated with an organization context.

---

There are two actions that result in deleting an organization participant. They are:

- Delete from Windchill 
- Delete from Windchill and Directory Server 

The first action has the effect of deleting the organization participant from the Windchill database. The second action deletes the organization participant from both the Windchill database and the directory service. To use the second action, you must have the required permissions to be able to delete organization participants from the directory service as well as the database.

The results of deleting an organization participant from the Windchill database are as follows:



- The organization is removed from all notification lists.
- All access control rules that identify this organization are removed from the access control policy for a domain. If any users had access permissions derived solely from membership in the deleted organization, it may be necessary to create new rules to restore the lost permissions.
- If the organization had been added to a local or shared team, the team membership shows the organization as deleted and, if a user was a member of the team only because he or she is a member of the deleted organization, then the user is no longer a member of the team. The deleted organization remains on the **Members** table so that anyone managing a team is aware of the deletion. The deleted organization row can then be removed from the **Members** table since the organization is no longer a member of the team.



When an organization participant is deleted from both the Windchill database and the directory service, it results in the above points in addition to the organization no longer being included in search results.

If an organization LDAP entry is not removed from the directory service, a new organization participant is created in Windchill database when the organization is selected from a search. This new organization object is not the same object that was deleted and all of the results of the earlier deletion still hold.


## Windchill Participant Status

Windchill participants can have one of several status values. The possible status values for participants include the following:

Status	Participant Type	Description
Active	All Participants (users, groups, and organizations)	An active user can log on to Windchill and take actions according to their user license. Most Windchill users are active users. Active groups and organizations are able to have members and are not otherwise disconnected or deleted from Windchill.  Active users, groups, and organizations do not have a status when they appear throughout Windchill.
Pending	Users only	A pending user cannot log on to Windchill. Pending users are created when a user is added to a context team via email, but the email entered is not currently associated with an active Windchill user.  Pending users have a status of <b>Pending</b>  when they appear throughout Windchill.  For more information, see <a href="#">Pending Users on page 283</a> .
Replicated	Users only	A replicated user cannot log on to Windchill. Replicated users are created when a user is imported into Windchill using a replication package delivery.  Replicated users have a status of <b>Replicated</b>  when they appear throughout Windchill.  For more information, see <a href="#">Replicated Users on page 283</a> .

Status	Participant Type	Description
Disconnected from directory service	All participants (users, groups, and organizations)	<p>A disconnected participant is a participant whose LDAP entry can no longer be found by Windchill. Disconnected participants can be reconnected or they can be removed from Windchill.</p> <p>Disconnected users, groups, or organizations have a status of <b>Disconnected from directory service</b>  when they appear throughout Windchill.</p> <p>For more information, see Managing Disconnected Participants in the PTC Windchill Help Center.</p>
Deleted	All participants (users, groups, and organizations)	<p>A deleted participant has been disabled in Windchill and can no longer be used. Participants can be deleted from Windchill and from the Windchill directory server. Deleted users can no longer log on to Windchill.</p> <p>Deleted users, groups, or organizations have a status of <b>Deleted</b>  when they appear throughout Windchill.</p> <p>For more information, see the PTC Windchill Help Center.</p>

## Pending Users

A user who is known only through email is stored in Windchill as a pending user. Commonly, these users are added to a context team via email and there is no Windchill user with a matching email address. A pending user does not have an associated LDAP entry. Pending users appear in Windchill with a status of **Pending**  and with only the available email address for the user name.

Pending users cannot log on to Windchill until they are activated.

## Replicated Users

A replicated user is a user who was added to Windchill through the import of a Windchill replication package delivery. Basic attributes for the user are available, depending on what was sent from the source Windchill installation. Often these

---

attributes include the user name, full name, email address, and last name. Replicated users do not have an associated LDAP entry. A replicated user appears in Windchill with a status of **Replicated** [☐](#).

When a replication package delivery is imported, Windchill attempts to match all imported users with current Windchill users. By default, user matching is attempted with the user's distinguished name. If no match is found, matching is next attempted by user name. If there is still no match to a current Windchill user, a replicated user is created. You can configure your system to match users by attributes other than user name. For more information, see the Identifying Users in Context Replication and Activating Replicated Users section of the *PTC Windchill Customization Guide*.

A replicated user can be added to a context team via email. However, replicated users cannot log on to Windchill until they are activated.

## Activating Pending and Replicated Users

Pending and replicated users are activated if a user is created in Windchill or loaded into Windchill with some of the same identifying attributes.

Activation occurs any time a new user is added to Windchill by one of the following means:

- Manually creating the user with the **Participant Administration** utility.
- A user with an entry in the corporate LDAP system logs on to Windchill for the first time or is discovered by Windchill during a particular action.
- User data is loaded into Windchill using a load file.

Pending users are activated if a user is created or loaded with the same email address.

Replicated users are activated if a user is created or loaded with the same user name or alternate user name as the replicated user. You can configure your system so that replicated users are activated if a user is created or loaded with the same email address as the replicated user rather than matching via user name.

When a pending or replicated user is activated, all places where the pending or replicated user was referenced are updated to reference the active Windchill user instead. For example, a part can be imported into Windchill with a reference to a replicated user as the creator of the part. If the replicated user is activated later, the reference to the user as the creator of the part is updated to the newly activated user.

---

 **Note**

If the new user created via the **Participant Administration** utility, an LDAP user log on, or a load file has an alternate user name that matches a pending or replicated user, the pending or replicated user is activated and any attributes associated with the new user overwrite the attributes established for the pending or replicated user.

---

## Participant (Users, Groups, and Organizations) Identification

Participants are identified across Windchill systems through the use of the participant Unique Federation Identifiers (UFIDs). The syntax for UFIDs is as follows:

*<distinguished\_name>:<guid>@<domain>*

where:

*<distinguished\_name>* is the distinguished name of the participant (which is made up of directory attributes that include the user name and directory location).

*<guid>* is the globally unique identifier of the repository in which the participant was first created or discovered.

*<domain>* is the internet-style domain name of the repository in which the participant currently resides.

Together, *<guid>@<domain>* identifies the directory service in which the participant resides.

## Best Practices for Assigning Domains to Participants

A domain is an administrative area that defines a set of administrative policies, such as access control, indexing, and notification. Objects associated with a domain are subject to its policies. When participant objects are created, they are associated with default domains as follows:

- Users who are affiliated with an organization (the organization attribute on their directory service entries is set) are associated with the domain that was created for the organization when the organization object was created. This domain usually has the same name as the organization (or a shortened version of the organization name) and the domain is a child of the site context User

---

domain. If the organization is associated with an organization context, then the domain is in the organization context; otherwise, the domain is in the site context.

- Users who are not affiliated with an organization (the organization attribute on their directory service entries is not set) are associated with the site context Unaffiliated domain. This domain is a child of the User domain. One exception to this rule is the Administrator user, which is associated with site context System domain.
- User personal cabinets are associated with the same domain as the user. The one exception to this rule is that the personal cabinet for the Administrator user is associated with the User domain in the site context.
- User-defined groups created in the site context are associated with the site context Unaffiliated domain. This domain is a child of the User domain.
- User-defined groups created in an organization context are associated with the domain that was created for the organization when the organization object was created. This domain usually has the same name as the organization (or a shortened version of the organization name) and the domain is a child of the site context User domain. The domain is in the organization context.
- Organizations are associated with the domain that was created for the organization when the organization object was created. This domain usually has the same name as the organization (or a shortened version of the organization name) and the domain is a child of the site context User domain. If the organization is associated with an organization context, then the domain is in the organization context; otherwise, the domain is in the site context.

---

 **Note**

The default domain associations described in the previous list only apply if you have not set up JNDI adapters that configure participant domain assignments. The domain assignments in a JNDI adapter take precedence over the system defaults.

---

User objects and personal cabinets are created automatically when users are selected in a search or when users log in. These user objects and personal cabinets are always associated with the default domains described earlier. When you create a user through the Participant Administration utility, you can select the domains. But in most cases, you should use the defaults (which are used when you do not select a domain).

When creating group objects through the Participant Administration utility, using the default domain is usually a good choice. However, you may want to choose a different domain if you want policy rules from a domain other than the default to apply to the group object.

---

When creating organization objects through the Participant Administration utility, using the default domain is usually a good choice. However, you may want to choose a different domain if you want policy rules from a domain other than the default to apply to the organization object. This may be the case if you want to allow users to select the owning organization when they create parts and documents. For more information on turning on the organization ownership feature, see [Owning Organization Participants on page 158](#).

## Receiving Administrative Notifications

When a user is deleted using the Participant Administration utility, the administrator receives a notification by email (or possibly through Windchill workflow). The administrator is notified that the participant has been disabled and that any additional manual actions should be taken, such as removing a user's personal cabinet.

Similarly, Windchill will notify the administrator that a repair is needed when it detects that a user, user-defined group, or organization needs to be repaired because the object in the Windchill database no longer references an existing directory service entry, possibly because the entry has been removed from or relocated in the directory service.

These notifications are initiated by calling the Info\*Engine tasks named `NotifyDisabled.xml` and `NotifyRepair.xml` in the `<Windchill>/tasks/wt/federation` directory (where `<Windchill>` is the Windchill installation directory). You can customize these tasks to tailor the way in which notification is done.

Also, you can change the email address used for the notifications by setting the `wt.org.principalAdministratorEmail` property in the `wt.properties` file. The default email address used is the email address of the Administrator user (if one is set) or the `postmaster@<server_hostname>` email address, where `<server_hostname>` is the value of the `wt.rmi.server.hostname` property in the `wt.properties` file.

## Managing the Participant Cache

To improve the access time required for users, user-defined groups, and organizations, Windchill maintains an in-memory cache of user, user-defined group, and organization information.

---

 **Note**

If user, user-defined group, or organization attributes are changed using an administration tool other than the Participant Administration utility (for example, using a directory administration tool), then the cache containing those attributes must be purged in order for Windchill to display the changed attributes.

---

You can manage the participant cache in two ways:

- By setting the maximum time that the information about a participant can remain available in the cache. Cache entries are automatically purged when the system accesses stale entries.
- By selecting actions that purge information from the cache from within the Participant Administration utility.

## Automatically Purging Entries from the Participant Cache

You can add the following properties to the `wt.properties` file to automatically purge cache entries:

- The `wt.principal.cache.timeToLive` property defines the amount of time that any given participant cache entry is available from the cache. Specify the property value in seconds. If the property value is not set or is set to zero or less than zero, then cache entries are not automatically removed from the cache. Out of the box, this property is not set.
- The `wt.principal.cache.timeToLiveRandomizer` property adds a random amount of time to the time stamp of each cache entry so that a large number of entries do not expire at the same time. Specify the property value in seconds. If the property is not set, the value defaults to 600 seconds (10 minutes). If the property is set to zero or set to less than zero, then no random value is added to the time stamp of each cache entry. Out of the box, this property is not set.

When a valid value is specified, the random amount added to the time stamp varies between 1 second and the property value. For example, if the property value is 600 seconds (10 minutes), a value between 1 second and 600 seconds is added to the time stamp of a cache entry when the entry is added to the cache.



---

Use the `xconfmanager` utility to add the properties. For example to add the `wt.principal.cache.timeToLive` property, specify the following `xconfmanager` command from a `windchill` shell:

```
xconfmanager -s wt.principal.cache.timeToLive=600
-t <Windchill>/codebase/wt.properties -p
```

Where `<Windchill>` is the location where Windchill is installed.

For more information about using the `xconfmanager` utility, see help available in the **Participant Administration** utility.

## Manually Purging Entries from the Participant Cache

From within the Participant Administration utility, you can purge either the entire cache or individual entries from the cache.


For specific instructions on how to perform these activities, see help available in the **Participant Administration** utility.

## Maintaining the Connections between Participant Objects and their Directory Server Entries

Sometimes the definitions of participants in the directory server are changed using a directory administration tool other than the Participant Administration utility. For example, another tool is sometimes used to move users, groups, or organizations from one directory location to another. When this happens, the distinguished names for the participants that are moved change. During normal operation, Windchill keeps track of the objects it encounters that do not have valid distinguished names.

You may search for disconnected participants and

- reconnect the disconnected participants
  - delete the disconnected participants from Windchill
- or
- delete the disconnected participants from Windchill and the Windchill directory server.

Clicking the **Search Disconnected Participants**  action on the **Participant Administration** table searches for the disconnected participants for which the distinguished name currently associated with the participant is not valid.

---


From the **Participant Administration** table, you can do the following activities:

- Search for additional participants that have non-existing distinguished names
- Reconnect disconnected participants
- Delete disconnected participants
- Purge all participants from the cache

For specific instructions on how to perform these activities, see help available in the **Participant Administration** utility.

## Registering a non-Windchill User

This procedure describes how to register a non-Windchill user. The registration can be done through an email notification when a non-Windchill user is added to project team. Perform the following:

1. Login as project creator.
2. Create a project.
3. Go to the **Team** page of the project and click the add participants to team icon .
4. Under **Email Invitation**, add the non-Windchill user email ID (for example, abc@gmail.com).

The user for abc@gmail.com must open the email that is sent and click the **Register** action in the email.

To configure Windchill ProjectLink self registration, change the following properties in the `<windchill>/conf/register/reg.properties` file

```
# the ldap used: provider_url=ldap://pl-pla1.ptc.com:389
```

```
ldap://<LDAPserverName>.<MyCompany>.com:<port>
```

```
# the Directory Manager
```

```
principal=cn=Manager
```

```
# password for Directory Manager
```

```
credentials=wcadmin
```

```
# user_registration_subtree= to point to ou=people node in the LDAP
```

```
user_registration_subtree=ou=people,ou=pdmpjl,l= <location> ,o= <MyCompany>
```

---

## Profile Management



Profiles allow the site and organization administrator to dynamically control which actions are visible to a user, group of users, or users in an organization by associating that information with a profile. A profile represents a typical category of user within a company and is based on the roles and privileges associated with that particular user category.

By defining a profile that exposes only the necessary functionality and information needed by a user, it creates a focused and simplified user interface, reducing confusion by eliminating areas of the user interface that could be distracting. This capability allows customers to ensure that a supplier, customer, or group of users is presented with a streamlined and focused set of information and actions.

Each user or group can be associated with one or more profiles. The least restrictive settings for visibility are assumed. For example, if a user is associated with two profiles where one profile hides an action, but the other profile allows visibility of that action, then the user will see the action in the user interface. If one profile allows read only visibility to an attribute, but another profile gives full rights to that same attribute, then the user will have full rights to the attribute.

Changes that are made to profiles take effect after the user subsequently logs into the system.

## Creating Profiles

Profiles are created from the **Profiles** sub-navigation link in either the **Site**  or the **Organization**  contexts.

Users, groups, and organizations can be associated with a profile when creating or editing a profile from the **Profile** page. When creating a user from the **Participant Administration** utility, the user can be associated with any existing profile.

- The **Profiles** page on the **Site** context provides you, the site administrator, with access to all profiles created in the site context.
- The link from the **Organization** context provides access to only those profiles that are available through the organization context **Profiles** table as well as any profiles created in the current site context.

Profiles that are created in an organization context are peers to the profiles created in the site context, unless they are given identical names – that is, the system will merge the settings from all profiles that are associated with a user, regardless of whether they are defined at the site or the organization contexts in order to determine what will be visible to the user. When a profile is created in an organization context with an identical name to a profile created in the site context, the organization profile overrides the site profile.

---

For more information on creating a profile, see help available in the **Participant Administration** utility.

## Profiles as a Visibility Control Mechanism

Profiles are not an access control mechanism; they are a user interface control mechanism.

The profiles that are associated with a user, group, or an organization control which actions and areas of the user interface are visible by those users. A user could have permission to edit an object based on an object domain-based policy, but not have visibility to that edit action for the object because this action is not included in the user's profile.

The primary goal in defining profiles is simply to hide the user interface elements (e.g., actions, tabs, and attributes) that a user has no need for or interest in. If a user does not have rights to an object or an action through access control rules, a profile will not add visibility to actions or information that are restricted by underlying access control policies. That is, you cannot grant a user visibility through a profile to an action or an area of the user interface for which that user does not already have access control rights. For example, a user could have access control permissions to the **Create Part** action in the system, but through a profile, that action can be hidden from the user and not visible in the user interface. On the other hand, if the user does not have access control permissions to the **Create Part** action, that action cannot be made visible to the user via a profile. It is the combination of a user being granted permission to an object or action via access control policies, and the profile granting visibility to those actions and objects, that will enable a user to see and perform an action.

When a profile is associated or disassociated from a user or group, no change in access permissions is implied or enforced.

## Default Profile Behavior for a New User

When a user is added to the system and the user is not associated with a profile, the user will inherit the profile that is associated with the organization of which the user or group is a member. If the organization to which the user is added is not associated with a profile, and the user is not associated with a profile, then the user's visibility to actions and areas of the user interface will be determined by the default profile system configuration. The user will not be associated with this default system profile but the system will use this profile for the user in the absence of any other profile association. For more information, see [Global Default Settings on page 293](#).

---

## Global Default Settings

The out-of-the-box system default profile provides visibility to all functions and areas of the user interface. This system profile may be modified by the site or system administrator to provide visibility to a minimal number of actions and information elements.

A site or system administrator can globally configure the default visibility for actions as well as the standard out-of-the-box roles. This is done by modifying the out-of-the-box system default profile. For more information, see the *PTC Windchill Customization Guide*.

## Overriding Profiles in an Application Context

Profiles that are created in both the site and organization contexts can be overridden in a specific application context by the application context manager, such as in a specific project. For example, assume that a user is associated with a profile that is defined in the site context and this profile does not allow visibility to the actions that would allow that user to create folders in any application context. A project manager can override the site-defined profile privileges and allow visibility to the action for creating folders for that user within a specific project. Application context managers override the site-defined profiles from the **Team** page by using the **Configure Actions for Roles** option in the team in which the user is a member.

For more information on configuring the actions for roles, see help available in the **Participant Administration** utility.

## Default Visibility for Application Context Managers

The site and organization administrator can choose to set defaults for and hide visibility over a specific product, library, project, program, or other application context action or user interface element. That is, the site and organization administrator can carefully control which elements that application context managers (project, program, product, and library managers) are able to override in a context instance.
























Removing the ability for an application context manager to override a profile setting is done by globally hiding visibility to the **Configure Actions for Roles** action for a specific context. If this is done, then the visibility of actions and areas of the user interface in a context instance cannot be modified by that application context manager.

If an action or user interface element is allowed to be configured or overridden by the application context manager in a context instance, then the user interface element will be displayed as a row in the **Configure Actions for Roles** table which is accessed from the context team's **Members** table.

The site administrator can define a default value (to show or hide) the user interface element but if the user interface element is made configurable in a context, then the application context manager can override the default and choose to show or hide the user interface element per role in the context team.

## Out-of-the-Box Profiles

The following table lists the profiles provided out-of-the-box and their descriptions:

Profile	Description
CAD Author	Provides visibility to the <b>Projects</b>  , <b>Products</b>  , <b>Libraries</b>  , and <b>Changes</b>  contexts and to the CAD data management functionality, including the <b>Add to Workspace</b> action.
Consumer	Provides visibility to the <b>Projects</b>  , <b>Products</b>  , <b>Libraries</b>  , and <b>Changes</b>  contexts, but hides import and export to excel functionality as well as all authoring functionality across projects, products, and libraries.
Customer	Provides visibility to the <b>Projects</b>  <b>► Folders</b> page but hides discussions, routings, import and export to excel functionality, and search functionality, including the CAD data management functionality.
Employee	Provides visibility to the <b>Projects</b>  , <b>Products</b>  , <b>Libraries</b>  , and <b>Changes</b>  contexts, but hides the CAD data management functionality.
Non-Employee	Provides visibility to only the <b>Projects</b>  context but hides import and export to excel functionality, global search, project search, and home page search as well as all authoring functionality.
PDM	Provides visibility to the <b>Products</b>  , <b>Libraries</b>  , and <b>Changes</b>  contexts, but hides the <b>Projects</b>  and <b>Programs</b>  contexts as well as the CAD data management functionality.
Procurement	Provides visibility to the <b>Projects</b>  , <b>Products</b>  , <b>Libraries</b>  , <b>Changes</b>  , and <b>Suppliers</b>  contexts, but hides the CAD data management functionality.
Project	Provides visibility to the <b>Projects</b>  context, but hides all other tabs as well as the CAD data management functionality.

Profile	Description
Supplier	Provides visibility to only the <b>Folders</b> 📁, <b>Teams</b> , and <b>Discussions</b> pages in the <b>Projects</b> 📁 context, and hides import and export to Excel functionality.
View-Print	Provides visibility to only the actions available to users in the View and Print Only license group, such as <b>View Information</b> . All creating, editing, and import and export to Excel actions are hidden.  The View and Print Only license group is added to this profile by default.

### Note

The CAD data management functionality referred to in the out-of-the-box profiles is controlled by the action, **View Related CAD Documents** in the set action visibility list.

## Profile Actions and User Interface Elements

When creating a profile, you can specify visibility at the global level or by making specific actions and user interface elements visible within a specific application context.

The **Set Action Visibility** step displays a list of all the actions and user interface elements that can be hidden or made visible in a profile. The actions and user interface elements are displayed based on the application context in which they reside in the user interface, for example, the **Products** 📁, **Projects** 📁, **Libraries** 📁, and **Programs** 📁 contexts.

Within each column, visibility can be given to all or only a subset of actions or user interface elements within a specific application context by selecting the corresponding checkbox.

For more information on setting visibility of the actions, see help available in the **Participant Administration** utility.

Visibility can also be specified at the global level using the **Global** column in the **Edit Profile** window. For example, if you are creating a profile where visibility should be given for everything in the Change and Library contexts, you can select the checkboxes in the Global column for **View Library Tab** and **View Change Tab**.


The global settings are available for profiles only and cannot be modified in a context instance. Application context managers can only modify the action list that is applicable to their active context.

---

## Default Settings for Actions

Out-of-the-box, most of the actions and user interface elements are selected by default. That is, they are made visible by default in a profile unless the administrator deselects the corresponding checkbox.

The following table lists the out-of-the-box actions that are deselected by default, unless an administrator specifically grants visibility by selecting the checkboxes:

Profile Action Name	Default
Configure Actions for Roles  <b>Note</b> This action sets the default visibility within a specific tab for the application context manager to override the profile for that specific instance in the context.	deselected (not visible)
Modify Teams Modify Team is not a specific action found in the user interface. The term is used to describe the general task of changing and modifying a team which includes multiple actions in the user interface.	deselected (not visible)



# 10

## Teams and Team Template Administration

Overview .....	298
Context Teams .....	298
Shared Teams.....	298

This section introduces basic concepts about context teams, shared teams, and team templates.

For more information, see the Teams and Roles help and the Team Template Administration help.

---

## Overview

Windchill teams are made up of participants and can be associated with objects, a context, or, in the case of team templates, life cycle or workflow processes.

- When business objects (such as parts and documents) are created, a unique team is created as its own object and is associated with the business object. The team contains all the roles consolidated from the team, life cycle, and workflow templates. The roles then get mapped to users.
- At the context level, the manager can create a context team specific to a particular project, library, program, or product. Each context team identifies the members of the specific project, library, program, or product and assigns the members to roles that have been established in the context. Each context team can be made up of a local team, a shared team, or the combination of a local team and shared team. Context teams are also used when creating the team and team roles associated with a specific business object.
- A team template can map participants and actors to roles. The team template can be assigned to a life cycle or workflow-managed business object, when it is created, to use as a template for roles resolution for the team.

For more information, see the Teams and Roles help and Team Template Administration help.

## Context Teams

A context team is a list of the members of a project, program, product, or library context. Using the **Teams** page for the context, a context manager can manage the team by adding users to roles and creating additional roles within the team.

For more information, see the Teams and Roles help.

## Shared Teams

Depending on how a context team is set up, team members can be added individually or they can be part of a shared team. Shared teams are created in an organization context and can be used by multiple application contexts within the organization. Using shared teams rather than adding all users individually to each context team can reduce the work of maintaining multiple context teams. Like context teams, shared teams have established roles available and additional roles can be added. Changes made to a shared team's members or roles are immediately evident in context teams that use the shared team. Shared teams can only be added when a context is created.

For more information, see the Teams and Roles help.

## Understanding Life Cycles

The Life Cycle Model .....	300
Basic and Advanced Life Cycles .....	301
Managing Life Cycle Processes .....	303
Accessing the Life Cycle Template Administration Utility .....	305
Out-of-the-box Life Cycle Templates .....	306
Working with Life Cycle Templates .....	310
Promotion Process .....	326
Overriding and Reassigning Life Cycle and Team Templates .....	329
Defining Additional Life Cycle States .....	330
Access Control for Life Cycle Administration .....	330
Best Practices .....	330

Life cycles define the way in which these business objects mature, providing a model for the commercialization process.

Business information and objects become more mature throughout the product development cycle. During this cycle, circumstances change, such as who can access data, what processes are related, and where an object can mature to next.

A Windchill user in the life cycle administrator role can create a variety of life cycles. These life cycles define the states and transitions associated with various business objects and the available transitions between those states.

For more information about using the Life Cycle Template Administration utility, see the life cycle help.

---

## The Life Cycle Model

A life cycle is an automated, graphical model, employing phases and gates, used to manage business objects as they progress from conceptualization through obsolescence.

While an object is in a specific life cycle phase, certain business rules apply, such as access control rules or a specific workflow defined for that phase.

When created, an object modeled to be life cycle-managed enters a life cycle phase, where it is assigned an initial state, and is then associated with the initial phase of its life cycle.

## Windchill Solutions

Object initialization rules are used to designate to which life cycle an object type is assigned when a user creates a new object of that type. Workflows associated with an object manage the maturing processes from state to state through workflow activity templates. When new versions of an object are created through the **Revise** action, the team and the life cycle is assigned to the object following the same rules as when the object was created, and the life cycle state is set to the first state of the life cycle.

Depending on several business environment considerations (impact of change, development team, maturity of object, type of object, and so forth), it may be important to tailor the life cycle to include certain business operations and to define how these operations are executed. Transition rules tailor how Change Management, Revise, Promotion, and Set State operations should behave and which workflow processes you should use to manage these processes.

## Life Cycle States

The sophistication of business processes to manage an object depends upon the maturity of the object. State is an enterprise object, and its meaning is applied regardless of the life cycle by which a given object was processed. For example, if an access control rule applies to a Requirements object in the Under Review state, the rule is applicable to all Requirements objects in that state, even if they arrived at the state through different life cycles. However, each phase of a life cycle must be associated with a life cycle state chosen from among all states defined in the system.

---

 **Note**

If the domain policy access control rule denies access to a user and if an ad hoc access control rule grants the user access, then the ad-hoc policy is used, that is, the user is granted access. Ad hoc policies overrule and can provide access to a user where the domain policy denied it. For more information, see the access control section of the *PTC Windchill Specialized Administration Guide*.

---

As a life cycle administrator, you can create a variety of life cycles. These life cycles, which are stored in the System folder, define the phases and gates associated with various business objects. For the life cycle of each object, you can define the transitions through which the object must move, and the behavior associated with the object while it is in a specific state.

Windchill provides a Default life cycle, with many predefined states, such as In Work, Under Review, and Released.

Before you begin creating life cycles, you should understand life cycle iteration and life cycle roles.

## Basic and Advanced Life Cycles

Windchill supports two types of life cycles: basic and advanced. There are major differences between the basic and advanced life cycle that are visible to the user. The main differences are in the setup of the team definitions for an object, in the workflow processes for managed objects, and in the system performance when creating and revising objects. Using basic life cycles provides improved performance for core creation and revise operations.

You can designate whether the life cycle includes certain aspects of a life cycle definition. This is especially useful for team definitions and the use of workflow processes in Windchill.

When you create a basic life cycle, only the life cycle template, state, and transitions are defined. When you create an advanced life cycle, extra capabilities can be defined including phase information, team, and workflow processes.

---

 **Note**

PTC recommends that you use the basic life cycle for improved performance and scalability.

---

---

Any particular context could have a mix of basic and advanced life cycles associated with objects. Ideally, an object is associated with an advanced life cycle only when necessary, such as when you route an object in Windchill ProjectLink.

Any time you need to manage access via life cycle team roles and to drive an object through its life cycle states by a workflow process, use an advanced life cycle.

## Basic Life Cycles

When you create a basic life cycle, you define the following:

- The life cycle properties, including name, location, an optional description, the object classes to which the life cycle applies, and whether the life cycle is enabled.
- Phases and gates that define the life cycle.
- Transitions to be defined from the current (selected) state to any defined state within the life cycle template.

The basic life cycle is designed to use the context team defined in any application context. A basic life cycle does not include workflow process definitions and relies on the workflow process definitions with change management, routing, or promotion processes. Use this type of life cycle for most Windchill objects because the basic life cycle provides improved performance during the creation and revision of objects.

When you create an object with a basic life cycle and select a team template, the selection of the team has no effect. Basic life cycles do not utilize teams or workflows.


## Advanced Life Cycles

When you create an advanced life cycle, you define the following:

- The life cycle properties, including name, location, an optional description, the object classes to which the life cycle applies, and whether the life cycle is enabled.
- Phases and gates that define the life cycle.
- Roles, such as Reviewer or Workflow Assignee, for each life cycle phase. These roles can be mapped directly to users or user-defined groups, but are most often mapped to team roles or actors.
- Access permissions for the role players associated with each life cycle phase.
- Workflow processes to be associated with each phase and gate.
- Transitions to be defined from the current (selected) state to any defined state within the life cycle template.

---

 **Note**

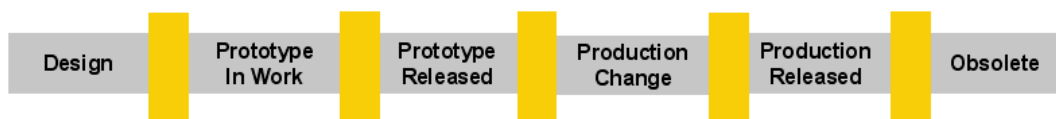
An advanced life cycle is denoted by  in the Life Cycle Template Administration utility.

---

The advanced life cycle type provides the ability for a separate team to be assigned for instances of this object type and to include workflow process definitions within the life cycle states to manage the maturing of the object type. Use this type for managing objects that require company-specific business processes, special access control requirements, or additional flexibility in managing these types of objects.

## Managing Life Cycle Processes

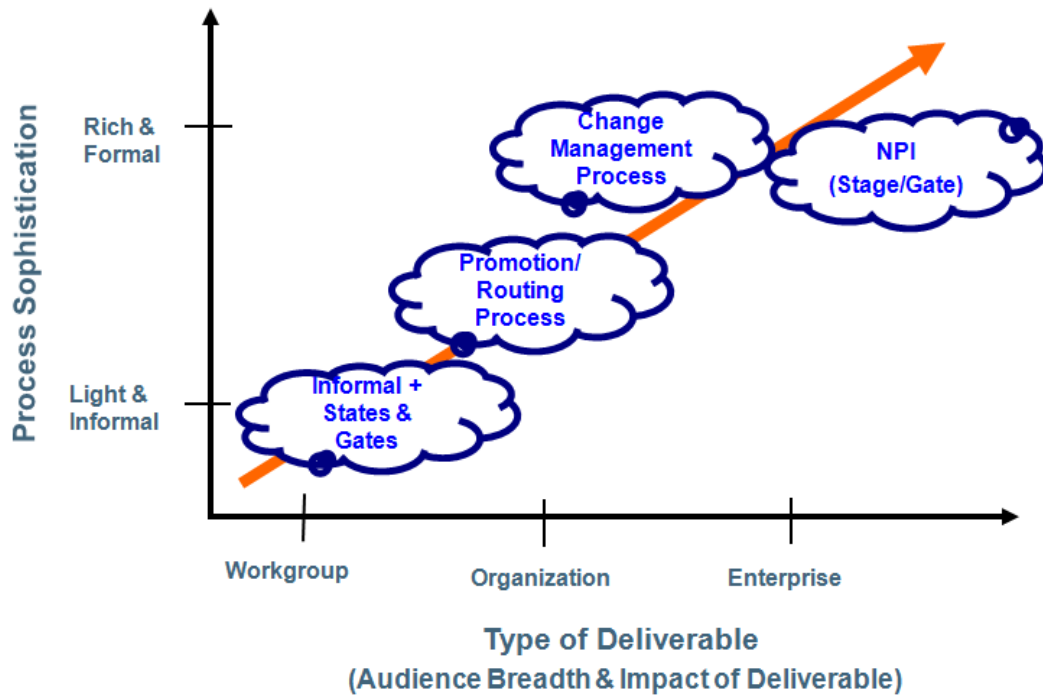
In Windchill, the life cycle is the core capability to manage an object's maturity (referred to as a life cycle state) as well as access control policies to manage or view the object for a set of roles in the system. Each object type in a Windchill system can have unique sets of life cycle states and access control policies. Object initiation rules are used to designate which life cycle an object is assigned when a user creates a new object of that type. Workflows can be used to manage the maturing processes from state to state through workflow activity templates. By default, when new versions of an object are created through the **Revise** action, the life cycle state is set to the first state of the life cycle. A life cycle administrator can specify the target state of the **Revise** action.



Depending on several business environment considerations (impact of change, development team, maturity of object, type of object, and so forth), it may be important to tailor the life cycle to include certain business operations and to define how these operations are executed.

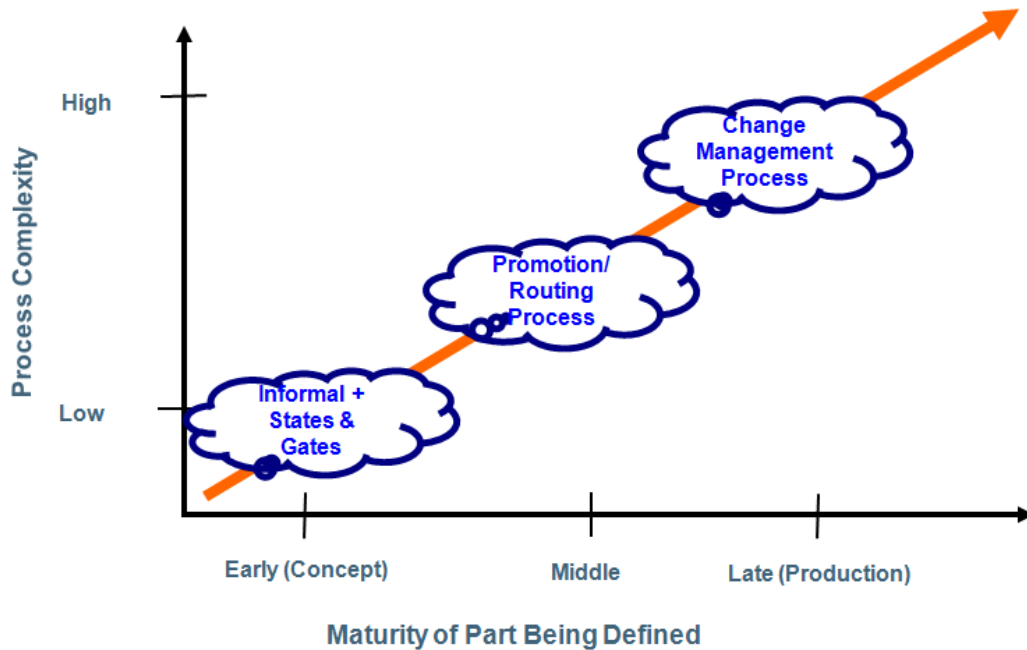
For example, a development team in the automotive division of a company can have different review processes for releasing a design specification than the industrial products division. The automotive division may require a prototype to be created for a new product before the first production versions of the product are released. Formal change processes are required to update these prototype designs. After a part has been initially released to production, new versions of the design are designated as Production Change, and they must undergo a formal change process.

The following figure is an example of the variety of business processes that can be used with a Windchill system to mature different types of product development deliverables. The development team processes for the review and release of a design specification can differ from those required for the release of a new configuration of the product.





The next figure illustrates a case when a combination of the business processes is required for some product development deliverable objects, such as parts, as they move from a concept, through prototyping, and into production.








Windchill PDMLink supports the following business processes that you can use to manage the life cycle of a part, document, or CAD document. You can use transition rules to control when in the life cycle this operation is available. For example:


- Set State - Enables you to informally set the life cycle state of an object.
- Promote - Enables you to set the state of one or more objects to a new life cycle state as part of a review process.
- Change - Enables you to execute a change order for a product development object.
- Revise - Enables you to create a new version of the object.



For more information on transition rules, see [Transition Rules on page 314](#).

## Accessing the Life Cycle Template Administration Utility

Life cycle templates are created and managed from the Life Cycle Template Administration utility. You can access the utility by clicking the **Life Cycle Template Administration** link on the **Utilities** page available from **Site** , **Organizations** , **Products** , or **Libraries** .

The **Life Cycle Template Administration** link from the **Site**  ► **Utilities** page provides the site administrator with unrestricted access to all life cycles. From the **Site** tab, you see only life cycle templates that have been created in the site context and those provided out-of-the-box.

From the **Organizations**  ► **Utilities** page, you see life cycle templates created in the site context and those that are in the organization context from which the Life Cycle Template Administration utility is launched.

The link from the **Products**  ► **Utilities** and **Libraries**  ► **Utilities** pages provide access to the life cycle templates created in the site and the organization contexts and those that are in the active context (Product or Library) from which the Life Cycle Template Administration utility is launched.

## Out-of-the-box Life Cycle Templates

The following out-of-the-box life cycle templates are identified as basic or advanced.

Basic Life Cycle Templates	Advanced Life Cycle Templates
Action Item	Approval Routing
Agreement	Change Activity Life Cycle
Approval	Change Notice Life Cycle
Basic	Change Proposal Life Cycle
Interference Report	Change Request Life Cycle
Interference	Default
Library Development	Notify Routing
Notify	Package Approval Routing
One Phase Development	Package Content Routing
Release	Package Delivery Routing
Requirement	Part Request Life Cycle
Review	Problem Report Life Cycle
Two Phase Development	Promotion Request
	Release Routing
	Review Routing
	Technical Data Package Approval Routing
	Technical Data Package Content Routing
	Technical Data Package Delivery Routing

Basic Life Cycle Templates	Advanced Life Cycle Templates
	Two Level Approval Routing
	Variance Life Cycle

## Windchill PDMLink

The following Windchill PDMLink out-of-the-box life cycle templates are basic life cycles:

- Basic
- Library Development



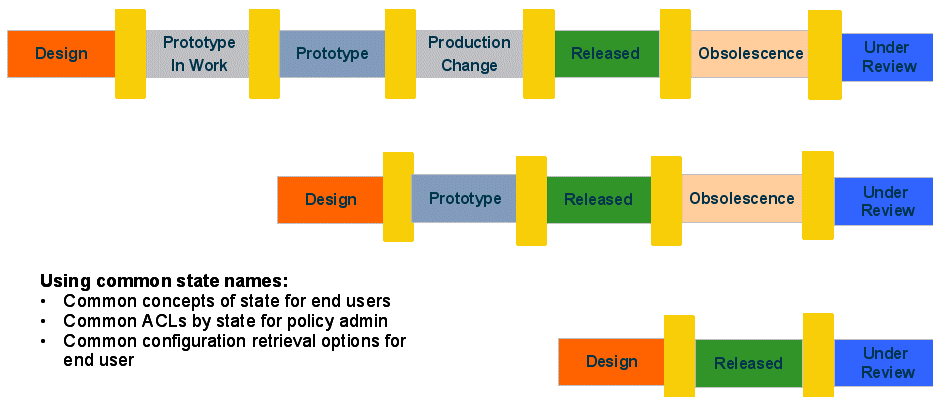
- One Phase Development



- Two Phase Development



The following figure shows the states that the three basic life cycle templates have in common.



**Using common state names:**

- Common concepts of state for end users
- Common ACLs by state for policy admin
- Common configuration retrieval options for end user

The following Windchill PDMLink life cycle templates are advanced:

- Change Activity Life Cycle
- Change Notice Life Cycle

- Change Proposal Life Cycle
- Change Request Life Cycle
- Default
- Package Approval Routing
- Package Content Routing
- Package Delivery Routing
- Problem Report Life Cycle
- Promotion Request
- Technical Data Package Approval Routing
- Technical Data Package Content Routing
- Technical Data Package Delivery Routing
- Variance Life Cycle

## Using the Product Design Template

The out-of-the-box Product Design template that is available in Windchill PDMLink establishes life cycle templates that are complete with transition rules and workflow processes for business objects; it uses the One Phase Development and Two Phase Development templates. Remember, the Product Design template should be used as an example. Your site should determine how to use transition rules and workflow processes, and set up default life cycles for the site, not just at a particular product level. For more information on the Product Design template, see [Product Design Template on page 183](#).

## Access Control for Parts Established Through the Product Design Template

The Product Design template also establishes access control policy rules for business objects. The following table shows the access control lists (ACLs) for parts as established in the Product Design template.

System Group	Design	Proto-type In Work	Proto-type	Produc-tion Change	Released	Obsolete	Under Review
Confirmed Members	No Access	No Access	Read	No Access	Read	Read	Read
Marketing	No Access	Read	Read	Read	Read	Read	Read
Procurement Engineer	No Access	Read	Read	Read	Read	Read	Read
Quality Engineer	No Access	Read	Read	Read	Read	Read	Read
Designer	Read Create	Read Modify	Read Modify	Read Modify	Read Revise	Read	Read

System Group	Design	Proto- type In Work	Proto- type	Produc- tion Change	Released	Obsolete	Under Review
	Modify Delete Revise NVV <sup>1</sup>	Delete Revise NVV	Delete Revise NVV	Delete Revise NVV	NVV		
Manufacturing Engineer	Read	Read	Read	Read	Read	Read	Read
Design Team Leader	Read Create Modify Delete Revise NVV	Read Modify Delete Revise NVV	Read Modify Delete Revise NVV	Read Modify Delete Revise NVV	Read Revise NVV	Read	Read
Product Manager	Full	Full	Full	Full	Full	Full	Full

1. NVV is New View Version.

For more information about the access control settings in the Product Design template, see [Product Design Template on page 183](#).

## Windchill ProjectLink

The following out-of-the-box Windchill ProjectLink life cycle templates are basic:

- Action Item
- Approval
- Basic
- Notify
- Release
- Review

The following Windchill ProjectLink life cycle templates are advanced:

- Approval Routing
- Default
- Notify Routing
- Release Routing
- Review Routing
- Two Level Approval Routing

---

## Security Labels and Agreements

Out of the box, the Agreement basic life cycle template is available. When security labels and agreements are enabled, this template can be applied to the agreement object. For more information, see the agreements help.

## Working with Life Cycle Templates

The **Life Cycle Template Administration** utility displays a list of existing life cycle templates and their locations. Using the buttons on this page you can create, edit, view, and delete life cycles. You can also import and export life cycles, among other functions.

You can sort the templates list in ascending and descending order by clicking on a column header.

From the **Life Cycle Template Administration** utility, you can create a new life cycle or edit an existing one:

- Click **New** to open the **Create Life Cycle** window.
- Click **Edit** to open the **Edit Life Cycle** window.

Editing uses essentially the same procedures as creating a new template, but you modify information, rather than creating a new template. When you edit a life cycle, it is automatically checked out.

You must have the necessary access permissions to create or edit a life cycle. If you do not have the required permissions, the **New** and **Edit** buttons are enabled, but you get an error message when you try the operation. For the necessary access control permissions, see [Access Control for Life Cycle Administration on page 330](#).

When you create a life cycle, you define the following:

- The properties of the life cycle, including name, location, the object types to which the life cycle applies, and whether the life cycle is enabled. (See [Life Cycle Properties on page 311](#).)
- Phases and gates defining the life cycle. (See [Defining Life Cycle Phases and Gates on page 313](#).)
- Transition rules to help determine the path from the selected state to any other state within the life cycle template. (See [Example of Defined Transitions on page 317](#).)

---

In addition, the following are defined for advanced life cycles only:

- Roles, such as Submitter or Promoter, for each life cycle phase. These roles are mapped to users, user-defined groups, organizations, actors, or other roles.
- Access permissions for the roles associated with each life cycle phase. (See [Life Cycle Access Control Rules on page 322.](#))
- Workflow processes to be associated with each phase and gate. (See [Associating a Workflow Process with Phases and Gates on page 323.](#))

Life cycle templates may be moved if the following conditions are met:

- The life cycle template must be checked in.
- There must be a higher level context in the hierarchy than the one in which the life cycle template currently resides.
- The name of the life cycle template must be unique in the target context.
- If there is a workflow template attached, the workflow template must be at a higher context level than the life cycle template. The workflow template may be either at the same context level to which the life cycle template is moving or at a higher context level.

For more information on moving life cycle templates, see the life cycle help.

You can view the iteration history of a life cycle from the **Life Cycle Template Administration** utility.

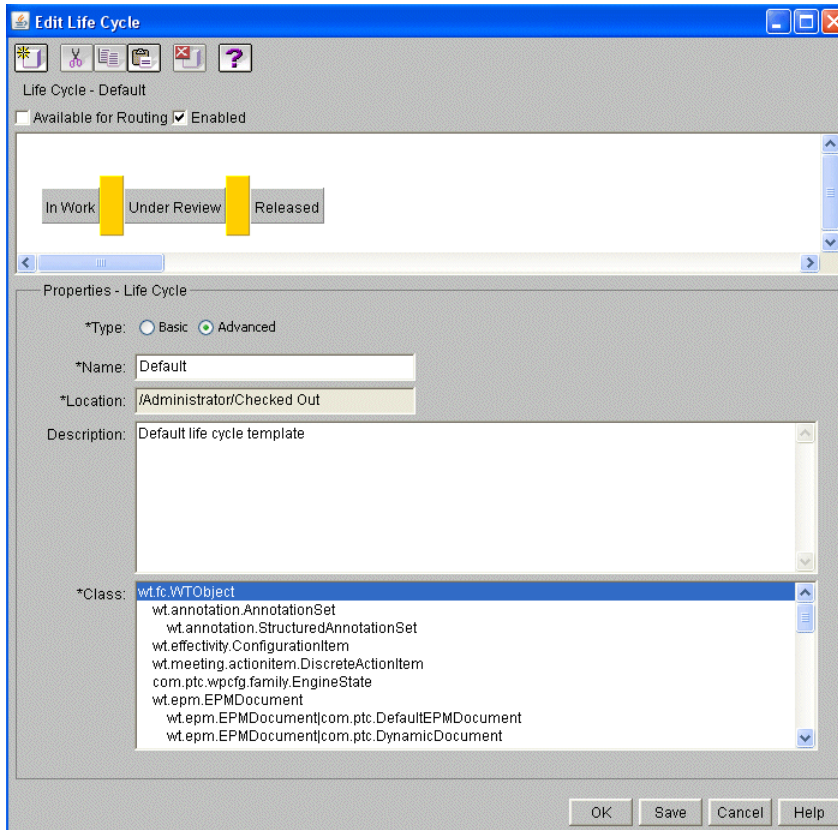
Select a life cycle template on the **Life Cycle Template Administration** utility navigation panel and then click **Iteration History**. A list of all the life cycle iterations appear with the date and time of last modification, and the name of the modifier. Select any iteration, and click **View** to view the life cycle.

## Life Cycle Properties

The properties of a life cycle template are available when viewing or editing a life cycle template. The upper half of the screen displays a graphical view of the life cycle's phases and gates while the **Properties** panel appears in the lower half of the screen. When no phases are selected, the **Properties** panel shows properties of the entire life cycle. These properties include the life cycle name, type, location, description, class, enabled status, and routing availability.

For more information about life cycle properties, see the life cycle help.

The following figure displays the **Edit Life Cycle** window, with the Default life cycle and its properties displayed:



The **Class** display in the example above provides a tree view of all object types subject to life cycle management. You must choose the type to which this life cycle applies. Because Windchill types are hierarchical, the life cycle is applicable to the selected type and all of its subtypes. A type can inherit more than one life cycle; you can directly associate a life cycle with a given subtype. For example, you could associate a life cycle with the type `WTObject`, and all its subtypes would also be associated with that life cycle. You could also associate those subtypes (for example a change request, `WTChangeRequest2`) with other life cycles.

When users create objects that are subject to a life cycle, a life cycle must be selected as part of the creation process. The list of selectable life cycles is dependent on what has been defined in the object initialization rules for the selected type. If the user does not have create permission based on the initial state of a life cycle, that life cycle will be filtered out of the list.



---

## Defining Life Cycle Phases and Gates

The properties of a life cycle phase are available when the phase is selected when viewing, creating, or editing a life cycle template. Available properties and tabs will vary if the life cycle is basic or advanced. For all life cycles, the following properties are defined:

- State

Windchill provides predefined states (for example, In Work and Under Review). You can define additional states by adding them to the StateRB.rbInfo resource file. For more information, see [Defining Additional Life Cycle States on page 330](#).

- Version Series

Options include Mil Std and Numeric. For more information, see [State-based Revision Sequences by Life Cycle State on page 313](#).

- Transitions

There are multiple transitions available out-of-the-box. You can define additional transitions by adding them to the TransitionRB.rbInfo resource file as described in the *PTC Windchill Customization Guide*. This resource file is located in the `<Windchill>/src/wt/lifecycle` directory.

For advanced life cycles, the following properties are also defined:

- Roles
- Access Control
- Workflow

For more information, see the life cycle help.

### State-based Revision Sequences by Life Cycle State

The versioning schemes for Windchill PDMLink are identified based on the object type through object initialization rules.

For a specific object type, such as a part or document subtype, each object type can use a specific version scheme referenced by a scheme name.

These version schemes are then identified in an XML file. For example, the out-of-the-box XML file loaded with Windchill PDMLink is:

```
StateBasedVersioning.xml
```

This file contains the sequences and seeds (for example, NUMERIC and MILSTD).

---

## Note

To change version schemes, do not manually modify the XML file; instead, use the steps to load an updated XML file described in *Setting Up a File-based or State-based Versioning Scheme* in the *PTC Windchill Specialized Administration Guide*.

---

For information on setting up the state-based versioning scheme that corresponds with the **Version Series** drop-down list that is available for each state, see [Administering the Versioning of Parts, Documents, and CAD Documents](#) on page 105.

## Transition Rules

The **Transitions** tab available when creating or editing a life cycle template allows you to define transition paths from the selected state to any other state within the life cycle template.

Life cycle transition rules provide capabilities for defining some behaviors of an object. These rules apply to the following actions in Windchill PDMLink:

- **Change** - Enables you to execute a change order for a product development object. In particular, the Change transition identifies the state to which an object is released from a given state.
- **Lock** - Enables you to identify a temporary state in which an object resides only while the promotion process is being executed: at the end of the process, the object either promoted to a specified state or returned to its original state. Typically, the state identified by a Lock transition specifies restricted access for modification. Lock transitions are always optional.
- **Promote** - Enables you to set the state of one or more objects to a new life cycle state as part of a review process. Transition rules can be used to control when in the life cycle this operation is available.
- **Revise** - Enables you to specify the initial life cycle state of a new version of the object. Transition rules can be set up to control the life cycle state of the new version based on the state of the version being revised. Additionally, rules can be set up for a life cycle state to use a new version sequence when the Revise action occurs.
- **Set State** - Enables you to informally set the life cycle state of an object. Set state is an extension of the administrative set state function to users without administrative privilege. The user must have create permission for the promotion request in the context in question.

---

 **Note**

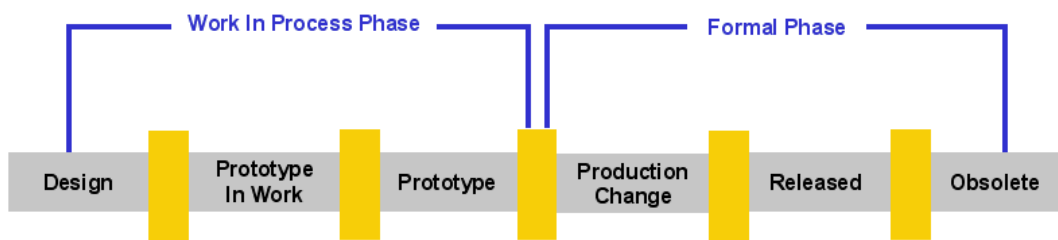
To perform a set state operation, a participant must have the Set State permission and there must be a valid state transition defined between the current state and the desired state. If there is no transition defined, the participant must have the Administrative permission to perform the operation.

For information about the Set State action and the permissions required, see Planning Object State Change Policies in the PTC Windchill Help Center.

---

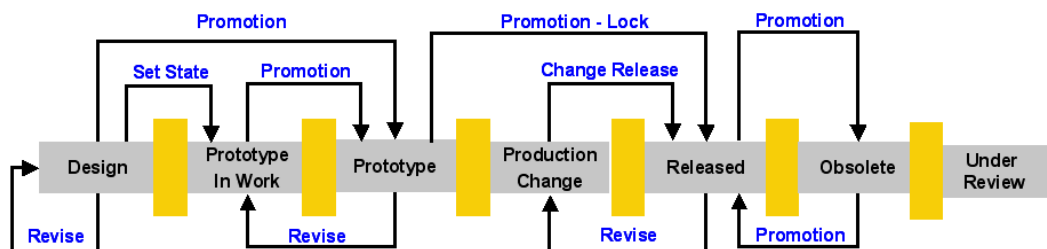
- Refine - Enables you to set the state of objects undergoing rework or being refined. This transition is not used out-of-the-box, but may be used in a custom workflow.
- Review - Enables you to set the state of objects progressing through a review process. This transition is not used out-of-the-box, but may be used in a custom workflow.

Using a set of transition rules, you can define appropriate sets of business processes for the stage of development for an object. For example, the processes for developing a part can be informal in the early stages of development, but will require more formal processes if the part is introduced into production.



Using transition rules, you can set up a variety of business processes to be available for each type of object in a Windchill PDMLink system.

The following diagram is an example of how these rules can be applied to a life cycle.



Some business practices require more formal processes, such as review and approval cycles. The Promotion and Change transition rules have associated workflows for that purpose. By default, the promotion transition rule has two workflow processes defined. Depending on your business practices, zero or more workflow processes can be configured for use with a specific promotion process.

For some promotion review processes, it is important to freeze or lock the promotion objects, so that no changes are made during the review process. For the example life cycle above, the lock transition can be added to set the objects to the Under Review state during a promotion process.

For change management processes, the new life cycle state for approved change notice is now defined by the Change transition and is no longer fixed to one specific life cycle state.

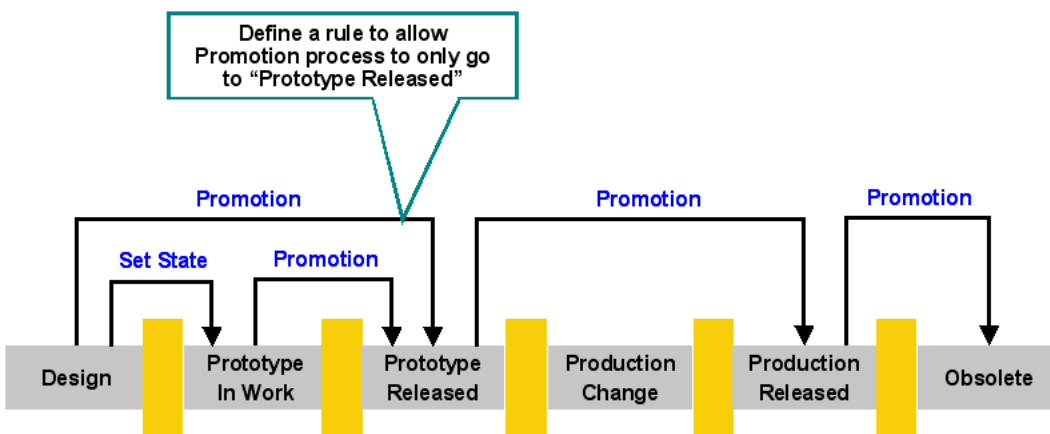
These transition rules are defined for each life cycle.

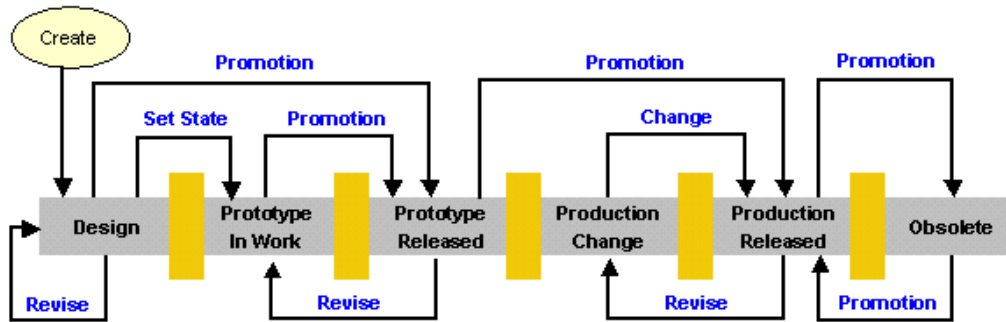
Transition rules may also identify whether the objects are locked during Promotion reviews. The object resides temporarily in the locked state while the promotion process executes. If a lock transition is defined for a particular state and an object using the life cycle is designated for promotion on a promotion request, the workflow of the promotion request sets the state of the object into the state identified with the lock transition.

Suppose your life cycle model looked like this:



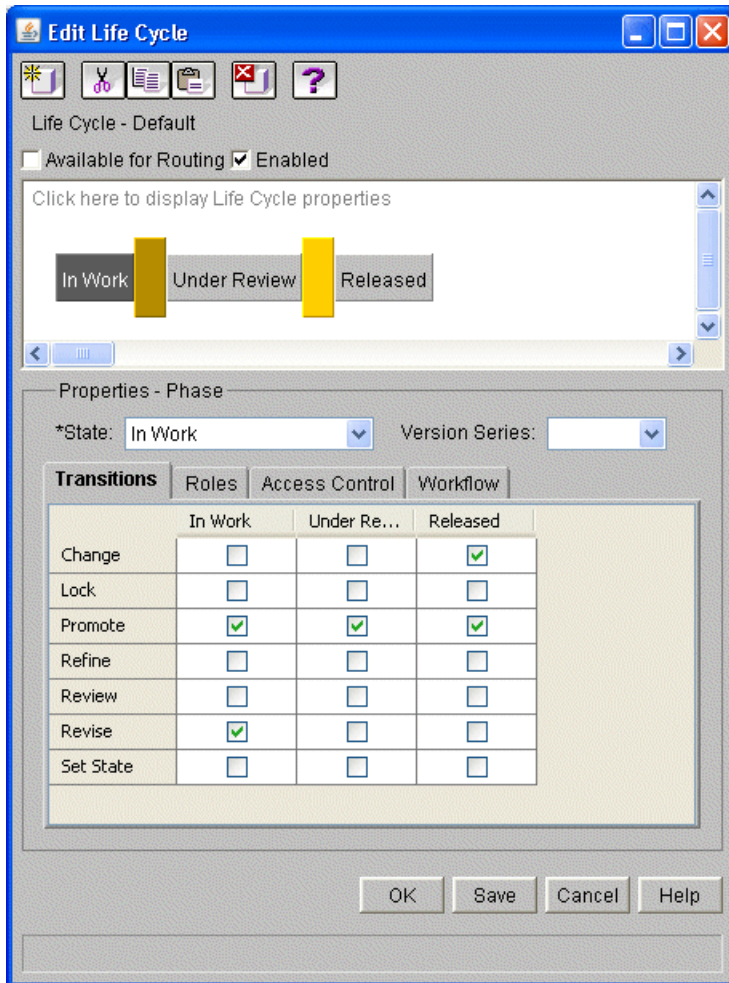
You determine that you want to establish transition rules:





### Example of Defined Transitions

A transition is a named path from a source phase to a destination phase in a given life cycle. In this figure, **In Work** is the source phase. The table of check boxes indicates to which destination states there are particular transitions.



For example, the check in the first column of the third row means that there is a Promote transition from **In Work** to **In Work**. This is an example of a reflexive transition, where the source and destination phases are the same.

Similarly, the check in the third column of the first row means that there is a Change transition from **In Work** to **Released**.

The defined transitions shown in this figure are:

- In Work – Change to Released
- In Work – Promote to In Work
- In Work – Promote to Under Review
- In Work – Promote to Released
- In Work – Revise to In Work

These are not all the transitions for the entire life cycle, but only for those with **In Work** as a source phases. Other transitions are viewed by activating the **Transitions** tab when other source phases are selected.

---

## Transition Defaults

Life cycle transition defaults are applied whenever a life cycle is saved (either interactively or via a bulk load) or is upgraded and does not otherwise contain explicit transition information.

Default transitions are initialized according to a specification recorded in the wt.properties file. The specification is encoded using a small language, whose grammar is given (beginning with a valid wt.properties entry):

```
wt.lifecycle.transitions.default.<transition_name>=<expression_list>
transition_name = { key element of wt.lifecycle.Transition }
expression_list = expression ["," expression_list]
expression = term ["|" expression]
term = "ALL" | "FIRST" | "LAST" | state_name
state_name = "\"" { key element of wt.lifecycle.State } "\""
```

Each property entry specifies a rule for creating default instances of a particular transition type in each life cycle. The rule is applied to a state in a life cycle. Every expression in the *expression\_list* is evaluated to create transitions to the specified states. However, each *term* in the *expression* is evaluated in order of appearance only until one is encountered that validly specifies one or more states; the remaining terms in the expression are ignored.

The out-of-the-box default transition expressions are:

```
wt.lifecycle.transitions.default.PROMOTE=ALL

wt.lifecycle.transitions.default.CHANGE="RELEASED"

wt.lifecycle.transitions.default.REVISE=FIRST
```

These rules can be interpreted as follows:

- **PROMOTE**: create a PROMOTE transition from each state to all other states in every life cycle.
- **CHANGE**: create a CHANGE transition from each state to the RELEASED state in every life cycle. If the life cycle does not have a RELEASED state, no transition is defined.
- **REVISE**: create a REVISE transition from each state to the first state in every life cycle.

---

## Role Mappings

Advanced life cycles can have a role associated with a particular life cycle phase. When an object is promoted to the phase in the life cycle, the role is assigned to a participant (user, group, or organization). A role mapping is resolved in one of several ways:

- You can directly map life cycle roles to users, user-defined groups, organizations, or other roles. However, since organizations generally want to define only a small number of life cycles, it is not often practical to map life cycle roles directly to participants. Using life cycles and teams together allows role participants to be identified when the phase is reached, rather than making this mapping an explicit part of the life cycle definition.
- You can map life cycle roles to team roles. When the phase is reached, the role is resolved according to the team role mapping. For example, the life cycle role Promoter could be mapped to the team role Team Leader, and the life cycle role Promoter would be resolved at runtime according to the Team Leader role, as mapped in the team.
- You can map a life cycle role to an actor. That is, you can map a role to someone who performs a specific action within the context of the business object. When the phase is reached, this role is then resolved to the participant who created the object with which the life cycle is associated. For example, you could assign the Creator actor to the Submitter role for a given life cycle phase. For that phase, the user who created the object would be assigned the Submitter role at runtime. If the Submitter role is defined in the team, it resolves to the team's Submitter role.

## Associating Life Cycles with Object Types

You can associate object types with life cycles using object initialization rules.

For more information about using object initialization rules to set an object's life cycle, see the object initialization rules help.



---

 **Note**

If you create a type and associate it with a default routing life cycle, there may be problems when users create documents using templates created with the type. The default routing life cycles start automatically, so when the user tries to create from a template using one of these life cycles and selects the **Check Out and Download** action, the checkout and set state (life cycle) gets caught in a race condition. This can cause two outcomes:

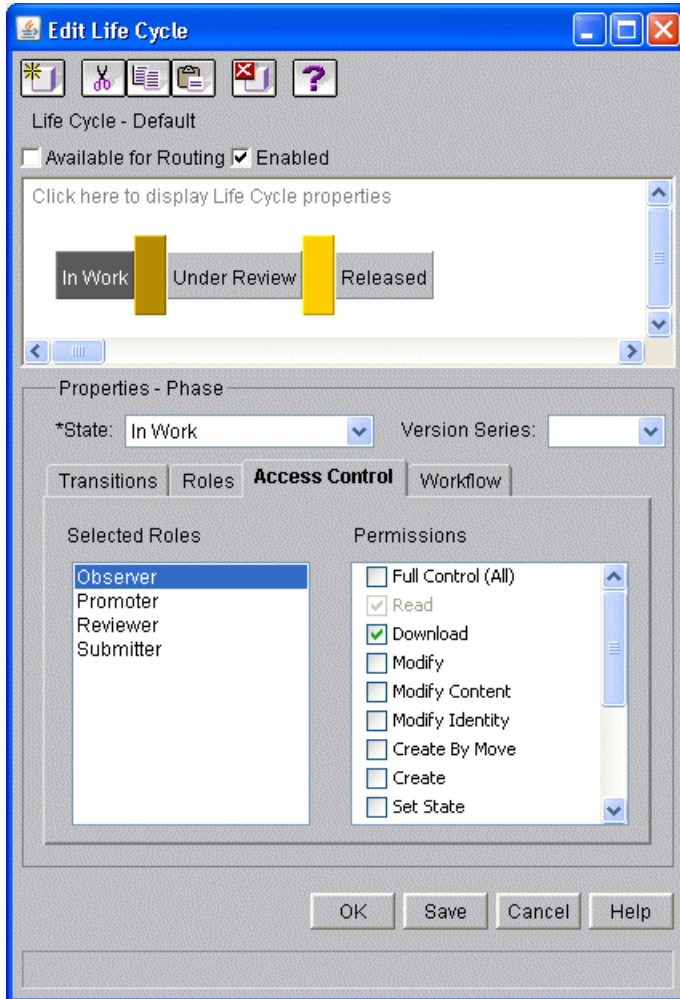
- The set state fails; the user has a checked-out document that is In Work, and the life cycle does not happen.
- The set state succeeds and the user has a checked-out, newly-created document that has been immediately routed for review.

PTC recommends you create your own routing life cycle that would contain a specific Submit task later in the process, not an automatic Submit upon creation.

---

## Life Cycle Access Control Rules

The **Access Control** tab is available when viewing the properties for a phase:



This functionality is only available for advanced life cycle templates.

When creating or editing an advanced life cycle template, you can specify ad hoc access control rules that apply to the object when it is in the selected life cycle phase. When the object moves to the next state, these permissions might change.

- Out-of-the-box roles are automatically given **Read** permission. This is necessary to allow the associated participants to access their tasks and view the object.
- The **Submitter** role is also given **Modify** permission by default. This allows submitters to submit the object for promotion as part of the edit process.

---

 **Note**

New roles and custom roles created at your site are not given default **Read** permission. You must manually configure the permission of new roles.

---

For each role, you can also select one or more of the permissions described in the access control section of the *PTC Windchill Specialized Administration Guide*.

For more information about using the **Access Control** tab, see the life cycle help. For more information about access control, see the access control section of the *PTC Windchill Specialized Administration Guide*.

## Associating a Workflow Process with Phases and Gates

---

 **Note**

This section applies only to advanced life cycle templates.

---

By default, all advanced life cycles have predefined workflow processes associated with the phases and gates.

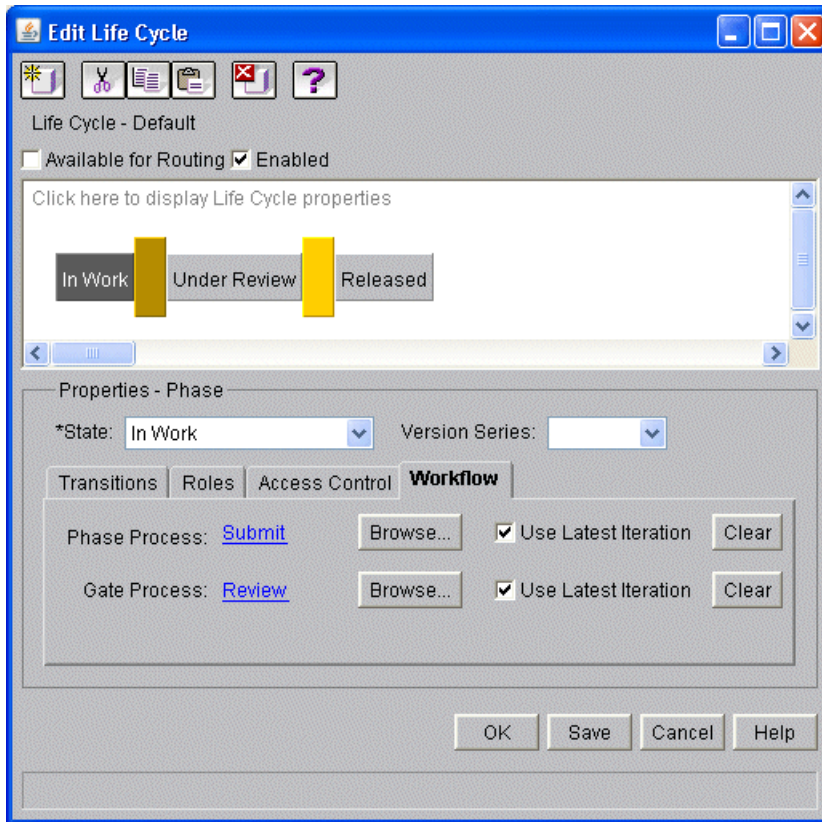
When a business object reaches a specific state, the workflow process associated with that state will be automatically initiated and the business object will be forwarded through the workflow process.

The workflow process that moves objects through the associated phases and gates is separate from the life cycle of the object. You can manage one or more objects with a workflow process.

To change the workflow process that is associated with a phase or a gate, modify the following properties in the `wt.properties` file:

- `wt.lifecycle.defaultPhaseProcess`
- `wt.lifecycle.defaultGateProcess`

As shown in the following figure, the Submit process is automatically associated with the In Work phase. The Review process is associated with the gate by which an object moves from In Work to its next phase.



**Note**

**Use Latest Iteration** is selected, so the most recent iteration of the workflow process template is used at instantiation. If this check box is cleared, the specific iteration selected is used, even if it is not the most recent.

---

As a result, the Review workflow, which is shown in the following Workflow Process Editor figure, defines the process and activities that are part of moving an object forward from the In Work phase.



This workflow process has three defined activities: Review, Observe, and Promote. You can view the properties of each link and activity within the process by clicking on the node or hyperlink associated with each link or activity. For example, for the Review workflow, the participant to be assigned the Review task is the Reviewer role.

Therefore, when an object is submitted for promotion from the In Work phase and the Review workflow process is started, the Reviewer role is mapped to an actual user, based on role mappings in either the life cycle or a team template. The Review task is added to the **My Tasks** table for the user.

The Submit and Review workflow processes are predefined and available for your use when Windchill is installed; however, your organization may have a number of additional workflow processes in place. To associate a specific workflow process with a phase or gate, click **Browse** to locate and select a process from the shared location.

## About Life Cycle Iteration

Working with life cycles is an iterative process. Like version-controlled objects, iterated objects are checked in to and out of shared locations; however, unlike version-controlled objects, they cannot be revised. Instead, any change to an object creates a new and separate iteration when it is checked in. Earlier iterations, which may still be in use, are unchanged and unaffected by the new iteration. Only the latest iteration is available for new uses.

To make changes to a life cycle template, you must check out a copy. (Click **Edit** on the Life Cycle Template Administration utility to check out a copy of the selected life cycle.) While it is checked out, no one else can check out a copy, but the original can be viewed or selected to manage an object. When you have

---

completed changes to the checked-out copy, you must save it and check it in, so it is available to others. It then becomes the latest iteration. Objects that are being managed by an earlier iteration continue to be managed by that iteration. They are not affected by the newer iteration.

## Importing and Exporting Life Cycle Templates

Before you begin importing or exporting life cycles, you should be familiar with the following information:

- Upgrade to the latest maintenance only release (MOR) as it becomes available, to ensure you have the latest enhancements to the import and export functionality.
- You can import a life cycle into a later version of Windchill; but not to an earlier version. To import from an earlier version of Windchill, you must set the `wt.ixb.import.allowCrossReleaseImport` property in `wt.properties` to true.
- Importing or exporting life cycles creates objects in a JAR or ZIP file format. (This is the same format that the `load.Installer` functionality uses.)

For more information about how to import or export life cycle templates, see the life cycle help.

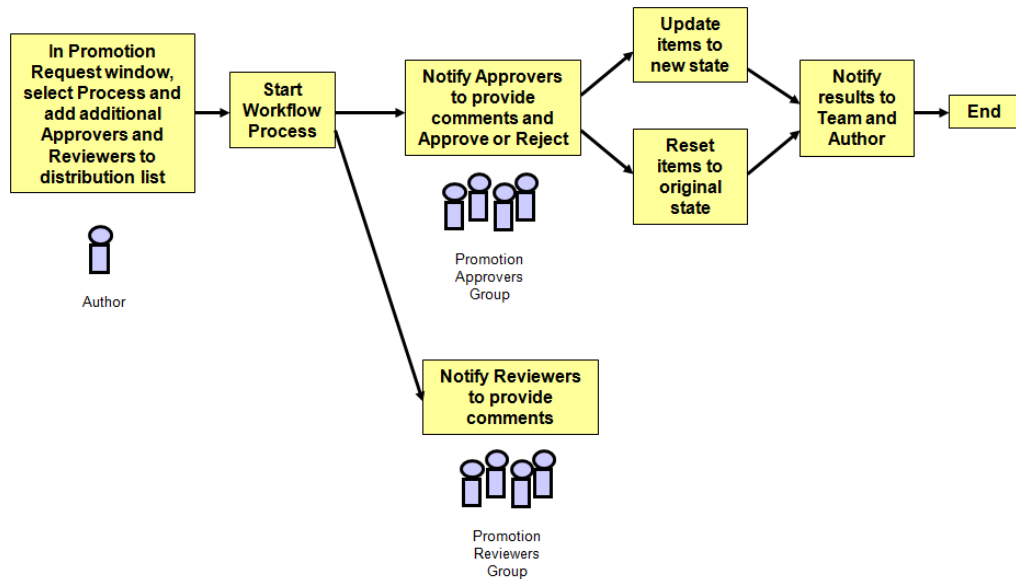
## Promotion Process

When you want to promote an object from one life cycle state to another, you can use two standard review and approve workflow processes within a life cycle template. With the enhancements to life cycle management, these two processes can be used to manage the development of CAD documents, parts, and documents.

The promotion request window guides a user requesting a promotion of one or more CAD documents, parts, and documents through the promotion process. The user can add dependents of parts and CAD documents to the request through this process. All objects requested for promotion must be set to the same target life cycle state. If the objects requested for promotion do not share any life cycle states, no promotion can be completed.

Two standard workflow processes for promotion are as follows:

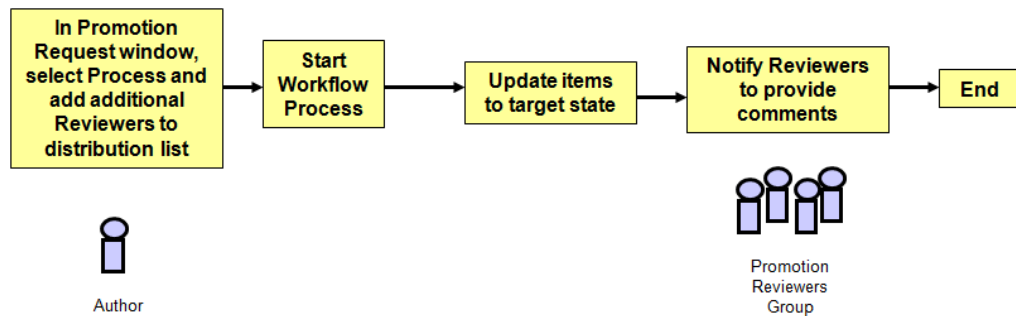
- **Promotion Request Approval Process** - A process to notify a set of Approvers to approve or reject the Promotion Request and invite a list of Reviewers to provide comments to the Promotion Request. If all Approvers approve the request, the objects in the promotion request are updated to the target life cycle state. Otherwise, these objects are returned to their original life cycle state.



- Promotion Request Review Process - A process to automatically set the state of promotion request objects to the target life cycle state and invite a list of Reviewers to provide comments on the promotion request.

#### Note

Users can set promotion candidates so that they revise automatically once the promotion request is approved. Refer to [About Automatic Revision on page 334](#) for details.



A list of Approvers who must approve the promotion request is defined by the Promotion Approvers system group for a product or library. A list of Reviewers, who are invited to provide comments to the objects under review, but do not approve the request, is defined by the Promotion Reviewers system group for that product or library. The user submitting the promotion request can also add (in the last step of the **Promotion Request** window) Approvers or Reviewers for each specific review through a list of users and user-defined groups for the product and library.

---

When a promotion request is created for one or more CAD documents, parts, and documents, the list of specific iterations of these objects is maintained in the baseline for this promotion request. Additionally, for a set of CAD documents on a promotion request, a set of viewables is generated for this baseline set, and it can be viewed directly from the promotion request task or from the promotion request form.

---

 **Note**





If you want to disable viewables from being generated in the promotion process, set the following property to FALSE: `publish.promote.enabled=false`.

---

## Out-of-the-Box Workflow Processes using the Promote Transition

Windchill PDMLink uses two out-of-the-box workflows which use the Promote transition; **Promotion Request Approval Process** and **Promotion Request Review Process**. For more information about these workflows, see [Promotion Process on page 326](#).

The **Default Promotion Processes** preference sets the default workflow processes that are used by the promotion process; initially, this is set to Promotion Request Approval Process and Promotion Request Review Process. These two workflow processes are presented for every promotion request; however, preferences may be configured to provide zero or more workflows to reflect business practices.

You can view and edit the preference value using the **Promotion Preference Management** utility from the **Utilities** page available from the **Products** , **Libraries** , **Organizations** , or **Site**  contexts.

---

 **Note**

The **Promotion Preference Management** utility is also used to manage new promotion preferences for use with custom promotion workflow processes. Only site administrators can create new promotion preferences. For more information, see the promotion requests help.

---



---

## Overriding and Reassigning Life Cycle and Team Templates

In Windchill PDMLink, during the creation of a part and a document, the life cycle template and the team template can be manually selected. It is also possible to reassign a life cycle and reset a team template on an existing part or document. In most cases, the manual selection can be done from either a drop-down list or through a search.

The life cycle drop-down list is automatically generated based on the object type being created and the class attribute value that is assigned in a life cycle template. A life cycle template contains an attribute that specifies for which class the life cycle is valid. The class attribute can be set to a value of an abstract class, a parent class, or a leaf node class.

Based on the object type being created, all enabled life cycle templates that have a class attribute value matching the selected object type being created, or a parent type, or an abstract class, will be included in the drop-down list.

Depending on the object type being created, the user may be able to search for any enabled life cycle template to which the user has access, independent of the life cycle templates class attribute value.

### Manual Selection of Life Cycle and Team Templates

The action to manually select the life cycle and the team template during the creation of a part and a document is available to users that have administrative privileges set on the object. For more information, see the access control section of the *PTC Windchill Specialized Administration Guide*.

### Reassigning Life Cycles and Resetting Team Templates

The action to reassign life cycle templates and reset team templates on existing parts and documents is only available in Windchill PDMLink. Users must have administrative privileges set on the object for either of these actions to be available. For more information, see the access control section of the *PTC Windchill Specialized Administration Guide*.

Additionally, resetting the team template is only available for objects with advanced life cycles.

---

## Defining Additional Life Cycle States

Windchill includes many predefined life cycle states and roles in the out-of-the-box life cycle templates. You can define additional states and roles by customizing the StateRB.rbInfo and RoleRB.rbInfo resource files as described in the *PTC Windchill Customization Guide*. These resource files are located in subdirectories under the `<Windchill>/src` directory. Newly defined states and roles are added to the existing states and roles when you recompile the resource files and deploy the class files to your production environment. For more information, see the enumerated types information in the *PTC Windchill Customization Guide*.

---

### Caution

Removing a value you previously added to an enumerated type (for example, removing a state in the StateRB.rbInfo resource file), could result in serious runtime error. Do not remove a state unless you are certain there is no reference to it within the system.

---

## Access Control for Life Cycle Administration

The access control rules listed in the following table provide life cycle administrators with permissions needed to manage life cycles and teams, and to move them after they have been created. These rules need to be defined for the domains (or ancestor domains) associated with folders in which life cycle templates and teams will reside.

Object Type	Permissions Required
AdministrativeDomain	Read
LifeCycleTemplate	Read, Modify, Create, and Delete
Team Template	Read, Modify, Create, and Delete
Cabinet	Read and Modify
SubFolder	Read and Modify
WTContainer	Read

## Best Practices

Site, organization, and application context managers manage life cycle templates.

- 
- Site administrators create, modify, delete, and view life cycle templates in the site context.
  - Organization administrators create, modify, delete, and view life cycle templates in the given organization context. Organization administrators can view life cycle templates from the site context.
  - Application context managers create, modify, delete, and view life cycle templates in the given application context. They can view life cycle templates from the parent organization context and the site context.

---

 **Note**

The Life Cycle Template Administration utility is not available to project or program application context managers.

---

The Life Cycle Template Administration utility displays a table that lists all life cycle templates belonging to the given context, in addition to those belonging to its parent contexts. A column in the table identifies the context owning each life cycle template.

When you create a life cycle template, the system saves the new life cycle template in the System cabinet or folder of the context in which it is created.

---

 **Note**

When assigning a workflow template to a life cycle template, you see a list of valid workflows. The list of valid workflow templates includes the ones defined in the current context, plus those defined in any parent contexts. Workflow templates defined in a sub-context override and filter out the workflow templates defined in parent contexts having the same name.

---

The search scope used to locate user-defined groups is determined by the type of administrator doing the search. For more information about the search scope, see [Searching for Participants in Administrative Clients on page 259](#).

## Life Cycle Support in Windchill ProjectLink

The following table shows the life cycle support in Windchill ProjectLink.

Feature	Support Level	Notes
Life cycle template definition	Full	Organization administrators may create, edit, move, and delete life cycles for their organization.
Life cycle-managed object support	Partial	Only document and part items are supported.
Phases	Full	
Gates	Full	
Default life cycles	Partial	The following default life cycles are supported out-of-the-box: Default, Basic, Approval, Review, and Release.
Workflow association	Full	Workflow templates must be defined in the organization and are available for reference at a life cycle phase or gate.
Roles	Partial	Roles must be defined in the project or program context.
Role-based access control	None	Access rules defined for objects in the project or program context take precedence. By default, members of the project or program manager group have full access to all objects in the project or the program. The life cycle access rules by role for each phase and gate are ADDITIVE. This means access rights can be added for each role only at each phase and gate.
Life cycle template import export	Partial	There is no organization association with the

Feature	Support Level	Notes
		imported or exported template so the life cycle import and export folder should be cleared between uses.
Access to current life cycle state	Partial	The life cycle state is provided on the information page for the object.
Set life cycle state	Full	Object owners and project managers can set the life cycle state for a document or part with the <b>Set State</b> action. For more information about overriding the life cycle state, see <a href="#">Overriding and Reassigning Life Cycle and Team Templates on page 329</a> .
Access to maturity history	None	The maturity history for a part or document is not available.
Queries based on life cycle state	None	
Access to running process through life cycle	None	

## Managing Promotion Processes in Windchill PDMLink

The decision to promote an object from one state to another often pertains to a business decision. As such, it is important to make sure that products and libraries are set up to allow for the proper approvals to be obtained prior to promotion. For more information, see [Understanding Products and Libraries on page 171](#).

For any process template used in the promotion process, users assigned to the particular tasks are obtained from the following:



- The process template itself (the process has a member defined for a specific task)
- The state of the life cycle of the promotion request
- The team instance of the promotion request

---

The out-of-the-box templates do not define users for the roles defined in the process templates or life cycle templates used by the promotion request.

The team template provided for the promotion request defines the roles Approver and Reviewer; however, no default users are assigned to these roles. The Approver and Reviewer roles should be populated by the context team. For more information, see the teams help.

If you are using a process template for the promotion process that defines roles in addition to Approver and Reviewer, add the roles to the team template used for promotion request creation. You can modify team templates through the **Team Administration** utility found on the **Utilities** page for each context. Create a copy of the team template (using the **Save As** functionality), edit the new template to add any new roles, and then modify the appropriate object initialization rule for the promotion request to point to the new team template in the appropriate context.

The primary method for allocating users to roles is by using the context team. You can find the team on the **Team** page of **Products**  or **Libraries** . Both out-of-the-box product templates define two context roles, Promotion Approvers and Promotion Reviewers, to work with the promotion process. These context team roles, along with role mapping, copy any users and user-defined groups from these roles into the team instance of the promotion request at creation. When a new product is created, the Promotion Approvers role is empty; any approval tasks are sent to the promotion request creator unless this role (or another mapping) is properly defined. For each product, resolve at least one user into the promotion request team instance for the Approver role to ensure that a proper approval is obtained prior to promotion. Out-of-the-box, this can be done in the following ways:

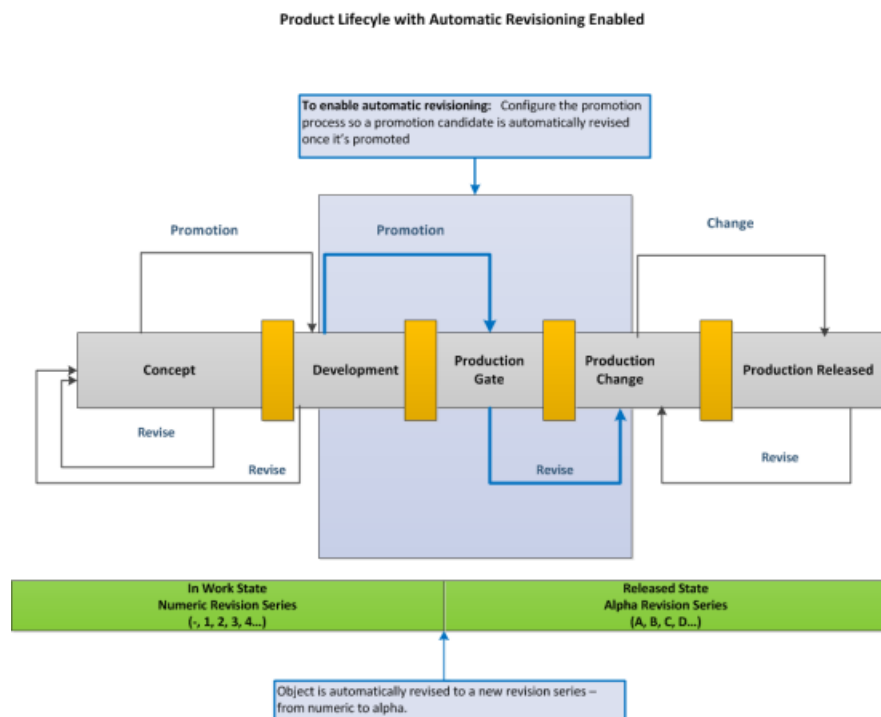
- Adding the approver to the Promotion Approvers role of the context team
- Modifying the team template to have a default participant for the Approver role
- Modifying the preference mapping to add additional roles for the Approver role, ensuring that at least one user is assigned to at least one of the roles in the context team.

## About Automatic Revision

Some companies use a gate review process when an object is moving into a production phase. A common practice is to change the revision scheme as part of this process. An object in a pre-production phase uses a numeric revision scheme and once in a production phase, the object uses an alpha revision scheme. A proper lifecycle design includes a gate state that can be modeled to achieve the desired target state. This automatically revises a promotion candidate to the initial revision for the new revision series.

Automatic revision states allow the automatic revisioning of promotion candidates based on a selected lifecycle states once the promotion request is approved. Companies can use the automatic revision mode to select a promotion process preference value. This enables a lifecycle transition that automatically revises an object once the promotion request is approved.

The following example shows how automatic revisioning works when promoting an object from Development to the Production Gate state when the preference is enabled:



For more information, see [Promotion Process](#) on page 326.

## Life Cycle Teams in Windchill ProjectLink

When routing a life cycle managed object in Windchill ProjectLink, only the members of the context team roles that match the life cycle phase roles will be pulled into the life cycle team. The entire context team is no longer pulled into the life cycle team. This is the default behavior for the wt.property file (wt.team.addEntireContainerTeam).

A message will be thrown if a user tries to create an advanced life cycle template via the Life Cycle Template Administration utility and does not associate a workflow template to the life cycle phases or gates. In this case, the message requests the user to change the life cycle template from advanced to basic for better performance and scalability.

---

## Restrictions on Moving Life Cycle Managed Objects Between Contexts

If you create a life cycle template in a specific product or library and the template is not available in other products or libraries, then you cannot move any object that uses the life cycle template.

---

### Note

For demonstration purposes, the Product Design template (available by default when you create a product) includes object initialization rules that set different default life cycle templates and versioning schemes for parts, documents, and CAD documents than are set out-of-the-box at the site level. This template demonstrates the use of simplified life cycles and state-based versioning. Unless you have overriding business practices that require unique rules, PTC recommends that if you want to use these features, you modify the organization or site object initialization rules and remove them from the Product Design template.

---



# 12

## Understanding Workflow

Overview .....	338
Managing Workflow Security .....	340
Workflow Version Control .....	343
Using the Workflow Template Editor .....	344
Exporting and Importing Workflow Templates Across Releases .....	354
Process Manager Toolbar Access Control .....	355
Using PDF Forms as Task Templates .....	356
Viewing Workflow History .....	356
Workflow Instance States .....	363
Out-of-the-Box Workflow Templates .....	364
Workflow Template Execution Flags .....	375
Electronic Signatures .....	384
Best Practices .....	387

This section provides information about workflow processes and the Workflow Template Administration utility.

---

## Overview





A workflow system gives you the ability to automate procedures in which information, tasks, and documents are passed among participants. This procedure is based on a process composed of well-defined rules designed to efficiently accomplish your business goals.


This reference information provides details about creating and editing workflow templates, importing and exporting templates, and viewing workflow history. Detailed information concerning configuring worklist fields and object subscription code is also available.

The Windchill workflow system consists of the following components:

- The Workflow Template Editor, which allows you to define a workflow process and save your definition as a process template. This graphical editor and its use are the focus of this chapter.
- The workflow runtime system, which executes a defined workflow process within the context of a specific business object (for example, a part or a document). Process execution includes delivering work assignments to users participating in the process, opening applications (for example, automatically interacting with the Windchill Explorer to check a business object out of the database), initiating subprocesses, and so on.
- The Workflow Process Manager, a graphical tool for monitoring and reporting on workflow processes. For access control information, see [Process Manager Toolbar Access Control on page 355](#).
- The Workflow History Viewer, which provides a simple ASCII interface used to access recorded workflow events, such as state changes, data transfers, or process start. [Viewing Workflow History on page 356](#) can assist you in optimizing or streamlining a workflow process.
- The Workflow Process Administration utility, which provides a centralized area to manage executing workflow processes and diagnose any warnings or errors that may occur.


## Accessing the Workflow Template Administration Utility

You can access the **Workflow Template Administration** utility on the **Utilities** page from the **Site** , **Organizations** , **Products** , and **Libraries**  contexts. Site, organization, and application context administrators manage workflow templates, as described below:



- When accessed from the **Site**  level, the site administrator has unrestricted access to all workflow templates in the site context.

---

Site administrators create, modify, delete, and view workflow templates in the site context.

- When accessed from the **Organizations**  level, access to the workflow templates in the site context and the templates that are within the active organization context is available to site and organization administrators.



Organization administrators create, modify, delete, and view workflow templates in the given organization context. Organization administrators can view workflow templates from the site context.

- The **Products**  and **Libraries**  level utilities provide access to the workflow templates that are in the active context, plus access to the templates that are inherited from the organization and site contexts.

Product and library administrators create, modify, delete, and view workflow templates in their respective context. They can view organization templates from the parent organization context and the site context.

---

 **Note**

The Workflow Template Administration utility is not available in the **Projects**  or **Programs**  contexts to administrators of these contexts. For more information about the specific workflow process support in Windchill ProjectLink, see [Workflow Process Support in Windchill ProjectLink on page 389](#).

---

The Workflow Template Administration utility displays a table that lists all workflow templates belonging to the given context, plus those belonging to its parent contexts. The Context column in the table identifies the context owning each workflow template.

When you create a workflow process in Windchill PDMLink, the system saves the new workflow process in the System cabinet of the context in which it is created. The system, not the user, decides where the new workflow template is to be located.

Workflow templates may be moved if certain conditions are met:

- The workflow template must be checked in.
- There must be a higher level context in the hierarchy than the one in which the workflow template currently resides.
- The name of the workflow template must be unique in the target context.

For more information on moving workflow templates, see the Workflow Template Administration help.






---

## Managing Workflow Security

Workflow creators are permitted to write workflow-embedded Java code to facilitate the execution of the workflow process. This embedded Java code is executed on the server, and there are no restrictions on the APIs available for use.

Considering this capability, an additional level of control has been provided for the site administrator to prevent a user who is not a member of at least one of three specific site context groups (Administrators, Workflow Administrators, or Workflow Author) from embedding Java code in workflows.

A user with permissions to create workflow templates (for example, a project manager) could potentially add malicious code in one of the workflow expressions, causing a possible security threat. For this reason, workflow templates that contain Java expressions must be written, reviewed, and thoroughly tested by individuals that are trusted by the organization.

The **Workflow Template Administration** link is available on the **Utilities** page of **Site** , **Organizations** , **Libraries** , and **Products** . Although it is not available on the **Project**  **Utilities** page, a Project Manager could potentially obtain the URL for the utility and access it by typing the URL directly into a browser address bar.

The following sections provide more detail about the roles that can author workflow processes, the site context groups that allow Java code to be embedded, and the areas that are disabled when a user is prevented from embedding Java code.

## Workflow Creators

Windchill PDMLink and Windchill ProjectLink permit all users with the role of Library, Product, and Project Managers, as well as Organization and Site Administrators to author (create and modify) workflows within the contexts (Organizations, Products, Libraries, or Projects) they manage. This is as-designed, and is a necessary component of the distributed administration model enabled by these solutions.

The embedded Java code that workflow creators are permitted to write to a workflow process includes embedding Java code in Execute Expression robots, Synchronize robots, Conditional gates and activities to perform conditional branching or execute custom application logic within the context of the workflow. This embedded Java code is executed on the server, and there are no restrictions on the APIs.

Application context managers for Libraries, Products, Projects, Programs, and Organizations are granted Full Control (All) permission on WLObject. This permits Organization Administrators and application context managers to effectively administer their contexts, through granting them the ability to modify access control policy rules, workflow and life cycle templates, and other

---

contextual administrative objects. However, through granting them the ability to author workflow templates they are also effectively being granted the ability to write Java expressions which will be run on the server when the workflow is executed.

With the introduction and adoption of the distributed administration model, the number of users with broad access permissions in the application contexts expanded significantly. PTC is no longer assuming that a user who is responsible for administering an individual context is trusted to author Java code which may provide access to information outside of the context they manage.


Considering this capability, a user with permissions to create workflow templates (for example, Project Managers) could potentially add malicious code in one of the expressions, causing a possible security threat. For this reason, workflow templates that contain Java expressions must be created and thoroughly tested by individuals that are trusted by the organization.

## Restricting Workflow-Embedded Java Code


An additional level of control has been provided for the site administrator to restrict which users can create and modify Java expressions within workflow templates. This is done by specifying membership in at least one of three of the following site context groups:

- Administrators
- Workflow Administrators
- Workflow Author


A user must be part of one of the above listed groups to have permission to embed Java code in workflows templates.

When a user attempts to add or modify expression code, the system will perform an additional check to verify that the user is a member of at least one of these three groups defined in the **Site**  context. If the user is not a member of at least one of these three groups, all expression code input fields in the Workflow Template Editor will be disabled. Furthermore, the workflow service will prevent saving a template with modified expression code, in cases where the workflow template may be created through other means.

## Administrative Groups

The Administrators and Workflow Administrators groups are part of the base data loaded with every Windchill installation. However, members of these groups are also granted the permissions necessary to create and modify workflow templates within the **Site**  context. Even though these permissions are not inherited by the domains used for organizations or other contexts, a member of one of these groups could potentially obtain the URL for and access the Site-level Workflow Template Administration utility by typing it directly into a browser address bar.

---

For this reason, a new group is available in the **Site**  context called Workflow Author. This group will not be granted any access permissions by default, but members of this group will be considered trusted to author Java expressions in locations where they are otherwise granted the permission necessary to author workflow templates.

For example, if a library context manager launches the Workflow Template Administration utility and creates a workflow template in the context of that library, they will be permitted to do so because they have been granted the necessary access control permissions through their membership in the library manager role (Full Control (All) permission on WLObject). However, when the library context manager attempts to access any of the input fields for expression code (for example, the **Transitions** tab for a workflow activity) in the workflow template, the system will perform an additional check to verify that the user is trusted to author expression code by confirming that the user is a member of either the Workflow Author, Workflow Administrators, or Administrators groups. If so, the expression code input fields will be enabled and the user will be able to edit the embedded expression code. If not, the expression code input fields will be disabled and the user will be able to view but not edit the expression code.

Thus, membership in one or more of these three groups serves as a second layer of permission controlling who is able to create and edit workflow-embedded Java expressions.

#### Disabled Areas of the User Interface

The following areas within the Workflow Template Administration utility will be disabled for users that do not have permission to create or edit Java expressions:

- Import button
- Export button
- Save As button

The text area used to enter Java expressions in the Workflow Template Editor will be disabled for the following components:

- Routing tab in the Assigned Activity / Ad hoc Activity process node
- Transition tab in the Assigned Activity / Ad-hoc Activity process node
- Routing tab from the Properties link
- Transition tab from the Properties link
- Expression Robot
- Block
- All connectors (And connector, Or connector, Threshold connector, and the Conditional router)

---

The following components will also be disabled in the Workflow Template Editor:

- Synch Robot
- Application Robot
- Expression Robot

No restrictions have been put in place when users create application context templates that load workflow templates. Context Creators will be allowed to load the workflow templates containing expressions, even if they are not members of the site-level workflow administrators group.

For more information about these components, see the [Workflow Template Administration help](#).

## Workflow Version Control

Administering workflow templates is an iterative process. Like version-controlled objects, iterated objects are checked in and out of shared locations. However, unlike version-controlled objects, they cannot be revised. Instead, any change to an object creates a new and separate iteration when it is checked in. Earlier iterations, which may still be in use, are unchanged and unaffected by the new iteration. Only the latest iteration is available for new uses.

To make changes to a workflow template, you must check out a copy. Clicking **Edit** on the Workflow Template Administration page automatically checks out a copy of the selected template. While it is checked out, no one else can check out a copy, but processes can still be initiated based on the current template. When you have completed changes to the checked-out copy, you must save it and check it in to make it available to others. It then becomes the latest iteration. Running processes that use an earlier iteration continue to run, unaffected by the newer iteration.

---

### Note

- When you initiate a workflow process, only the most recent iteration is used. You cannot initiate a process using a checked-out workflow template.
  - You cannot delete a checked-out workflow and you cannot perform undo checkout on a new workflow template. To delete a new workflow template, you must first check it in.
-

---

## Using the Workflow Template Editor

The Workflow Template Editor is a graphical interface for defining workflow processes that range from the simple to the highly complex. It features a large set of predefined activity nodes that you can place and connect. The Workflow Template Editor supports nested processes, branching, merging, loops for iterative activities, and defining assigned activities.

### Working with Workflow Templates

The **Workflow Template Administration** utility displays a list of existing workflow templates, with their locations, enabled status, and context. Using the buttons on this page, you can create new templates, edit and view existing templates, and delete templates, as well other activities, including importing and exporting workflows. Click **New** or **Edit** to access the Workflow Template Editor. When you edit a workflow process, it is automatically checked out if it is in a vault.

For more information about using the **Workflow Template Administration** utility, see the Workflow Template Administration help.

To verify that your process definition is correct, select **Process** ► **Validate All** at the top of the Workflow Template Editor window. The **Validate** window either confirms the process definition or identifies dangling activities or malformed processes.

A Java compiler is integrated with the Workflow Template Editor to support expressions of arbitrary complexity. Workflow routing functionality includes links and event triggers. Events that cause a link to fire are displayed on the link itself, so anyone viewing the process definition can easily understand and verify the process behavior. For example, the Approve and Revise events in the examples above are events that cause a link to fire.

When you have completed your process definition, it is saved in your personal folder. To change a process definition that has been saved in a vault, it must be checked out and checked back in.

Updating workflow processes is an iterative process. A new iteration is created when an edit is checked in. You can view iterations on the **Workflow Template Administration** page.

The following sections describe the tools and components available to help you define a workflow process in Windchill.

### Navigating a Process Diagram

The Workflow Template Editor is designed for easy navigation of processes and their subprocesses using common web navigation techniques. For example, you can edit a subprocess diagram by clicking a subprocess hyperlink.



---

To navigate between a parent process and a subprocess, use either the **Back** and **Forward** buttons, or the **Location** drop-down list.

The title bar of the Workflow Template Editor displays the name of the process or subprocess you are currently editing.

Hyperlinks display the properties of each activity type and link. For example:

- Click an activity node hyperlink to open the properties window for that activity. You can then create, edit, or view the properties that define the node's behavior.
- Click the **Properties** hyperlink (to the right of the **Location** drop-down list) to view and edit the properties of the process itself.
- Double-click the link that connects a node to open a window to map events that are broadcast (or emitted) from the preceding activity to actions in the succeeding activity. By default, the completion event for a given task triggers the start of all successor tasks.

## Placing Process Nodes

You can build a process definition by adding, selecting, and linking nodes that are represented by icons at the left of the Workflow Template Editor.

For more information about adding and linking nodes, see the Workflow Template Administration help.

The following list describes the process nodes that can be added to your process definition. The list is displayed in order of each icon's appearance on the Workflow Template Editor.

- The Assigned Activity is an activity assigned to one or more users or user-defined groups or an actor to perform.
- The Ad Hoc Activity is assigned to a user to define a group of activities at runtime. The group of activities is similar to a simple block.
- The Block represents a group of activities, connectors, or robots. You can reduce the complexity of a process by creating blocks of activities that can be expanded when needed.
- The Proxy Process is a subprocess embedded within the main parent process, which can be nested to reduce complexity and provide reuse.
- The And Connector fires when all the predecessor links have fired, but not before.
- The Or Connector fires when any one of the predecessor links has fired. Preceding activities are terminated if **Terminate Open Predecessor Activities When Fired** has been selected.
- The Conditional Router allows you to branch a process based on a conditional expression.

- The Threshold Connector fires when a user-defined number of predecessor links have fired. Preceding activities are terminated if **Terminate Open Predecessor Activities When Fired** has been selected.
- The End stops the process. All process activities should eventually be connected to an end.
- The Ground stops a parallel branch of activities within the process, but it does not stop the process.
- The Notification Robot notifies the appropriate user with a user-defined email. You can define notification robots containing an attachment or metadata of the primary business object associated with the workflow. You can use braces to delimit variables created for the process or node, for example, {varname}. Use back slashes to escape the delimiter, for example, \{\{varname\}\}. For a detailed procedure, see the Workflow Template Administration help.
- The Method Robot represents one of several single actions performed when adding the robot to the process. No other configuration is required. The following table lists the robot actions:

Robot	Description
Checkin	Checks in the primary business object to the Windchill database.
Checkout	Checks out a business object to the specified user. For example, you can use the Checkout robot to automatically check a part out to the engineer assigned the task of applying changes after a design review cycle is complete.
Demote	Causes the primary business object to transition to a predecessor phase, with an associated state change, and the application of new business rules (such as those for access control).
Deny	Removes the primary business object from the gate and returns it to the phase of the same state.
Drop	Causes an object to be removed from its current life cycle and sets its state to dropped. For example, you could have a process branch in which two vendors submit bids for review. These bids could be entered into the database as Windchill documents, which would move through a review and approval process by application of a process definition. In this case, your process may require that, when one bid is approved, its document object is automatically promoted to its next life cycle phase, while the document containing the rejected bid is dropped from its life cycle and goes no further.
Promote	Causes the primary business object to transition to a successor phase with an associated state change and the application of new business rules, such as those for access control. For example, you could define a process in which an object is

Robot	Description
	automatically promoted to the next phase in its life cycle, if a specific user approves the object. In this case, you could add the Promote robot to your process definition to execute all of the actions associated with an object's promotion.
Set State	Sets a life cycle–managed object to an ordinal state or a specific state. The ordinal state is entered as any non-zero integer. The specific state is selected from those defined in the wt.lifecycle.StateRB enumerated type.
Submit	Moves the business object associated with this process to the gate for its current life cycle phase. After a submit, an object awaits promotion to the next life cycle phase. For example, you could add the Submit robot to a process definition to indicate that, when a user creates a change request, it is automatically submitted for promotion to the Open state.

- The Checkpoint Robot records the time it takes the workflow process to get from one checkpoint node to the next. An email notification is sent to subscribers when the node is reached.
- The Timer Robot delays the start of an activity by a specified amount of time, based on the time it is fired or the time the parent process is begun.
- The Launch Application Robot executes system commands on the server. These commands are executed using the Java runtime.exe command. The execution can be either synchronous or asynchronous.
- The Execute Expression Robot enters a synchronous Java expression to be executed in a workflow. By default, the expression returns true. A return of false indicates a problem during execution, and an exception is thrown on the server.
- The Synchronization Robot synchronizes the start of an activity or process with events that are not time related. You can set the robot to start an activity when certain generic external or Windchill-keyed events occur.

If synchronization does not work, make sure that the time zone is set correctly on the server where your Windchill solution is installed.

- The URL Robot executes a URL to communicate with another server, for such purposes as initiating various Info\*Engine tasks or providing information necessary to complete workflow tasks. It can initiate an operation or retrieve status information to be collected in a string variable. HTML links to binary objects, such as graphics, can be retrieved, although the objects themselves cannot.

---

You can specify the results of a failure by the robot to execute the URL. The following list of error codes may be helpful.

- 400 Bad Request: Request has not been recognized by the server, because of incorrect syntax. Request should not be repeated.
- 401 Unauthorized: Request requires user authentication. Under normal usage, the URL robot does not support authentication. Request should not be repeated.
- 403 Forbidden: Request has been recognized but the server has refused to honor it. Authentication was not the reason. The request should not be repeated.
- 404 Not Found: Server has found no match for the Request-URI. May be temporary or permanent. Repeat of request may be appropriate.
- 500 Server Error: Server has encountered an unexpected condition, which prevents it from fulfilling the request. Repeat of request may be appropriate.
- 501 Not Implemented/Internal Error: Server does not support the functionality required to fulfill the request. Request should not be repeated.
- 503 Service Unavailable: Server is temporarily unable to handle the request. Repeat of request may be appropriate.
- 504 Gateway Timeout: Server has not received a timely response from the upstream server specified by the URI. Repeat of request may be appropriate.

For more information on error messages, see the Internet standards at W3C HTTP RFC (<http://www.w3.org>).

## Declaring Variables

When you define a process, variables can be used within transition condition or automatic routing expressions. Variables can be either global (applicable to the process itself) or local (applicable to an assigned activity or a subprocess).

---

### Note

When the Windchill 8.0 out-of-the-box change management workflows are run in Windchill 10.x, the user will see the activity variables in the task details page that are defined in the 8.0 workflow templates instead of the activity variables that are defined in the 10.x workflow templates.

---

---

Variables can be declared as any Java type or as any Windchill class. The only restriction is that the variable must be serializable. If the variable is typed as a Windchill business object, attributes of that object can be referenced through standard getter APIs. Variables can be declared as follows:

- Visible or invisible
- Required or optional
- Read only or read/write
- Resettable or static

Variable values can be initialized from parent process variables when an activity or subprocess is started and can also be copied into parent process variables when the activity or subprocess is complete.

---

 **Note**

Although you can declare a workflow variable to be any Java type or Windchill class (provided it is serializable), PTC encourages you to consider the following guidelines:

- Workflow variables are composited within a `ProcessData` object, which in turn, is persisted in the Oracle database in a BLOB column. If the persistent signature of a BLOB object changes after it is stored in the database, an error may be thrown at the time it is retrieved from the database and de-serialized; therefore, PTC recommends that workflow variable types be restricted to the following:
  - java primitives
  - Evolvables
  - Persistables

Evolvables provide methods to handle changes in their persistent signatures. Persistables are stored in workflow variables as `ObjectReferences` (not the fully inflated object).

- Persistables should not be composited within another class as this may lead to data inconsistency or corruption. Doing this will also lead to a `wt.pds.NotEvolvableException` during migration.
  - Persistables may be an element in a `java.util.Vector` (this is because the `Vector` class receives special handling by the `WfVariable` class), but this should be avoided if possible. Use of a `CachedObjectReference` or `ObjectReference` pointing to a persistable is the preferred practice.
  - A Workflow Variable can contain, composite, or otherwise encapsulate a `ObjectReference` to a persistable as necessary.
-

---

For information on the Windchill evolvable classes and interfaces, see the *PTC Windchill Customization Guide*.

## Defining an Assigned Activity

An assigned activity is a task that gets assigned to a specific user or group of users when an instance of this process definition is running. When you define an assigned activity, you specify a task that the selected user is to perform as part of a workflow process. The task is then added to the user's **Tasks** table.

For more information, see the Tasks help.

The assigned activity properties are described in the sections that follow.

## Defining a Subprocess

A subprocess, or proxy process, can be included as a node of a parent process.

For more information about creating a proxy process, see the Workflow Template Administration help.

The task assignments that are generated from an activity defined in the proxy process will not display roles that have been defined in the parent process (the outer process nodes). However, activities that are defined in the parent process nodes display a list of all roles used anywhere in the (outer) workflow process. This means that an assignee of an activity that belongs to a proxy process won't be able to modify the participant roles that belong to the parent process. However, the assignees of activities that belong to a parent process can modify the participant roles that belong to the proxy process.

Roles are defined in the outer process activity nodes on the Role Setup tab. The Set Up Participants table (accessed from the **Tasks** table of the assignee) will display roles based on the permissions that are granted by the workflow administrator in the **Role Setup** tab of the workflow process.



For example, if the Approval Process workflow is selected when defining the proxy process, only the roles that are defined in the Approval Process workflow will display in the generated task assignments of the activities in defined in the proxy process. The task assignments that are generated from the outer process activity nodes will display all of the roles that have been defined anywhere in the outer process (also referred to as the parent process), plus all the roles that are defined in the inner process (in this example, the Approval Process).

---

For more information about defining roles and specifying permission for each role, see the workflow help.

Set a deadline for the proxy process by clicking the **Deadline** tab. For more information, see the workflow help.

To map variables, click the **Variable Mapping** tab. For more information, see the workflow help.

---

 **Note**


Ad hoc activities and blocks are also composed of a group of activities. A block is a way of simplifying the graphical representation of the process, by combining a number of activities under one icon. An ad hoc activity is a group of activities defined at runtime.

---

## Defining Connectors

The Workflow Template Editor supports the following connector types:

Connector Type	Description
Start	The Start connector represents the starting point in a process. Each process has only one Start connector, which cannot be removed or duplicated.
And	An And connector does not fire until all predecessor links have fired. It waits for all preceding activities to complete before allowing the process to continue. For example, a Promote activity can be connected to multiple review activities by an And connector.
Or	An Or connector fires if any of its predecessor links fire. That is, it allows the process to continue if any of the preceding activities have completed. For example, a Revise activity can be linked to multiple review activities by an Or connector.

Connector Type	Description
Threshold	<p>A Threshold connector fires if a user-defined number of predecessor links fire. That is, it allows the process to continue only when the user-defined number of preceding activities have completed. To set the number of activities that must complete before a Threshold connector fires, enter a number in the <b>Firing Threshold</b> text box, on the <b>Threshold Properties</b> window.</p> <p>To set a dynamic threshold, in which the firing threshold is set to 0 at runtime and is reset to the number of started predecessor activities, select <b>Add one</b> from the <b>Action in Threshold</b> list on the preceding <b>Link Properties</b> window.</p>
Conditional Router	<p>A Conditional Router fires user-defined events based on an automatic event firing expression. Because you can define user events and fire them with an expression for all connectors, the Conditional Router is essentially an Or connector identified by a special icon.</p> <p> <b>Note</b></p> <p>Whenever possible, expressions should be inside a try catch block. Inside the catch block, take corrective action for the exception.</p>

Specify custom routing events, which can be used to control process flow, on the **Routing** tab panel on the Connector Properties window. For more information, see the workflow help.

---

 **Note**

Because the Or connector and the Threshold connector do not require all activities to be completed before allowing the process to continue, unnecessary activities can remain open. To terminate these activities, click **Terminate Open Predecessor Activities When Fired** on the **Or Properties** window or the **Threshold Properties** window.

---

## Defining Links

Links define the flow of control among nodes within a process definition. They also determine which actions are performed in an activity when a predecessor activity broadcasts (or emits) events. For example, when a user completes a review task (indicating completion by clicking a button on that task page), you can specify that the completion event will cause a link to the next activity to fire.



---

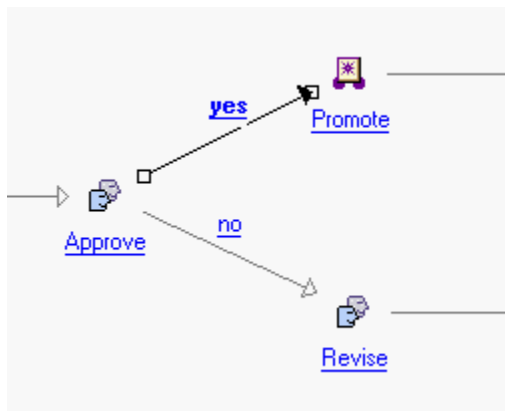
On the **Link Properties** window, you can map events to actions.

To map an event (in the left column), select a successor action from the drop-down list in the right column. You can specify more than one event to cause the same action to occur. To indicate that an event will be ignored, leave the field in the **Action** column blank. If an event is ignored, no action is performed when that event is emitted.

To reset all connectors in an events path when it is fired, select the **Loop Link** checkbox. Selecting the Loop Link checkbox ensures that connectors that are in the loop get reset prior to the workflow loop getting traversed again. The connectors that have already fired are reset, and they can be fired again. Loop links are designed to reset all connectors in the path of the workflow activity that is the target of the loop link. A connector is considered in the path of this activity if it is reached by going forward from the activity AND going backwards from the activity. Loop links appear in red.

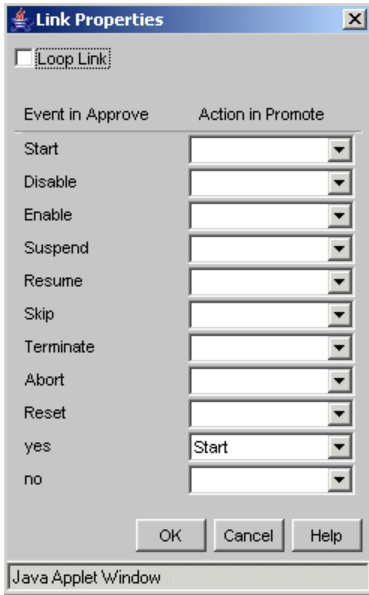
You can define custom routing events for most activities and processes. When you do so, these events are also displayed in the **Link Properties** window, and you can map them to actions in a successor activity. For example, you could include in a process definition the following assigned activities:

- Approve
- Revise
- Promote



The Approve activity defines two custom routing events, yes and no. This activity has two links: one link connects to the Revise activity and another connects to a Promote robot. The link to the Revise activity can be configured to perform the Start action in Revise when the no event is emitted from the Approve activity. The other link can be configured to perform the Start action in the Promote robot when the yes event is emitted from Approve. In this way, the flow of control to the Revise or Promote activity is controlled by the event emitted from the Approve activity.

The figures that follow show possible results:



OR



## Exporting and Importing Workflow Templates Across Releases

Importing workflow templates across releases is denied by default due to the fact that it could cause data corruption.

---

The cross-release import function can be enabled by setting a property file. However, any data inconsistency issues that arise after allowing such an import will not be supported.

Set the following wt.property file to true.

```
wt.ixb.import.allowCrossReleaseImport=true
```

Restart the method server to reload the property file.

## Process Manager Toolbar Access Control

The workflow process manager toolbar allows authorized users to change workflow processes. An authorized user can make vital changes to an activity or a process, such as terminating or completing it.

Access to the process manager actions is defined in the following file:

```
<install directory>/codebase/wt/clients/workflow/manager/process-manager.properties
```

Out-of-the-box, full access is given only to the system administrator and the workflow administrator, as defined in the following properties:

```
activityrestartAccessControl=Administrators
activitysuspendAccessControl=Administrators
activityresumeAccessControl=Administrators
activityterminateAccessControl=Administrators
activitycompleteAccessControl=Administrators
processsuspendAccessControl=Administrators
processresumeAccessControl=Administrators
processterminateAccessControl=Administrators
processcompleteAccessControl=Administrators
activityrestartAccessControl=WorkflowAdministrators
activitysuspendAccessControl=WorkflowAdministrators
activityresumeAccessControl=WorkflowAdministrators
activityterminateAccessControl=WorkflowAdministrators
activitycompleteAccessControl=WorkflowAdministrators
processsuspendAccessControl=WorkflowAdministrators
processresumeAccessControl=WorkflowAdministrators
processterminateAccessControl=WorkflowAdministrators
processcompleteAccessControl=WorkflowAdministrators
```

To add other user-defined groups, add additional values using the following format:

```
<action>AccessControl=<group name>
```

---

## Using PDF Forms as Task Templates

When managing and creating workflow templates, you can specify custom templates to render workflow task information pages.

One option is to render the task form as a PDF. To do this, you must install and configure Adobe Experience Manager to work with Windchill. For more information, see the *PTC Windchill Installation and Configuration Guide*.

Adobe Designer creates XDP templates that include various form fields such as labels, text fields, and radio buttons that act as placeholders to display the workflow task attributes. When closing their workflow task, the assigned user completes the form with the required information. Windchill is updated and the workflow proceeds to the next step.

---

### Note

If the Adobe forms software is not installed and configured for use with Windchill, the workflow tasks are rendered in the HTML default format using the JSP template type.

---

For more information, see the following:

- “Using Task Form Templates” in the PTC Windchill Help Center
- “Task Form Templates Table” in the PTC Windchill Help Center
- “Customizing Workflow Task Pages” in the *PTC Windchill Customization Guide*

---

### Note

PTC provides a default task form template that is used with the out-of-the-box workflow template activities. If you are using the out-of-the-box workflow templates, do not delete this task form template.

---

## Viewing Workflow History

To optimize and streamline your workflow process definitions, you should capture and record events, such as state transitions and variable updates that occur during process execution. The ordered sequence of these events is called a workflow history, which allows you to capture significant events.

---

In addition, you can specify that a keyed event be emitted, which allows synchronization of other Windchill managers and servers with process events. As described in this section, you can specify the following:

- Which events are to be ignored
- Which are to be recorded
- Which are to be emitted as keyed events
- Which are to be both recorded and emitted

---

 **Note**

When there is a loop link in a workflow with a conditional route, only the last vote is recorded.

---

## Selecting Events

The following events can be generated during execution of a workflow process:

- Process creation, which occurs when a Start command is issued for an existing, enabled process definition.
- Change of state, which occurs when an execution object (a process or an activity) changes states (for example, from running to completed).
- Change of data value, which occurs when values are read into a process activity or written to process variables.
- Change of assignee, which occurs when assignment of a workflow task changes from one user to another.
- Error event, which occurs when an exception is thrown during process execution.

You can identify the events to be recorded in the workflow history or emitted as keyed events by setting the default event configuration in the `wt.properties` file.

---

 **Note**

Workflows that are created before changes to the `wt.properties` are applied are not affected.

---

When one or more of the following properties is set to true, the corresponding event is recorded or emitted:

`wt.workflow.engine.recordProcessStateChange`  
`wt.workflow.engine.recordProcessDataChange`

---

```
wt.workflow.engine.recordActivityStateChange
wt.workflow.engine.recordActivityDataChange
wt.workflow.engine.recordProcessCreation
wt.workflow.engine.recordAssigneeChange
wt.workflow.engine.recordException
wt.workflow.engine.recordVoting
wt.workflow.engine.emitProcessStateChange
wt.workflow.engine.emitProcessDataChange
wt.workflow.engine.emitActivityStateChange
wt.workflow.engine.emitActivityDataChange
wt.workflow.engine.emitProcessCreation
wt.workflow.engine.emitAssigneeChange
wt.workflow.engine.emitException
```

All running workflow processes record and emit events based on this default configuration. You can use the Workflow History Viewer to change the events recorded or emitted by a given process.

## Using the Workflow History Viewer

You can view workflow-generated events on the Workflow History Viewer, a simple ASCII utility. Issue the following command to start the Workflow History Viewer:

```
windchill wt.workflow.engine.WfMonitor
```

The following is the main menu of the Workflow History Viewer:

```
Workflow Monitor - Main Menu

Existing Workflow Processes
-----

>> 1. Simplest, key = 3347 (Running)

Audit events
-----

No event retrieved
1. Select process.
2. Show selected process.
3. Delete selected process.
4. Refresh processes.
5. Change event configuration for selected process.
```

- 
6. Show selected events for selected process.
  7. Show all events for selected process.
  8. Show selected events for all processes.
  9. Show all events for all processes.
  10. Select event.
  11. Show event.
  12. Show event source.
  13. Refresh events.
  14. Delete events for selected process.
  15. Delete events for all processes.
  16. Exit

>>> Choose an option:

This menu includes a list of all existing processes and a list of all retrieved events. The list of retrieved events is initially empty.

In addition to these lists, the main menu provides 16 options. A description of each follows:

### **Select Process**

Select this option to select a process, so associated events can be queried. The selected process is preceded by the characters >>.

### **Show Selected Process**

Select this option to display the following information about the selected process, as well as all of its activities and subprocesses that have been started:

- The process status (for example, running).
- The process creator.
- The team with which the process is associated.
- An indication of whether or not the process or activity is overdue (that is, whether it has exceeded its specified duration).
- The time at which the process or activity started.
- The time at which the process or activity ended (not shown if the process or activity has not been closed).
- The deadline for the process or activity, if one exists.
- The event configuration for the process.
- Suspend and alert times, in milliseconds.

The following shows a sample process display:

```
Simplest - Running
Creator: Administrator
Team: Default
Times: is overdue = false
```

---

```
start time = 1998-11-20 14:08:53.0
suspend time = 0, alert time = 0
Event configuration:
Process (RECORD/EMIT): Creation: R, State change: RE
Activity (RECORD/EMIT): Data change: E
Exception (RECORD/EMIT): Exception: R
Activities:
*** act_simplest (wt.workflow.engine.WfTestActivity) - Running
Times: is overdue = false
start time = 1998-11-20 14:08:56.0
suspend time = 0, alert time = 0
```

### **Delete Selected Process**

Select this option to delete the selected process.

### **Refresh Processes**

Select this option to refresh all processes. The Workflow History Viewer does not automatically edit the status of a displayed process. You must explicitly refresh it in order to see new processes and changes of state since the last refresh.

### **Change Event Configuration**

Select this option to open an event configuration editor. With the editor you can select the events that should be emitted, recorded, or ignored, for the selected process.

Edit event configuration

Current configuration

Process (RECORD/EMIT): Creation: R, State change: RE

Activity (RECORD/EMIT): Data change: E

Exception (RECORD/EMIT): Exception: R

1. Create process - record: true
2. Create process - emit: false
3. Change process state - record: true
4. Change process state - emit: true
5. Change process data - record: false
6. Change process data - emit: false
7. Change activity state - record: false



- 
8. Change activity state - emit: false
  9. Change activity data - record: false
  10. Change activity data - emit: true
  11. Change assignment - record: false
  12. Change assignment - emit: false
  13. Execution error - record: true
  14. Execution error - emit: false
  15. Save configuration
  16. Save configuration and return
  17. Return (looses changes since last save)

>>> Choose an option:

As previously described, all processes are governed by the event configuration specified in the `wt.properties` file, unless this submenu is used to change that configuration for the selected process. Selecting an option on this submenu toggles the current setting. For example, if you select option 1, you will change the setting of `Create process` from true to false. Consequently, process creation would no longer be a recorded event.

### Show Selected Events for Selected Process

Select this option to open the submenu shown below. You can select an option from this submenu to specify the type of event in which you are interested. (In the example, option 8 is selected, indicating that the user is interested in all events associated with the selected process.)

- ```
Types of events to show
1. Process creation
2. Process state change
3. Process data change
4. Activity state change
5. Activity data change
6. Assignment change
7. Execution error
8. All
9. None (return)
```

>>> Choose an option: 8

When you have select an option from this submenu, the requested events are retrieved, and the list of events is refreshed. For each event, the list identifies the event type and the execution object associated with it:

```
Audit events
```

---

```
>> 1. PROCESS_STATE_CHANGED, process = Simplest
```

### **Show All Events for Selected Process**

Select this option to represent a shortcut to selecting **All**, (option 8) from the submenu of event types described in the preceding section. If this main menu option is selected, all events associated with the selected process are shown.

### **Show Selected Events for All Processes**

Select this option to display all events of the selected type for all processes.

### **Show All Events for All Processes**

Select this option to display all stored events for all processes. This list can be very large.

### **Select Event**

Select this option to select another event. When events are retrieved, the first event in the list is automatically selected.

### **Show Event**

Select this option to display detailed event information for a selected event, as follows:

```
event type = PROCESS_STATE_CHANGED
timestamp = 1998-11-20 14:08:53.0
activity key = 0 activity name = null
process key = 3347
process name = Simplest
process template name = simplest
old state = Not started
new state = Running
```

### **Show Event Source**

Select this option to display the execution object (process or activity) that is the source of the selected event.

### **Refresh Events**

Select this option to refresh all events corresponding to the selected process and event type. This is necessary to view events generated since the last refresh.

### **Delete Events for Selected Process**

Select this option to delete all the events of the last selected type associated with the selected process.

### **Delete Events for All Processes**

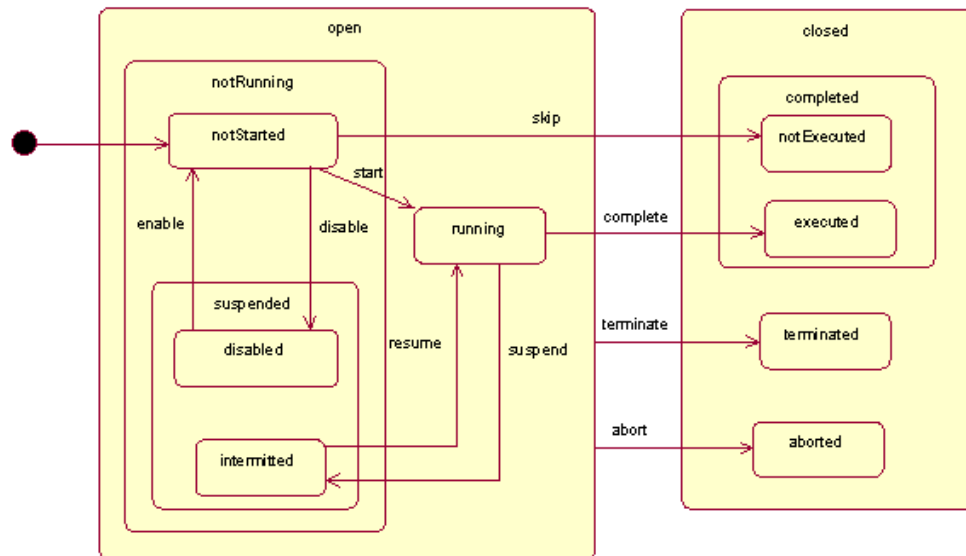
Select this option to delete all events of the last selected type associated with all processes.

## Exit

Select this option to terminate the Workflow History Viewer session.

## Workflow Instance States

The following diagram shows the states that an execution object (activity or process) can be in, and the transitions from state to state.



Rounded boxes represent states; arrows represent transitions. The actual states are always the innermost ones. The others are super-states, indicating a collection of substates. For example, a query for closed processes returns the processes that have completed successfully and also the processes that have terminated or were aborted.

The initial state for all execution objects is the not started state. The following is the normal sequence of states for an execution object is:

1. Not Started
2. Running
3. Executed

The final state can be reached with the following two transitions:

- Start
- Complete

Some transitions apply to more than one state. This is indicated by an arrow that begins in a super-state. For example, terminate transitions from any open state to the terminated state. An additional transition, reset, is not shown in the diagram. The reset transition brings any object back to the not started state.

---

Both Open.NotRunning.Suspended.Disabled and Open.NotRunning.Suspended.Intermitted are labeled suspended; however, the Open.NotRunning.Suspended.Disabled state is currently not used, so there is no chance of confusion.

The following is the model for connectors:

- Enabled
- Disabled

## Out-of-the-Box Workflow Templates

This section provides information about the out-of-the-box workflow templates and process images that can be associated with them.

The out-of-the-box workflow templates in Windchill allow you to automate procedures in which tasks and documents are passed among participants.

PTC Global Services consultants can help you determine how the out-of-the-box workflows correspond to your business processes. Although you can modify workflows if necessary, you will get better results if you map the existing workflows to your processes, rather than create new workflows based on your processes.

---

### **Caution**

Changes you make to workflows may not be compatible with future Windchill release and service packs, and may require additional support from PTC Global Services consultants.

---

The following list provides all out-of-the-box workflow templates by solution that are loaded into the site context during installation:

- Windchill PDMLink:
  - Change Activity
  - Change Notice
  - Change Request
  - Package Approval Process
  - Package Content Routing Process
  - Package Delivery Process
  - Problem Report
  - Promotion Request Approval Process
  - Promotion Request Review Process
  - Review

- 
- Submit
  - Variance Workflow
  - Windchill ProjectLink:
    - Approval Process
    - Notify Process
    - Release Process
    - Review Process
    - Two Level Approval Process

---

 **Note**

The Workflow Template Administration utility is only accessible in Windchill PDMLink. It cannot be accessed from the project or program contexts.

---

- All Windchill solutions:
  - Submit
  - Review

## Change Management Workflows

---

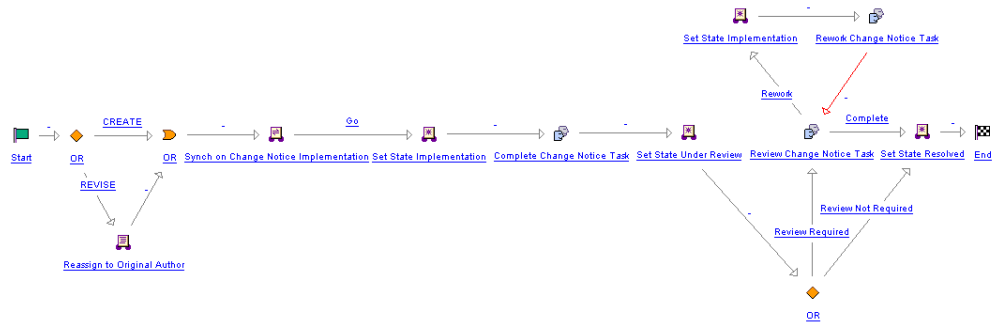
 **Note**

When the Windchill 8.0 out-of-the-box Change Management workflows are run in Windchill 10.x, the user will see the activity variables in the task details page that are defined in the 8.0 workflow templates, instead of the activity variables that are defined in the 10.x workflow templates. Additionally, when running the Windchill 8.0 Change Management workflows, the user might see two Comment fields on the task details page; one for a defined activity variable and one for the Routing History table.

---

The following section provides out-of-the-box workflow templates specific to Change Management. Each is listed below along with a summary of the steps in each workflow.

## Change Activity Workflow



### 1. Synch on Change Notice Implementation

Waits for the Change Notice workflow to emit a CHANGE IMPLEMENTATION event proceeding. For more information, see [How Change Notice and Change Activity Workflows Work Together](#) on page 368.

### 2. Complete change notice task

Review the assigned change notice task, specify edits to the affected data, and submit the completed task.

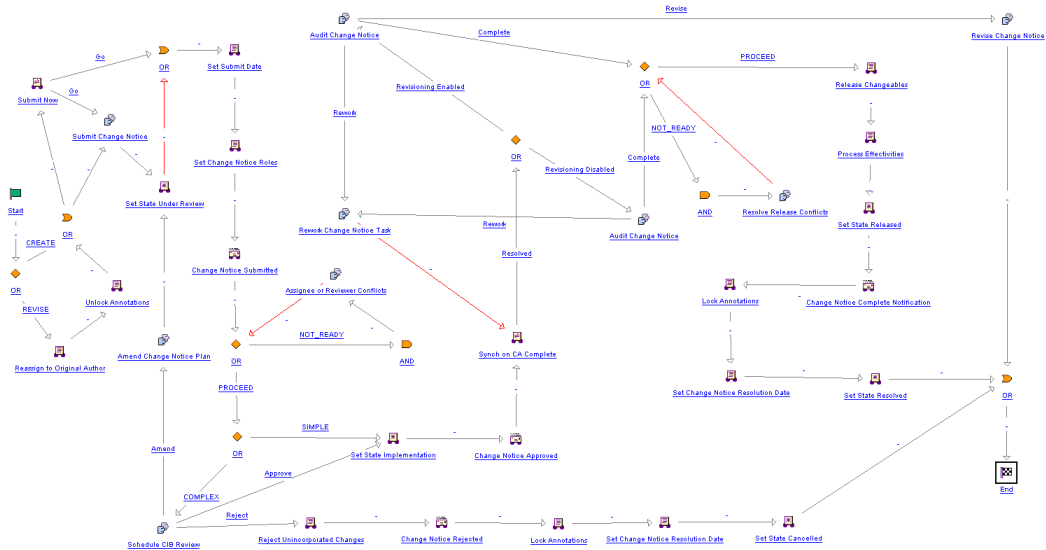
### 3. Review change notice task

Review the data modifications resulting from the preceding step and approve or reject the modifications.

### 4. Rework change notice task

According to the reviewer's instructions, perform the required modifications and resubmit them for audit.

## Change Notice Workflow



### 1. Submit change notice

Submit change notice to the system.

### 2. Assignee or reviewer conflicts

If necessary, resolve any assignee or reviewer conflicts by updating the change notice or change task with a user or role as a valid assignee or reviewer and completing the task.

### 3. Schedule CIB review

If the change notice has full track complexity, schedule and facilitate the Change Implementation Board (CIB) review and record the CIB decision.

### 4. Synch on CA complete

Sends the CHANGE IMPLEMENTATION event to all Change Activity workflows associated with the change notice. As each change task reaches the Resolved state, the CHANGE IMPLEMENTATION event is re-emitted if the next sequence is scheduled. For more information, see [How Change Notice and Change Activity Workflows Work Together](#) on page 368.

### 5. Amend change notice

If necessary, amend the change notice plan based on the CIB's review and resubmit to the CIB.

### 6. Audit change notice

---

Review the change notice data modifications and approve or reject the change notice implementation.

7. Rework change notice task

Rework change notice task and resubmit to Change Administrator II for audit.

8. Resolve release conflicts

If necessary, resolve existing release conflicts.

9. Revise change notice

If necessary (and revisioning is enabled), revise the change notice based on the CIB's review.

## How Change Notice and Change Activity Workflows Work Together

If you have Windchill ProjectLink installed, change tasks can be divided into blocks of tasks that execute according to a defined sequence. This feature is enabled by setting the **Change Management** ► **Sequenced Plan Execution Order** preference to Yes in the **Preference Management** utility.

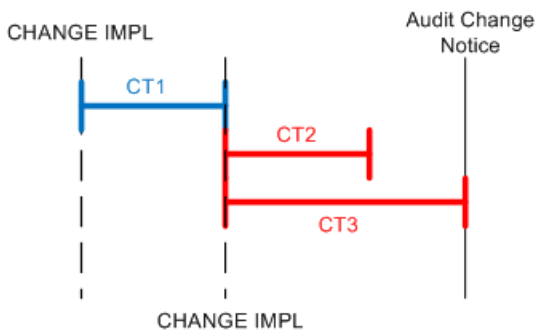
---

### Note

If you have customized Change Activity workflows from a previous release of Windchill, the workflows will function as though there is no sequence plan. To use the sequencing feature, update the Change Activity workflow template to listen for the CHANGE IMPLEMENTATION event.

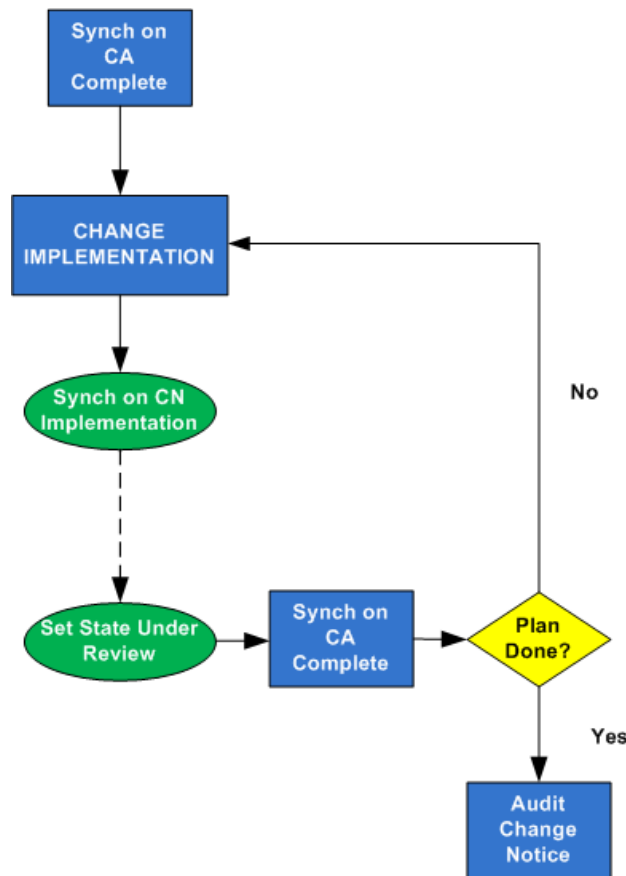
---

When the Change Notice workflow reaches the “Synch on CA Complete” synchronization robot, it initially emits a CHANGE IMPLEMENTATION event. The Change Activity workflows associated with the change tasks listen for this event with the “Synch on Change Notice Implementation” synchronization robot and, when the event is received, determine if the Change Activity workflow should proceed.



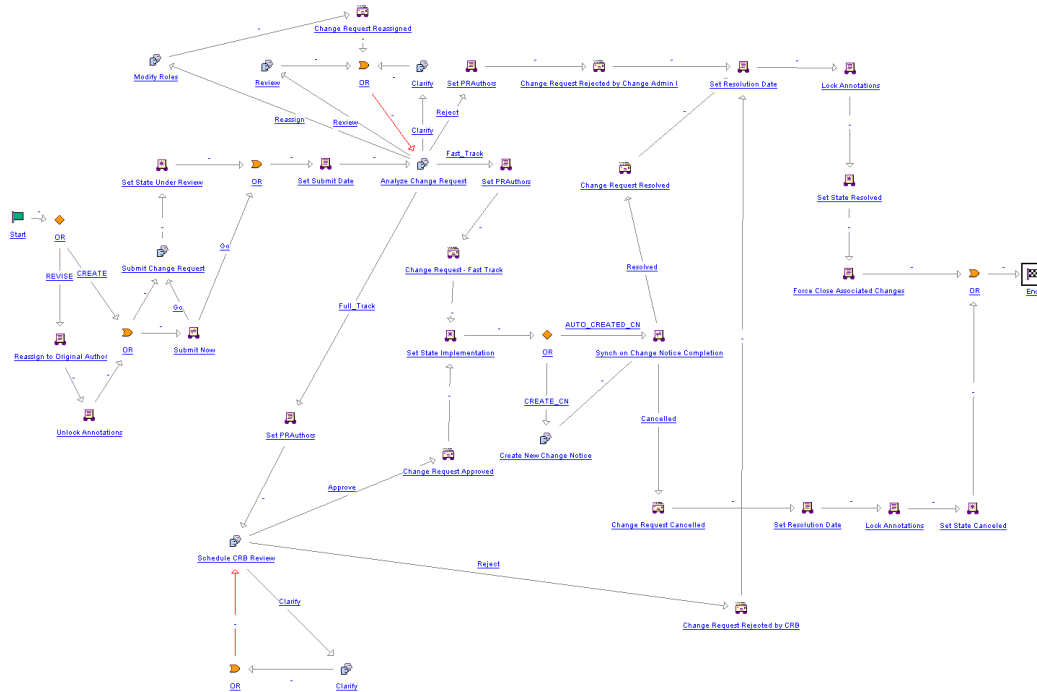


In the example, there is a sequence plan and Change Task 1 is the first sequence in the plan. When the CHANGE IMPLEMENTATION event emits for the first time, the workflow associated with Change Task 1 proceeds. Change Task 2 and Change Task 3, which are later in the sequence, do not proceed. The “Synch on CA Complete” synchronization robot in the Change Notice workflow listens for when change tasks change state. When Change Task 1 resolves, the Change Notice workflow emits another CHANGE IMPLEMENTATION event. At this time, the Change Task 2 and Change Task 3 workflows proceed. When both change tasks resolve, the sequence plan is complete and the Change Notice workflow moves on to the “Audit Change Notice” activity.



If there is no sequence plan, the “Synch on CA Complete” synchronization robot emits a CHANGE IMPLEMENTATION event. At that time, all Change Activity workflows for existing change tasks proceed. If another change task is added while the change notice is in the Implementation state, the Change Activity workflow for the new change task automatically proceeds. When all change tasks complete, the Change Notice workflow moves on to the “Audit Change Notice” activity.

## Change Request Workflow



1. Submit change request
 

Submit the change request for review.
2. Analyze change request
 

Validate the change request, coordinate the technical analysis and generation of a recommended solution, associate relevant analysis information, and determine the disposition of the change request.
3. Clarify change request
 

The change request is sent back to the author for the addition of further information.
4. Review change request
 

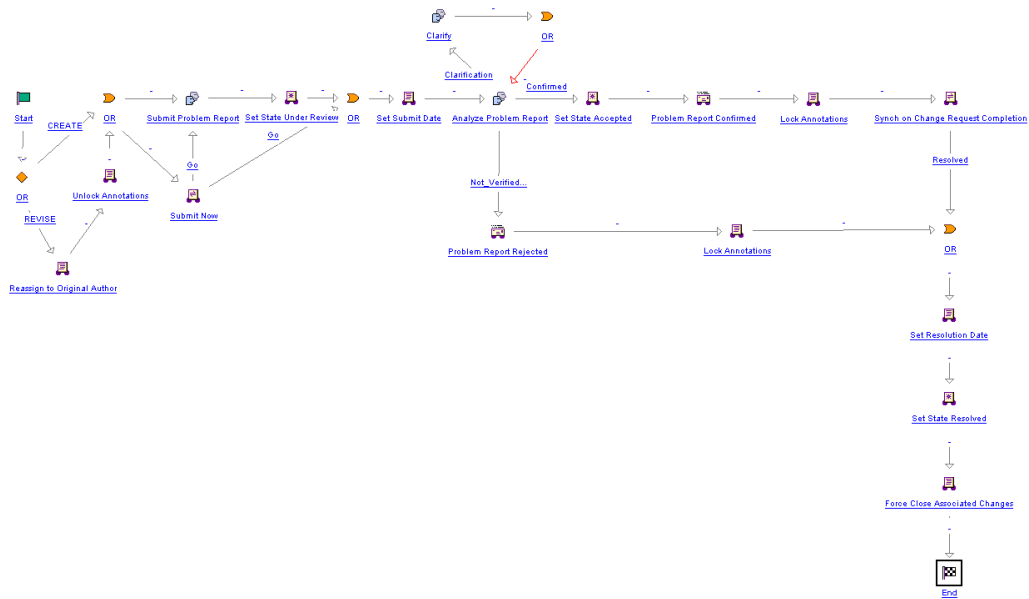
Review the change request and provide comments as needed.
5. Modify roles
 

Update the change request team roles as needed.
6. Create new change notice
 

Create a new change notice as necessary for the corresponding change request.
7. Schedule Change Review Board (CRB) review

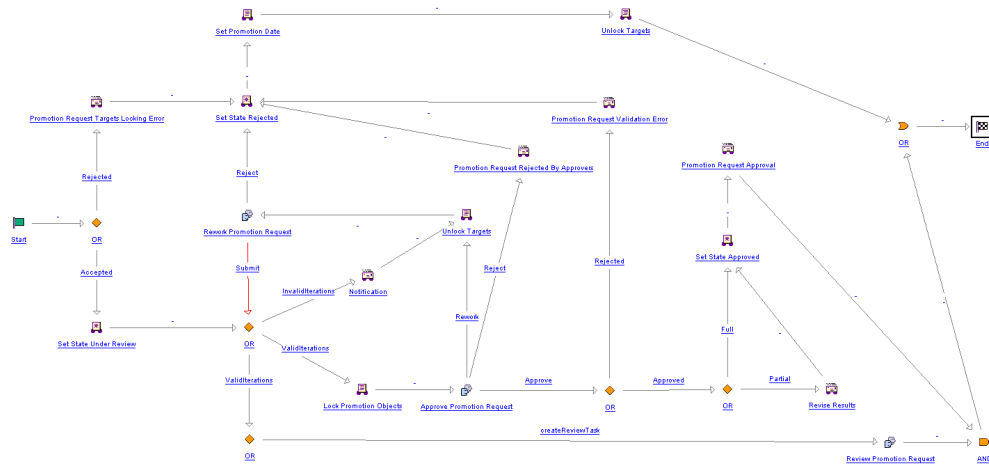
For full track change requests, schedule and facilitate CRB review and record the CRB decision.

## Problem Report Workflow



1. Submit problem report  
Submit the problem report for review.
2. Analyze problem report  
Analyze the problem report, associate the relevant analysis information, and then confirm or reject (as not verified) the problem report.
3. Clarify problem report  
The problem report is sent back to the author for the addition of further information.

## Promotion Request Approval Process Workflow



### 1. Review promotion request

Invite reviewers from the Promotion Reviewers role, as well as participants added by the requesting author, to provide comments on these objects.

### 2. Approve promotion request

Invite approvers from the Promotion Approvers role, as well as participants added by the requesting author, to approve these objects.

### 3. Rework promotion request

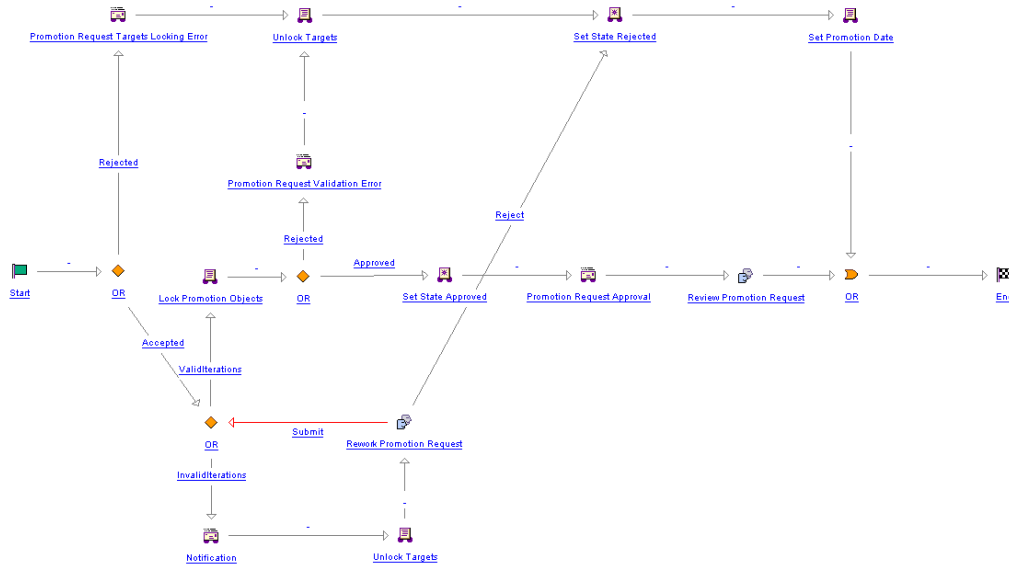
Invite the requesting author to review comments from one or more of the approvers, adjust the objects based on suggestions, and refresh the objects for approval.

### Note

Ensure all promotion candidates are checked in. Otherwise, task assignees must complete a rework task before proceeding.

This behavior is controlled by the Default Promotion Request Business Rule Set. For more information about business rules, see *PTC Windchill Administration - Configuring Your PTC Windchill Environment*.

## Promotion Request Review Process Workflow



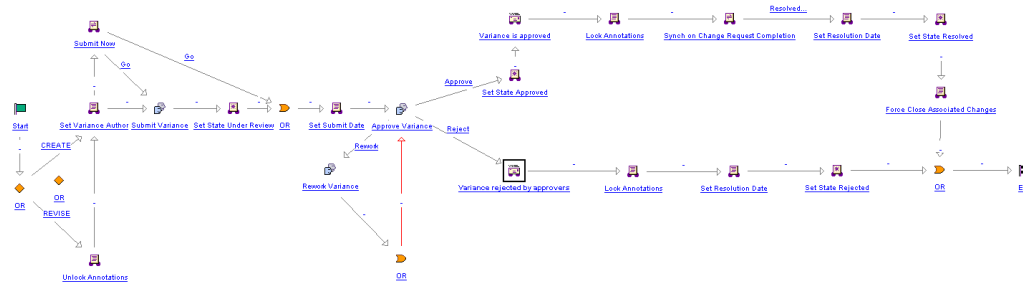
The Review Promotion Request workflow routes the promotion request to a group of people to review and comment on the objects. All objects on the promotion request are automatically promoted to the requested life cycle.

### Note

Ensure all promotion candidates are checked in. Otherwise, task assignees must complete a rework task before proceeding.

This behavior is controlled by the Default Promotion Request Business Rule Set. For more information about business rules, see *PTC Windchill Administration - Configuring Your PTC Windchill Environment*.

## Variance Workflow



### 1. Submit variance

Submit the variance for approval.

### 2. Approve variance

Validate the variance, review the identified variance objects and then approve, reject, or request rework by the variance author.

### 3. Rework variance

Rework the variance and resubmit for approval.

## Adding Change Locks to a Workflow Template

Change locks are intended to prevent modifications to annotations. Use the following steps to add a change lock or unlock expression to your workflow template.

### Lock Annotations

Lock annotations after a change object is confirmed, approved, completed, resolved, or rejected:

Create a new expression and enter “Lock Annotations” in the **Name** field and enter the following in the **Expression** tab:

```
wt.fc.collections.WTSet revisedChangeObjects =
wt.fc.collections.CollectionsHelper.singletonWTSet
(primaryBusinessObject);
```

```
wt.change2.ChangeLockHelper.service.lockRelatedMaterials(revisedChangeObjects,
wt.change2.ChangeApplicationLock.LOCK_SUPPORTINGMATERIAL);
```

### Unlock Annotations

Unlock annotation after a change object has been revised:

---

Create a new expression and enter “Unlock Annotations” in the **Name** field and enter the following in the **Expression** tab:

```
wt.fc.collections.WTSet revisedChangeObjects =  
wt.fc.collections.CollectionsHelper.singletonWTSet  
(primaryBusinessObject);  
  
wt.change2.ChangeLockHelper.service.unlockRelatedMaterials  
(revisedChangeObjects,  
wt.change2.ChangeApplicationLock.LOCK_SUPPORTINGMATERIAL);
```

For more information, see “Change Locks” in the PTC Windchill Help Center.

## Out-of-the-Box Process Images

Process images are available out-of-the-box for routing and change management processes and can be associated with workflow templates via the Workflow Template Administration utility. Process images can also be edited to correspond with changes you make to the workflow templates.

Process images are graphical overviews of the workflow process providing an at-a-glance summary of the process flow. They can also include textual descriptions of the process flow.

Once the process images have been associated with the workflow templates, they can be viewed from the **Tasks** table in the context of a specific routing task or change request. They provide the end-user with a quick look at the process flow and the behavior of the task in which they are participating.

For detailed procedures for editing and associating process images to the workflow templates, see the Workflow Template Administration help.

## Workflow Template Execution Flags

The workflow engine uses several flags to control behavior during the execution of the workflow. These flags default to wt.property values. Execution flags fall into three categories:

- Process - These flags affect the entire workflow process.
- Activity - These flags affect individual workflow activities.
- Both process and activity - These flags are meaningful for both workflow processes and workflow activities.

## Process Flags

These flags are meaningful only to workflow processes.

---

 **Note**

The associated properties are preceded by `wt.workflow.engine` in `wt.properties`.

---

| Flag                                 | Description   |
|--------------------------------------|---|
| <b>Create process - record</b>       | Associated property: <b>recordProcessCreation</b><br>Determines if the workflow process creation events are recorded as part of the workflow history. You can change the value of this property for a specific process by altering its execution characteristics.   |
| <b>Create process - emit</b>         | Associated property: <b>emitProcessCreation</b><br>Determines if workflow process creation events should be emitted as a keyed event. This event can be listened to and used for synchronization and other purposes. You can change the value of this property for a specific process by altering its execution characteristics.                              |
| <b>Change process state - record</b> | Associated property: <b>recordProcessStateChange</b><br>Determines if the workflow change of state events should be recorded as part of the workflow history. You can change the value of this property for a specific execution object by altering its execution characteristics.  |
| <b>Change process state - emit</b>   | Associated property: <b>emitProcessStateChange</b><br>Determines if the workflow state change events that occur with processes should be emitted as a keyed event. This event can be listened to and used for synchronization and other purposes. You can change the value of this property for a specific process by altering its execution characteristics. |
| <b>Change process data - record</b>  | Associated property: <b>recordProcessDataChange</b><br>Determines if the workflow change of data events should be recorded as part of the workflow history. You can change the value of this property for a specific execution object by altering its execution characteristics.  |
| <b>Change process data - emit</b>    | Associated property: <b>emitProcessDataChange</b><br>Determines if the workflow state change events that occur with processes should be emitted as a keyed event. This event can be listened to and used for synchronization and  |



| Flag                              | Description   |
|-----------------------------------|---|
|                                   | other purposes. You can change the value of this property for a specific process by altering its execution characteristics.   |
| <b>Execution error - record</b>   | Associated property: <b>recordException</b><br>Determines if the workflow execution exceptions should be recorded as part of the workflow history. You can change the value of this property for a specific execution object by altering its execution characteristics.   |
| <b>Execution error - emit</b>     | Associated property: <b>emitException</b><br>Determines if workflow execution exception should be emitted as a keyed event. This event can be listened to and used for synchronization and other purposes. You can change the value of this property for a specific execution object by altering its execution characteristics. |
| <b>Notify on exception</b>        | Associated property: <b>notifyOnException</b><br>This event can be listened to and used for synchronization and other purposes. You can change the value of this property for a specific process by altering its execution characteristics.   |
| <b>Abort process on exception</b> | Associated property: <b>abortProcessOnException</b><br>Determines whether to abort the workflow when an exception occurs. If true, the process instance is aborted if a contained activity aborts.  |
| <b>Notify on overdue</b>          | Associated property: <b>notifyOnOverdue</b><br>Determines whether a notification should be sent to the participants in the overdue notification list when the process or activity is overdue. You can change the value of this property for a specific process by altering its execution characteristics.                       |
| <b>Notify on complete</b>         | Associated property: <b>notifyOnComplete</b><br>Determines whether a notification should be sent to the process responsible when the execution object completes. You can change the value of this property for a specific process by altering its execution characteristics.  |
| <b>Notify on past deadline</b>    | Associated property: <b>notifyOnPastDeadline</b><br>Determines whether a notification should be sent to the process responsible after some time has elapsed since the execution object completed. The time is defined in an attribute if the object is past the deadline.   |
| <b>Notify on</b>                  | Associated property: <b>notifyOnApproachingDeadline</b>   |

| Flag                                    | Description   |
|---|---|
| <b>approaching deadline</b>             | Determines whether a notification should be sent to the process responsible when the time to deadline has been reached. You can change the value of this property for a specific process by altering its execution characteristics.   |
| <b>Asynchronous execution</b>           | Associated property: <b>asynchronousExecution</b><br>Determines if the execution of an activity is asynchronous, that is, not terminated when the host process or block completes. If an asynchronous activity occurs in a loop, one may have several instances of the same activity template executing concurrently.   |
| <b>Has dedicated queue</b>              | Associated property: <b>dedicatedQueueMode</b><br>Determine whether workflow processes have dedicated queues for event propagation and user work. <ul style="list-style-type: none"> <li>• <code>true</code>—Enable dedicated queues for processes. You might want a dedicated queue for a process when you want to prevent its execution from being affected by other workflows.</li> <li>• <code>false</code>—Queues are shared between workflow processes. This is the default value.</li> </ul> This attribute is used when the <b>dedicatedQueueMode</b> property is set to <code>propagation</code> , <code>userWork</code> , or <code>all</code> .<br>You can control this property in an individual process base by setting the appropriate execution flag in the process template. |
| <b>Select Latest Template Iteration</b> | Associated property: <b>useLatestTemplateIteration</b><br>Determines whether the latest iteration of a specific version of an object is used the first time the subprocess is encountered in the workflow. If the subprocess template is iterated and then the process loops back, the initial version (not the iterated version) continues to be used because the subprocess referenced that version.<br>The default value is <code>true</code> , which means that the latest iteration is used the first time the subprocess is encountered.  |

---

## Activity Flags

These flags are meaningful only to workflow activities.

---

### Note

The associated properties are preceded by `wt.workflow.engine` in `wt.properties`.

---

| Flag                                  | Description   |
|---------------------------------------|---|
| <b>Change activity state - record</b> | Associated property: <b>recordActivityStateChange</b><br>Determines if the workflow state change events that occur with activities are recorded as part of the workflow history. You can change the value of this property for a specific process by altering its execution characteristics.  |
| <b>Change activity state - emit</b>   | Associated property: <b>emitActivityStateChange</b><br>Determines if workflow state change events that occur with activities should be emitted as a keyed event. This event can then be listened to and used for synchronization and other purposes. You can change the value of this property for a specific activity by altering its execution characteristics. |
| <b>Change activity data - record</b>  | Associated property: <b>recordActivityDataChange</b><br>Determines if the workflow change of data events that occur with activities are recorded as part of the workflow history. You can change the value of this property for a specific process by altering its execution characteristics.   |
| <b>Change activity data - emit</b>    | Associated property: <b>emitActivityDataChange</b><br>Determines if workflow change of data events that occur with activities should be emitted as a keyed event. This event can be listened to and used for synchronization and other purposes. You can change the value of this property for a specific activity by altering its execution characteristics.     |
| <b>Change assignment - record</b>     | Associated property: <b>recordAssigneeChange</b><br>Determines if workflow change of assignment events should be recorded as a part of the workflow history. The value of this property for a specific activity can be changed by altering its execution characteristics.   |

| Flag                            | Description   |
|---------------------------------|---|
| <b>Change assignment - emit</b> | Associated property: <b>emitAssigneeChange</b><br>Determines if workflow change of assignment events should be emitted as a keyed event. This event can be listened to and used for synchronization and other purposes. You can change the value of this property for a specific activity by altering its execution characteristics.                            |
| <b>Ignore unresolved Role</b>   | Associated property: <b>ignoreUnresolvedRoles</b><br>Determines whether unresolved roles should be ignored rather than automatically assigned to the responsible role. If set to true and all roles in an activity are unresolved, no work item is generated without an indication that something went wrong. This is the global installation default behavior. |

## Both Process and Activity Flags

These flags are meaningful to both workflow processes and activities.

### Note

The associated properties are preceded by `wt.workflow.engine` in `wt.properties`.

| Flag                            | Description   |
|---------------------------------|---|
| <b>Execution error - record</b> | Associated property: <b>recordException</b><br>Determines if the workflow execution exceptions should be recorded as part of the workflow history. You can change the value of this property for a specific execution object by altering its execution characteristics.   |
| <b>Execution error - emit</b>   | Associated property: <b>emitException</b><br>Determines if workflow execution exception should be emitted as a keyed event. This event can be listened to and used for synchronization and other purposes. You can change the value of this property for a specific execution object by altering its execution characteristics. |
| <b>Notify on abort</b>          | Associated property: <b>notifyOnAbort</b>   |

| Flag                       | Description  |
|----------------------------|--|
|                            | Determines whether a notification should be sent to the process or activity responsible when the process or activity aborts. You can change the value of this property for a specific process by altering its execution characteristics.   |
| <b>Abort on exception</b>  | Associated property: <b>abortOnException</b><br>Determines whether to abort the activity or process if an exception occurs during its execution.   |
| <b>Reassign on overdue</b> | Associated property: <b>reassignOnOverdue</b><br>Automatically reassigns the process or activity when the process or activity is overdue. The new assignee is read from a variable named <code>reassignPrincipal</code> . You can change the value of this property for a specific activity by altering its execution characteristics.   |
| <b>Complete on overdue</b> | Associated property: <b>completeOnOverdue</b><br>Determines whether an activity or process is automatically completed once it is overdue.  |
| <b>Skip on overdue</b>     | Associated property: <b>skipOnOverdue</b><br>Automatically skips the process or activity when the process or activity is overdue. Note that an execution object can be skipped only if it has not been started. Also this transition needs to be as the event of an outgoing link for it to be propagated. You can change the value of this property for a specific activity or process by altering its execution characteristics. |

## Modifying Execution Flags

To modify the execution flags, use the `SetConfiguration` tool.

### Running SetConfiguration

To run `SetConfiguration`, issue the following command:

```
java wt.clients.workflow.definer.SetConfiguration
Y:\Windchill>java wt.clients.workflow.definer.SetConfiguration
Inspection Runtime Mode = true
Windchill DataStore: Oracle

Workflow process templates

>> 1. Submit - (10003aaa)
```

- 
2. Review - (10003aaa)
  3. Problem Report Workflow - (10003aaa)
  4. Change Request Workflow - (10003aaa)
  5. Change Notice Workflow - (10003aaa)
  6. Change Activity Workflow - (10003aaa)
  7. Promotion Request Approval Process - (10003aaa)
  8. Promotion Request Review Process - (10003aaa)
  9. Approval Process - (1001faaa)
  10. Notify Process - (1005faaa)
  11. Release Process - (1005faaa)
  12. Review Process - (1005faaa)
  13. Two Level Approval Process - (1001faaa)
  14. Change Notice Workflow - (10003aaa)

Activity templates of selected process:

>> 1. Submit - (10003aaa)

Set template configuration

-----

1. Select process template
2. Show/edit process template configuration
3. Select activity template
4. Show/edit activity template configuration
5. Refresh templates
6. Exit

>>> Choose an option:

This tool shows a list of workflow templates, with the active template selected with the >> symbol. The next list is a list of the activities of the selected process templates. The active activity is shown with the >> symbol. In our example above, the Submit process template is active and the Submit activity is the active activity within the Submit process. To change the active process template, choose option 1. To change the active activity, select option 3.

---

To modify an exception flag, choose option 2. To modify an activity flag choose option 4. A list of flags is shown. For example if you choose 4:

```
Y:\Windchill>java wt.clients.workflow.definer.SetConfiguration
Introspection Runtime Mode = true
Windchill DataStore: Oracle
```

```
Workflow process templates
```

```
>>  1. Submit - (10003aaa)

      2. Review - (10003aaa)

      3. Problem Report Workflow - (10003aaa)

      4. Change Request Workflow - (10003aaa)

      5. Change Notice Workflow - (10003aaa)

      6. Change Activity Workflow - (10003aaa)

      7. Promotion Request Approval Process - (10003aaa)

      8. Promotion Request Review Process - (10003aaa)

      9. Approval Process - (1001faaa)

     10. Notify Process - (1005faaa)

     11. Release Process - (1005faaa)

     12. Review Process - (1005faaa)

     13. Two Level Approval Process - (1001faaa)

     14. Change Notice Workflow - (10003aaa)
```

```
Activity templates of selected process:
```

```
>>  1. Submit - (10003aaa)
```

```
Set template configuration
```

```
-----
```

```
1. Select process template
2. Show/edit process template configuration
```

- 
3. Select activity template
  4. Show/edit activity template configuration
  5. Refresh templates
  6. Exit

>>> Choose an option:

Selecting an option toggles the value to either true or false.

## Saving Your Work

To save the configuration, select either option 30 or 31. Make sure that the relevant workflow process template is checked out. Also, make sure that all existing instances of the relevant process template are terminated. If one of these conditions is not met, an exception is thrown.

New workflow processes will use the new behavior defined by these execution flags.

## Electronic Signatures

Windchill products allow you to require electronic signatures on workflow activities to authenticate the activity.

### Electronic Signature Setup

If the eSignatures are in an LDAP directory that has already been established for Windchill, there is no additional setup required.

If an LDAP directory is not used with Windchill, you can use the JNDI adapter to validate authentication. See the *PTC Windchill Installation and Configuration Guide* for information about creating a JNDI adapter entry and repository description.

---

#### Note

To use a JNDI adapter for electronic signature authentication, the following fields in the JNDI adapter definition must be populated with the distinguished name and password to be used to authenticate requests made to the LDAP directory service:

- Directory System Agent User
  - Directory System Agent Credentials
-



---

You must identify the directory in the **wt.org.electronicIdentity.authenticationService** property. From a windchill shell, execute the following commands:

- To display the current value of the property:

```
xconfmanager -d wt.org.electronicIdentity.authenticationService
```

- Specify the existing and new value (append new value to the existing property value). You can specify one or more JNDI adapter Service Names. Use a comma to separate the adapter names. See the xconfmanager guidelines for specifying multiple property and property value combinations:

```
xconfmanager -s wt.org.electronicIdentity.authenticationService=  
<JNDIadapter service name(s)> -t <Windchill>/codebase/  
wt.properties -p
```

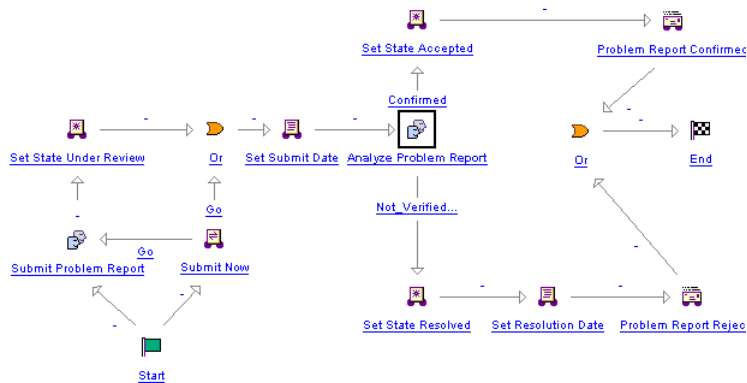
Where *<Windchill>* is the location where Windchill is installed.

- The parameter `wt.org.electronicIdentification.class` can be set to determine the authentication required. The parameter can be set as follows:
  - `wt.org.electronicIdentity.engines.LDAPPASSWORDSignatureEngine` – this signature engine only requires a password to be supplied. It verifies that the password belongs to the currently logged in user.
  - `wt.org.electronicIdentity.engines.LDAPFDACompliantSignatureEngine` – this signature engine requires both a user name and a password field to be entered, in compliance with FDA rule 21 CFR part 11 section 11.2. It verifies that the user name and password belong to the currently logged in user.

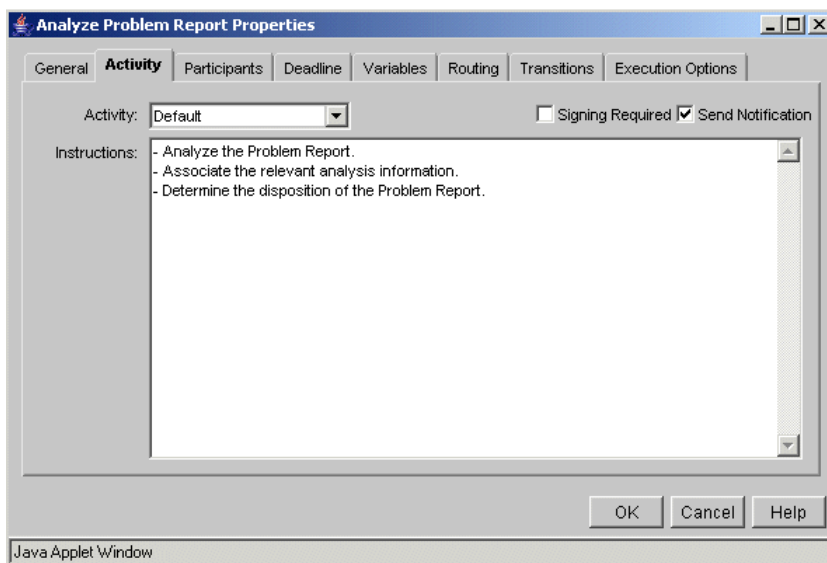
## Requiring Electronic Signatures in a Workflow

To require electronic signatures, perform the following steps:

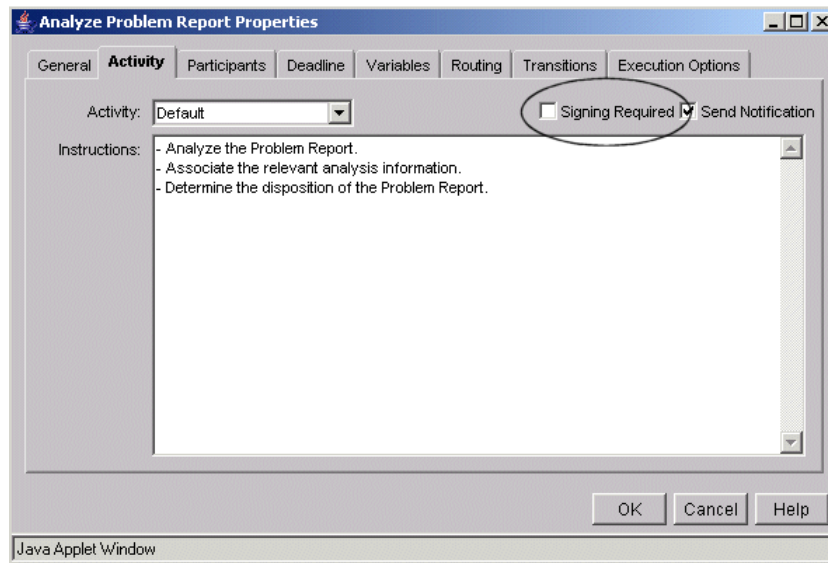
1. Use the Workflow Template Administration utility to make an electronic signature required for a particular activity. When you create or edit a process template, the process window appears.



2. If you double-click the activity, or right-click the activity and select **Properties**, a properties window appears. In this window, select the **Activity** tab.



3. Select the **Signing Required** checkbox to require an electronic signature at this point in the process.



---

 **Note**

If you select **Signing Required**, you are prompted for authentication in order to start the activity.

---

## Best Practices

The following sections contain best practices for workflow templates and processes.

### Access Control and Workflow Templates

Access control is generally defined for the domain to which an object belongs. However, it is possible to specifically add unique ad hoc access control rules to a Windchill object (such as a specific part or document). For example, you can use ad hoc access control rules inside a workflow, or you can define object-level ad hoc access control rules using the **Edit Access Control** action.

If you are likely to have an extremely high number of running workflow activities referencing the same object, make sure that you grant ad hoc access only as needed. Use policy access control where appropriate.

For more information, see the Access Control information in the *PTC Windchill Specialized Administration Guide*.

---

## Access Control and Process Nodes

Access control permissions are not checked for expressions in a workflow activity or robot node. You can use the Windchill API if your process requires that access control permissions are enforced within expression execution. The following is an example of the appropriate code:

```
boolean oldAccessEnforcedSetting = SessionServerHelper.manager.setAccessEnforced(true);
try {...
    // workflow expression code
    ...
}finally{
    SessionServerHelper.manager.setAccessEnforced(oldAccessEnforcedSetting);
    // At the end of your code, reset access check setting to its initial value
}
```

---

### **Caution**

You must ensure that the access check setting is reset to its original value at the end of the code.

---

## Using a Single Workflow in a Life Cycle Having Multiple States

Duplicate tasks get started when a Set State robot is used along with a loop link to the task related to the new state.

In order to avoid this situation, create an initial dummy life cycle phase that is associated with the workflow and that represents a state that is never returned to in a loop or in a set state robot.

---





### **Note**

When you assign a workflow template to a life cycle template, you see a list of valid workflows. The list of valid workflow templates includes the ones defined in the given application context, plus those defined in the ancestor organization and site contexts. Workflow templates defined in a subcontext override and filter out the workflow templates defined in parent contexts having the same name.

---

## Workflow Process Support in Windchill ProjectLink

The following table shows the workflow process support in Windchill ProjectLink.

| Feature   | Support Level | Notes   |
|---|---------------|---|
| Use of Workflow Template Administration interface | Partial       | Site and organization administrators can see all templates in the context from which they launched the Workflow Template Administration utility and those inherited from ancestor contexts. In Windchill ProjectLink, you can launch the Workflow Template Administration utility from the <b>Utilities</b> page of the <b>Organizations</b>  and the <b>Site</b>  contexts. The Workflow Template Administration utility is not available in the <b>Projects</b>  or <b>Programs</b>  contexts to administrators of these contexts. From the Organization context, you will see the templates from the site and the organization context from which the utility was launched. From the organization context, the site templates can only be viewed or saved. |
| Use of workflow process editor interface          | Full          | The full capabilities of the process editor are exposed. There is no bootstrap capability with Windchill ProjectLink; therefore, a high bandwidth connection to the server is necessary to use the workflow process editor.   |
| Default task choices                              | Partial       | Life cycle and default task types are supported. Change tasks are not supported.  |
| Email task delivery                               | Full          | All tasks can be delivered by email, in addition to being added to the user's <b>Tasks</b> table.   |
| Ad hoc task support                               | None          | There is no support for ad hoc workflow tasks.  |
| Custom task form used and definition              | None          | Windchill ProjectLink default task forms are rendered as JSP pages. However, an administrator can create custom task forms. For more information, see "Using Custom Task Form Templates" in the workflow help.  |
| Electronic signature support                      | Full          | Windchill ProjectLink requires additional authentication, as specified by the signature engine, for tasks generated from activities that require signing.   |
| Activity-based access control                     | Partial       | Activity-based access control can be used for the primary business object only. Access right can only be added to the rights currently defined for the  |

| Feature               | Support Level | Notes   |
|-----------------------|---------------|---|
|                       |               | object. Access rights cannot be removed.  |
| Variable support      | Partial       | All standard variables are supported. Variables that represent Windchill classes can be defined and used, but will not be rendered in the task.   |
| Routing               | Full          | Exclusive and nonexclusive manual routing is supported. Automatic routing is supported via expressions. Routing selections are displayed only for required roles.   |
| Robots                | Full          | Notification, set state, timer, execution, and expression robots are all supported.   |
| Connectors            | Full          | Start, stop, and, or, and threshold connectors are all supported.   |
| Process references    | Full          | Only processes defined for the organization associated with the logged-in user may be referenced.   |
| Blocks                | Full          | A block represents a group of activities, connectors, or robots. Reduce process complexity by creating blocks of activities that can be expanded when needed.   |
| Transition conditions | Full          | Transition is movement from one internal state to another within a workflow template. This movement reflects a change in the workflow status. Conditions are defined on the Transitions tab for an activity.  |
| Roles                 | Partial       | Roles that are referenced must be satisfied in the project or program instance associated with the process instance.  |
| Voting                | Full          | Voting support is limited to Review and Promote activity types.   |
| Variable substitution | Full          | Variable support is limited. Variables representing Windchill classes can be defined and used, but will not be displayed in the task pages.   |
| Import/export         | Partial       | Process templates can be exported to XML format. There is no organization association with the imported or exported template so the workflow import/export folder should be cleared between uses.   |
| Process initiation    | Partial       | Within Windchill ProjectLink, a workflow process cannot be explicitly initiated by an end user. A workflow process may be instantiated indirectly only by creating a life cycle managed object or by initiating a routing action. Through a customization, it is also possible that a workflow process could be |

| Feature   | Support Level | Notes   |
|---|---------------|---|
|   |               | initiated within a project.   |
| Participation identification                          | Partial       | Participation in a downstream task can be accomplished through the use of user and group variables that are satisfied by an assignee in a task form. You can add or remove assignees from a running process by updating the route participants. The change applies to unstarted started activities, it will not affect tasks that are currently running. There is no support for the setup participants capability. |
| Content holder access                                 | None          | There is no workflow content holder exposed in a workflow task.   |
| Ad hoc tasks  | None          | Ad hoc tasks cannot be created from a parent task.  |
| Access to primary business object                     | Partial       | A link to the subject is provided.  |
| Adding comments                                       | Partial       | A link to the subject's discussion forum is available in the task form. Comments can also be added to a string variable.  |
| Task actions  | Partial       | A user can open and reassign tasks, but there is no capability to delegate them or to access a user calendar. When tasks are reassigned, the assignee pool is the project or program team.  |
| Tasks customization                                   | None          | The <b>Tasks</b> tables support multiple predefined views. There is no capability to further define custom views.   |
| Project or Program tasks view                         | Full          | There is a specific view of all tasks in a project or program.  |
| Access to the Workflow Process Manager                | Partial       | There is no access to the process manager for a general workflow user.  |
| Access to workflow participation or execution history | Partial       | Windchill ProjectLink exposes no explicit access to workflow participation or history information for non-administrators. However, individual task forms can accumulate information regarding participation and disposition. Comment history can be captured in a discussion forum associated with the primary business object.   |

---

| <b>Feature</b>                               | <b>Support Level</b> | <b>Notes</b>  |
|--|----------------------|---|
| Local search support for process information | None                 | There is no support for searching running or completed processes. |
| Workflow process management                  | Partial              |   |



# 13

## Understanding Context Templates

|   |     |
|---|-----|
| Out-of-the-box Context Templates .....                                    | 394 |
| Methods of Creating Additional Context Templates .....                    | 394 |
| Creating Business XML Files for Context Templates .....                   | 396 |
| Required Contents of Files Used to Create a Context Template .....        | 396 |
| ZIP File Contents of an Exported Context Template .....                   | 398 |
| Required Contents of ZIP File Used for Importing a Context Template ..... | 399 |
| Managing Context Templates .....  | 401 |

This section provides details on how to create and manage context templates.

---

### **Note**

Many of the descriptions in this section assume you are familiar with XML. The XML files that are used must be coded against the `standardX26.dtd`. You can download the `standardX26.dtd` by downloading any of the context templates. The DTD is contained in the downloaded ZIP file.

---

---

## Out-of-the-box Context Templates

An initial set of context templates was loaded when your Windchill solution was installed. For a list of the loaded templates, see [Installed Site Templates on page 76](#). For details about the loaded templates, see the following:


- For organization templates, see [Out-of-the-box Organization Templates on page 147](#).
- For product and library templates, see [Out-of-the-box Product and Library Context Templates on page 182](#).
- For program and project templates, see [Out-of-the-box Project and Program Templates on page 241](#).

The XML elements in the template load files are basically the same as those used for the import and export functionality. However, there are minor variations and the load files are not meant to be used directly when you create new context templates.


## Methods of Creating Additional Context Templates

Only site administrators can create organization templates. Site and organization administrators can create product, library, program, and project templates.

You can create additional context templates in the following ways:

- Using the new template icon  to create a template using a custom context template input file. This option is available for all contexts. For more information, see [Create a Context Template with a New Input File on page 394](#).
- Using the Save as Template action to create a new template from the current context. This option is only available for application contexts. For more information, see [Create a Template from the Current Context on page 395](#).
- Using the Export as Template action to export the current product, library, project, or program context as a template. This option is only available for application contexts. For more information, see [Create a Context Using Export on page 395](#).

### Create a Context Template with a New Input File

You can include an additional context template by creating the input file manually, select the appropriate view from the view drop-down list, and click the new template icon  from the **Templates** table to create the template. This is the only

---

option available for creating an organization template. For more information on the required contents of the file that is used, see [Required Contents of Files Used to Create a Context Template on page 396](#).

## Create a Template from the Current Context


The **Save as Template** action provides a way to create a new template from the current context.


A newly created product, library, program, or project template is saved in the organization context that is a parent of the current context and appears in the **Templates** table of that context when the table view is set for that context template type.




## Create a Context Using Export

The **Export as Template** action allows you to export the current product, library, program, or project context as a template by creating a ZIP file on your system.

For more information on the contents of the exported ZIP file, see [ZIP File Contents of an Exported Context Template on page 398](#).

You can import an exported template by navigating to either the site or the organization under which you want the template imported and clicking the **Templates** link. From the **Templates** table that appears, select the type of template from the view and click the import from file icon . For more information on the required contents of the ZIP file that is imported, see [Required Contents of ZIP File Used for Importing a Context Template on page 399](#).

Using the import from file icon  creates a template with the same name as the exported template. If you want to specify a different name for the template, you can do either of the following:



- Select the new template icon  instead of the import from file icon . On the window that opens, you specify the name and description of the template. This information is used in place of the name and description in the ZIP file.
- Modify the contents of the `TAG-ContainerTemplate-0.xml` file that is in the exported ZIP file to change the name and description of the template and then use the import from file icon  to import the exported template.

The import and create functions do not validate that the input XML conforms to the DTD; you must do this before doing the import or create function.

---

## Creating Business XML Files for Context Templates

Business XML files are used as input for create and import activities (see [Methods of Creating Additional Context Templates on page 394](#)):

- Using the import from file icon  requires that the business XML file and additional files (as described in [Required Contents of ZIP File Used for Importing a Context Template on page 399](#)) be packaged in a ZIP or JAR file.
- When using the new template icon , the business XML file can be used alone as the input when no additional content files are referenced in the business XML file, or it can be used in a ZIP or JAR file when additional content files are referenced in the XML file.


All business XML files must start with the following lines:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE context_type SYSTEM "standardX26.dtd">
```


where *context\_type* is one of the following:

- `OrganizationConfig` for organization templates
- `ProductConfig` for product templates
- `LibraryConfig` for library templates
- `ProjectConfig` for project and program templates

## Required Contents of Files Used to Create a Context Template

When creating a context template from the Templates table using the new template icon , you must supply a file containing the content of the template. The input file can be just the business XML file if no additional content is needed or it can be a ZIP (or JAR) file that has both the business XML file and other content files named in the XML file.

The input file you provide in the create operation is not the same as the file used for importing. For a create operation, you can use a file that you manually create; however, PTC recommends that you always start with a business XML file that you have either downloaded or located in the Windchill installation directory. If you do use one of the Windchill load files as your starting point, PTC recommends that you do not modify the ENTITY tags in the file nor modify the content of any of the XML files referenced in the ENTITY tags.

The following sections describe the contents of the files you can use as input when you create context templates using the new template icon .

---

## Organization Templates

The only option available for creating an organization template is to create the input file manually and create a new template. For more information, see [Create a Context Template with a New Input File on page 394](#).

You can include the following administrative items in a new organization template:

- Additional domains, folders, user-defined groups, and access control policy rules for the organization. The access control rules can include rules set for the dynamic roles that are available in the organization context. For additional information, see [Using Dynamic Roles on page 100](#).
- Additional product, library, program, and project templates that are available from the organization.
- Object initialization rules.
- Project roles (if the organization is used with Windchill ProjectLink).

## Product and Library Context Templates

When using any of the options for creating templates, you can include the following administrative items in a new product or library template:

- Domains
- Folder structure (not including the folder contents)
- Team roles (including role access to actions)
- Team members
- Document templates
- Object initialization rules
- Access control policy rules
- Template visibility
- Preferences

## Program and Project Context Templates

When using any of the options for creating templates, you can include the following administrative items in a new program or project template:

- Domains
- Folder structure (not including the folder contents)
- Folder links and structure
- Project or program plan
- Deliverables

- 
- Team roles (including role access to actions)
  - Team members
  - Documents
  - Document templates
  - Discussion specification
  - Discussion template
  - Object initialization rules
  - Template visibility
  - Shared objects in a project (if any have been created in an existing project that is exported)
  - Preferences

Additionally, you can save an existing project (or program) as a new project (or program). Using this option creates a duplicate of a project (or program) under a new name.

## ZIP File Contents of an Exported Context Template

The ZIP file created on your system from an **Export as Template** action contains the framework options you selected. Depending on your system configuration, you may be prompted to save the ZIP file or the file may be saved on your local drive with the name `<context_name>_generated_template<integer>.zip`, where `<context_name>` is the name of the product, library, program, or project being exported and `<integer>` is an integer that ensures that the file has a unique name when the download occurs. The name used is not significant and can be changed.

The ZIP file contains the following:

- The `importList.txt` file, which is not currently used during an import and can be ignored.
- The `TAG-ContainerTemplate_<integer>.xml` file, which contains information about container template itself, such as name and container class of the template. Here also, `<integer>` is used to ensure that the files are unique.
- The `TAG-0.xml` file (which is in the `CONTENTS` directory) lists the contents

---

of the exported template. This file is also known as the business XML file and contains information that is used when creating a container from this template (for example, folder structure, access control policy rules, and so on).

- Additional files that make up the contents of the exported template. If unzipped, these files are put in the CONTENTS directory. For example, the ZIP file of a program or project template could contain documents and document templates that then belong in the CONTENTS directory.

## Required Contents of ZIP File Used for Importing a Context Template

The ZIP file you use to import a context template must have the same basic structure as the ZIP created when exporting a context template (as described in the previous section). The ZIP file must contain the following:

- An XML file at the top level of the ZIP that contains the definition of the context template itself, such as name and container class of the template. This corresponds to the TAG-ContainerTemplate\_<integer>.xml file that is generated in an export. For more information on the content of this file, see [Contents of Top-level XML File for Imported Templates on page 400](#).
- The business XML file (which is defined as coming from the CONTENTS directory) that lists the contents of the template you want to import and contains information that is used when creating a container from this template (for example, folder structure, access control policy rules, and so on). This is also known as the TAG-0.xml file that is generated on export. The name of this file must match the file named in the zipEntry element in the top-level XML file. For more information on the content of the business XML file, see [Creating Business XML Files for Context Templates on page 396](#).
- Additional files to include in the contents of the template you want to import. These files are named in the business XML file to be added as content items through the use of the contentItem element. Before creating the ZIP file, put these files in the CONTENTS directory. Examples of files that can be in this directory are documents and document templates that you want to import as part of a Windchill ProjectLink project template.

---



### Note

The file used could also be a JAR file rather than a ZIP file.

---

---

## Note

The ZIP file created by selecting the **Download** action from the right-click actions menu of a context template row on the **Templates** table cannot be used as the template data file for creating a context template using the import from file icon ; it does not contain all of the required information that is needed to create a new context template. The downloaded ZIP file can be used to update an existing context template or create a template using the new template icon .

---

## Contents of Top-level XML File for Imported Templates

The top-level XML file is used to define the template that you are importing. The file must begin with the following lines:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ContainerTemplate SYSTEM "standardX26.dtd">
```

The content of the top-level XML file is defined by the following DTD element:

```
<!ELEMENT ContainerTemplate (name,
                             description?,
                             containerClassName,
                             defaultValuesRule?,
                             locale?,
                             enabled?,
                             updateIf?,
                             (xmlText | loadPath | zipEntry)?)>
```

The following example illustrates how to use the `ContainerTemplate` element to define the template you want to import. The example is for a Windchill PDMLink product template as signified by the use of `wt.pdmlink.PDMLinkProduct` in the `containerClassName` element.

In the example, the name of the template is `DEMO Product Template` and, when the template is imported, it is enabled and visible. The business XML file that contains the content of the template is contained in the `CONTENTS/DEMOProductTemplate.xml` file that is in the imported ZIP file:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ContainerTemplate SYSTEM "standardX26.dtd">
<ContainerTemplate>
  <name>DEMO Product Template</name>
  <description>A description of the DEMO template</description>
  <containerClassName>wt.pdmlink.PDMLinkProduct</containerClassName>
```



```
<enabled>true</enabled>
<zipEntry>CONTENTS/DEMOProductTemplate.xml</zipEntry>
</ContainerTemplate>
```

### Note

Although the DTD element shows that you can specify the business XML file in multiple ways (through `xmlText` | `loadPath` | `zipEntry`), only the use of the `zipEntry` element is supported when you are importing a template.

To specify a project template instead of a product template, use `wt.projmgmt.admin.Project2` in the `containerClassName` element. For a library template, use `wt.inf.library.WTLibrary`. For a program template, use `com.ptc.Program`.

## Managing Context Templates

To view the set of context templates that are available from a context, view the **Templates** page for that context. From the view drop-down list on the **Templates** table, select the type of template. For example, the following picture shows the resulting **Templates** table when navigate to **Site** ► **Templates**, and the select **Organization Templates** from the drop-down list:

Name	Visibility	Enabled
Customer	Show	Yes
Demo Template	Show	No
Enterprise	Show	Yes
General	Show	Yes
General (PDM)	Show	Yes
General (PDM)	Show	Yes

From the **Templates** table, you can perform the following tasks:



- Create new templates.
- Import templates that had been previously exported (all context templates except organization templates).
- Filter the visibility of one or more of the templates.
- Enable and disable templates.

- 
- Edit template information.
  - Check out and check in updated templates.

For a template to be available for use, it must be both visible and enabled.

The following sections provide some additional information about the tasks. For task details, see the online help that is available from the **Templates** table.

## Filtering Template Visibility

You can determine a user's ability to see the templates that are listed in the **Templates** table using the show icon  and hide icon  that are located above the table rows or using the **Show** and **Hide** actions from the right-click actions menu on individual rows of the table.

When you hide a template's visibility, the template is no longer displayed when creating a context of that type in the applicable context. For example, assume that you hide the Enterprise organization template from the site **Templates** table. Then when creating an organization context, the Enterprise template is not listed in the **Template** drop-down list.

If a template is hidden in a parent context, it is also hidden in all child contexts unless you explicitly change the visibility to show the template in the child context. For example, assume you have hidden an organization context template from the site **Templates** table. Then all product or project contexts will also show the template as hidden. However, you can navigate to a project or product context and show the template in that application context.

## Enabling Templates

Enabling a template means that the template is ready for use.

All loaded templates are, by default, enabled.

When you create a new template, you can choose to enable or disable it.

Enabling or disabling a template enables or disables the template in all contexts where it is available; you cannot enable a template in one context and disable it in another.