ORACLE®

PRIMAVERA

P6 Professional Administrator's Guide for a Microsoft SQL Server Database

May 2011

Copyright

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle and Primavera are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

To view the list of third party technology disclosures related to this product, please see the *Commercial Notices and Disclosures* document for the release.

Contents

Preface

Oracle provides comprehensive, multiproject planning and control software, built on Oracle and Microsoft® SQL Server databases for organization-wide project management scalability. P6 Professional provides a client/server connection for planning- and scheduling-focused users.

In This Chapter

P6 Professional Documentation

You can access reference manuals and administrator's guides from the P6 Professional Documentation Center, located in the \Documentation\<language> folder of the P6 Professional physical media or download. Most documentation assumes a standard setup of the product, with full access rights to all features and functions.

Media packs include all files necessary to install P6 Professional applications, all manuals and technical documents related to the installation, administration, and use of P6 Professional components, and the Quick Install Guide. For information on the contents of the P6 Professional Media Pack, see the *P6 Professional Quick Install Guide*.

The following table describes documentation publications and lists the recommended readers by role. P6 Professional roles are described in the *P6 Professional Administrator's Guide*.

Title	Description
P6 Professional Administrator's Guide	Explains how to set up the P6 Professional database, servers, and components; it also provides an overview of all the components in the P6 Professional solution. The guide describes the procedures required to administer P6 Professional, including setting up security and configuring global preferences. ⬛ The P6 Professional network administrator/database administrator should read this guide.
Tested Configurations	Lists the configurations that have been tested and

Title	Description
	verified to work with P6 Professional. The network administrator/database administrator and P6 Professional administrator should read this document.
P6 Professional Standalone Installation and Configuration Guide	Explains how to install and configure P6 Professional as a standalone application.
P6 Professional Help	Explains how to use P6 Professional to plan, set up, and manage projects in a multiuser environment. If you are new to P6 Professional, use this Help to learn how to use the software effectively to plan and manage projects. The P6 Professional administrator, program manager, project manager, resource/cost manager, and team leader should read this Help.
P6 Professional User's Guide	This guide explains how to plan, set up, and manage projects in a multiuser environment. If you are new to P6 Professional, start with this guide to learn how to use the software effectively to plan and manage projects. When you need more detail, refer to the P6 Professional Help. The program manager, project manager, resource/cost manager, and team leader should read this guide.
Primavera Timescaled Logic Diagram Help	Describes how to create, modify, and manage Timescaled Logic Diagrams. Timescaled Logic Diagrams condense the project schedule displayed in the Gantt Chart into a more readable, easier to understand format that provides a snapshot of the entire project plan and the chains of activities that drive the project schedule.
P6 SDK *Web-based documentation*	Describes how to use the P6 SDK to connect to the P6 Professional database. The tables, fields, and stored procedures that you can access through the P6 SDK are described. Examples are also provided to show how you can use the P6 SDK to perform several basic tasks, such as creating a new project or assigning a resource to a project activity. The P6 Professional network administrator/database administrator should read this documentation, which is available in *local drive*\Program Files\Oracle\Primavera P6 Professional\PMSDK\Doc\ by default. Double-click the INDEX.HTML file to open the Table of Contents.

Title	Description
P3 to P6 Professional Migration Guide	This guide provides best practices for migrating your P3 data to P6 Professional, and details how P3 functionality maps to P6 Professional functionality.

Distributing Information to the Team

You can copy the online documentation to a network drive for access by project participants. Each team member can then view or print those portions that specifically relate to his or her role in the organization.

Throughout this documentation, the Security Guidance icon helps you to quickly identify security-related content to consider during the installation and configuration process.

Where to Get Documentation Updates

For the latest updates to the P6 Professional Documentation library, go to *http://download.oracle.com/docs/cd/E23006_01/index.htm*.

Where To Get Training

To access comprehensive training for all Primavera products, go to:

http://education.oracle.com

Where to Get Support

If you have a question about using Oracle products that you or your network administrator cannot resolve with information in the documentation or help, go to:

http://www.oracle.com/us/support/index.html

This page provides the latest information on contacting Oracle Global Customer Support and the support renewals process.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info* or visit *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs* if you are hearing impaired.

Layout of the P6 Professional Administrator's Guide

This book is a step-by-step guide to installing and configuring P6 Professional software modules. (This guide is not intended for users who plan to install and configure a standalone version. Those users should refer to a separate guide, the *P6 Professional R8.1 Standalone Installation and Configuration Guide*.)

This manual is organized as follows:

Overview

Provides an overview of P6 Professional software components, discusses how to plan an implementation for your organization, and offers an overview of the process of installing and configuring P6 Professional software components. Security guidelines are also outlined to assist you with creating a secure P6 Professional installation.

Database Installation and Configuration

Provides steps for using a wizard to automate the process of creating the P6 Professional database on either Oracle or Microsoft SQL Server and loading application data into the databases. This part also details how to manually create a database and use a wizard to automatically upgrade your database from previous versions of P6 Professional.

Client Installation and Configuration

This section explains how to:

- Install P6 Professional
- Install the P6 SDK (Software Development Kit)
- Create and run an unattended setup
- Configure module connectivity to the P6 Professional database
- Install Job Service

P6 Professional Application Administration

Describes how to customize P6 Professional applications, once installed. Specifically, this section covers how to:

- Set up users and configure security
- Modify application settings and global enterprise data
- Set up authentication and provision users

Tips

Throughout this documentation, the Security Guidance icon helps you to quickly identify security-related content to consider during the installation and configuration process. See **Security Guidance** (on page 21) for more information about security guidelines.

Planning Your Implementation

Read this chapter when you are ready to plan your P6 Professional implementation. For more detailed information and assistance, please consult with Oracle Global Customer Support (if you have questions about installation) or Oracle Primavera GBU Consulting (if you want Oracle Primavera to assist you with your implementation.)

In This Section

Which Components Do I Need?

When planning your P6 Professional implementation, you will first need to know which client modules and server components you will need to install and configure, and where those modules and components need to be installed. The following is a set of questions that you will want to answer before you begin.

Which relational database management system (RDBMS) will we use on our database server?

You can use either Oracle or Microsoft SQL Server on your database server for most P6 Professional installations.

Which workstations will require P6 Professional?

All P6 Professional users will need access to the database server. If using Oracle as the RDBMS, you will need to install the Oracle client software on each computer that runs this client module. If using Microsoft SQL Server as the RDBMS, the required Microsoft SQL Server files have already been included with Windows.

Do we want our administrators to install P6 Professional using standardized preconfigured settings?

If you want your client module to be configured identically, your administrators can run an unattended setup based on a standard configuration. You can create one or more sets of unattended setup files and share them on a network server.

Do we need to integrate our project data with other global systems?

If you need to integrate your project data with other global systems, such as Accounting or Human Resources applications, you will need to install the P6 SDK on computers that require access to the data. The P6 SDK makes project data available to external applications through Open Database Connectivity (ODBC) interfaces, such as OLE DB.

Do some users require the ability to manage their projects in Microsoft Project while utilizing P6 Professional to manage global data?

Your organization might currently use Microsoft Project to manage projects. Use P6 Professional import/export functionality to share projects, resources, and roles data with Microsoft Project. For more information, see the P6 Professional Help.

Do we want to utilize password security features?

When the authentication mode is set to "Native," most of P6 Professional, with the exception of the P6 SDK, offers a strong password policy feature. When enabled, this feature requires that all new and modified passwords be between 8 and 20 characters and contain at least one number and one letter. If using LDAP authentication, the security set on the host authentication server overrides the password security features in P6 Professional.

Client and Server Requirements

After determining your P6 Professional implementation plan, ensure that your hardware and software can support it. The following tables summarize supported configurations for P6 Professional.

For the full list of system requirements, versions, and tested configurations, go to the \Documentation\<language>\Tested_Configurations folder of the P6 Professional physical media or download.

Supported Platforms for P6 Professional

For P6 Professional

- Microsoft Windows XP sp3
- Microsoft Windows Vista sp2
- Microsoft Windows 7
- Citrix Presentation Server 4.5

Citrix XenApp 5.0

Supported Configurations for Client Modules

For database clients running P6 Professional

- Oracle 11.1.0.7.0 Runtime (only required for Oracle databases and only the 32-bit version is supported). Oracle 11G R2 is also supported.
- TCP/IP network protocol

Note: P6 Professional R8.1 is compiled with a /LARGEADDRESSAWARE option (also known as LAA) that can address additional virtual memory above 2GB. Applications like P6 Professional that are compiled with the /LARGEADDRESSAWARE option can take advantage of the 3GB switch in 32-bit Windows and can address up to 4GB of virtual memory in 64-bit Windows. For more information on the 3GB switch for the /LARGEADDRESSAWARE option, please contact Microsoft Support.

Supported Configurations for Servers

For the P6 Professional database server

▶ Oracle 10.2.0.5.0
▶ Oracle 11.2.0.2.0
▶ Microsoft SQL Server 2005 sp3
▶ Microsoft SQL Server 2008 R2

Supported E-Mail Systems and Network Protocols

▶ Internet e-mail (SMTP)
▶ MAPI is supported for P6 Professional
▶ Network protocols depend only on database vendor
▶ Web site requires TCP/IP

Security Guidance

This chapter provides guidelines on creating an overall secure environment for P6 Professional. It summarizes security options to consider for each installation and configuration process and details additional security steps that you can perform before and after P6 Professional implementation.

In This Section

Security Guidance Overview

During the installation and configuration process for P6 Professional, several options are available that impact security. Depending on your organization's needs, you might be required to create a highly secure environment for all P6 Professional applications. Use the following guidelines to plan your security strategy for P6 Professional:

▶ Review all security documentation for applications and hardware components that interact or integrate with P6 Professional. Hardening your environment is recommended. See *Additional Sources for Security Guidance* (on page 26) for links that can help you to get started.

▶ Read through the summary of considerations for P6 Professional included in this document. Areas covered include: safe deployment, authentication options, authorization, confidentiality, sensitive data, reliability, and cookies usage.

▶ Throughout this documentation, the Security Guidance icon helps you to quickly identify security-related content to consider during the installation and configuration process. Once you begin the installation and configuration of your P6 Professional environment, use the Security Guidance icon as a reminder to carefully consider all security options.

Tips

As with any software product, be aware that security changes made for third party applications might affect P6 Professional applications. For example, if you configure WebLogic to use only SSL v3.0, you must disable TLS v1.0 for the client JRE for P6 to launch properly. If using an Internet Explorer browser, you must also disable TLS v1.0 in Internet Options.

Safe Deployment of P6 Professional

To ensure overall safe deployment of P6 Professional, you should carefully plan security for all components, such as database servers, application servers, and client computers, that are required for and interact with P6 Professional. In addition to the documentation included with other applications and hardware components, follow the P6 Professional-specific guidance below.

Administrative Privileges Needed for Installation and Operation

As the P6 Professional Administrator, you should determine the minimum administrative privileges or permissions needed for installation, configuration, and daily operation of P6 Professional. For example, to successfully install the required JRE for P6 Professional Web applications (for example, P6 and P6 Progress Reporter), you must be an administrator on the client machine during this installation or update.

Minimum Client Permissions Needed for P6 Professional

Users do not have to be administrators on their machines to run P6 Professional. Instead, you can grant minimum permissions to create a more secure environment.

The following is a summary of the minimum system requirements needed to access and run components of P6 Professional R8.1:

Files within Window Folders:

▸ *local drive*\Program Files\Oracle\Primavera P6\P6 Professional

dbexpsda40.dll

dbexpsda30.dll

dbexpint.dll

dbexpoda40.dll

dbexpoda30.dll

DbExpPrC.dll (only needed when using Compression Server)

dbexpsda.dll

dbxadapter30.dll (only needed when using Compression Server)

Read&Execute/Read permission to access files needed to run P6 Professional applications and to create and modify database alias connections.

▸ *local drive*\Program Files\Oracle\Primavera P6\P6 Professional\pm.ini

Read&Execute/Read/Write permission to access the ini file, which is required to log into P6 Professional applications.

▸ *local drive*\Program Files\Oracle\Primavera P6\P6 Professional\Java\

dbconfig.cmd

admin.cmd

Read&Execute/Read permissions to run the Database Configuration setup, the P6 Administrator application.

For your reference, the following are the default installation locations for the PrmBootStrap.xml file:

Windows XP:

\%USERPROFILE%\Local Settings\Application Data\Oracle\Primavera P6\P6 Professional

Windows Vista and 7:

\%LOCALAPPDATA%\Oracle\Primavera P6\P6 Professional

During installation, the PrmBootStrap.xml file is also copied to one of the locations below, depending on your operating system. The files will never be modified during use of P6 Professional, so they can be copied to the current user location (USERPROFILE or LOCALAPPDATA) if you need to revert P6 Professional back to its original state (for example, if files become corrupted).

Windows XP:

\%ALLUSERSPROFILE%\Application Data\Oracle\Primavera P6\P6 Professional

Windows Vista and 7:

\%PROGRAMDATA%\Oracle\Primavera P6\P6 Professional

▸ Output directory for File > Export, Log output files

Read&Execute/Read/Write to create and write output files.

Registry Keys:

▸ HKEY_LOCAL_MACHINE\Software\Primavera

READ

> **Note:** For the Update Baseline and Schedule Comparison/Claim Digger tools, the key is opened in Read/Write/Delete mode.

Physical Security Requirements for P6 Professional

All hardware hosting P6 Professional should be physically secured to maintain a safe implementation environment. Consider the following when planning your physical security strategy:

▸ Components of the intended environment should be properly installed, configured, managed, and maintained according to guidance in all applicable Administrator's Guides for P6 Professional.

- Components of P6 Professional should be installed in controlled access facilities to prevent unauthorized physical access. Only authorized administrators for the systems hosting P6 Professional should have physical access to those systems. Such administrators include the Operating System Administrators, Application Server Administrators, and Database Administrators.
- Administrator access to client machines should only be used for installation and configuration of P6 Professional modules.

Files to Protect after Implementation

While P6 Professional requires specific files for installation and configuration, some are not needed for daily operations. Although not intended as a comprehensive list, the following are files that should be protected or moved to a secure location after installation and configuration:

- **DatabaseSetup.log**

   Captures processes performed during P6 Professional database installation.

   Default Location = user home directory (for example, C:\Documents and Settings\Administrator)

- **dbconfigpv.cmd** (or **dbconfig.sh** for Linux)

   Tool used to create the connection between the P6 Professional database and P6.

   Default location = P6 home directory, as specified during installation

- **p6-emplugin.jar**

   A P6 Professional-specific plug-in used to enable the display of P6 metrics in Oracle Enterprise Manager.

   Default location = P6 home directory, as specified during installation

Authentication Options for P6 Professional

Authentication determines the identity of users prior to granting access to P6 Professional modules. P6 Professional offers the following authentication modes:

- **Native** authentication is the default mode for P6 Professional. In this mode, when a user attempts to log into a P6 Professional application, authentication is handled directly through the module with the P6 Professional database acting as the authority.
- **LDAP** (Lightweight Directory Access Protocol) is directory-based authentication and is available for all P6 Professional applications. In this mode, when a user attempts to log into a P6 Professional application, the user's identity is confirmed in an LDAP-compliant directory server database. Additionally, P6 Professional supports the use of LDAP referrals with Oracle Internet Directory and Microsoft Windows Active Directory. Referrals chasing allows authentication to extend to another domain.

   You can also configure multiple LDAP servers to use for authentication. This allows failover support and enables you to search for users in multiple LDAP stores.

The use of LDAP will help you to create the most secure authentication environment available in P6 Professional.

Authorization for P6 Professional

Appropriate authorization should be granted carefully to all users of P6 Professional. The most secure application security options are detailed in the *P6 Professional Administrator's Guide*.

To help you with security planning, the following are authorization-related options to consider:

▸ Use Module Access rights to limit access to P6 Professional modules.
▸ Use Global profiles to limit privileges to global data. Assign the Admin Superuser account sparingly.
▸ Use Project profiles to limit privileges to project data. Assign the Project Superuser account sparingly.
▸ Assign OBS elements to EPS and WBS nodes to limit access to projects.
▸ Assign resource access limitations to each user.

Confidentiality for P6 Professional

▸ Confidentiality ensures that stored and transmitted information is disclosed only to authorized users. In addition to the documentation included with other applications and hardware components, follow the P6 Professional-specific guidance below.
▸ For data in transit, use SSL/TLS to protect network connections among modules. If LDAP authentication mode is used, ensure that LDAPS is used for the connection to the directory server.
▸ For data at rest, refer to the documentation included with the database server for instructions on securing the database.

Sensitive Data for P6 Professional

▸ Measures should be taken to protect sensitive data in P6 Professional, such as user names, passwords, and e-mail addresses. Use the process below as an aid during your security planning:
▸ Implement security measures in P6 Professional to carefully grant users access to sensitive data. For example, use a combination of Global Profiles, Project Profiles, and OBS access to limit access to data.
▸ Implement security measures for applications that interact with P6 Professional, as detailed in the documentation included with those applications.

Reliability for P6 Professional

The following measures can be taken to protect against attacks that could cause a denial of service:

‣ Ensure that the latest security patches are installed.
‣ Replace the default Admin Superuser (admin) immediately after a manual database installation or an upgrade from P6 version 7.0 and earlier.
‣ Ensure that log settings meet the operational needs of the server environment. Refrain from using "Debug" log level in production environments.
‣ Document the configuration settings used for servers and create a process for changing them.
‣ Protect access to configuration files with physical and file system security.

Additional Sources for Security Guidance

The databases, platforms, and servers that you use for your P6 Professional implementation should be properly secured. Although not intended as a comprehensive list, you might find the links below helpful when planning your security strategy.

> **Note:** Due to the dynamic nature of the Web, the URLs below might have changed since publication of this guide.

Oracle Database

http://download.oracle.com/docs/cd/B19306_01/network.102/b14266/toc.htm

Microsoft SQL Server 2005 Database

http://www.microsoft.com/sqlserver/2005/en/us/security.aspx

Microsoft SQL Server 2008 Database

http://www.microsoft.com/sqlserver/2008/en/us/Security.aspx

Microsoft Windows 2008 Server

http://technet.microsoft.com/en-us/library/dd548350(WS.10).aspx

Microsoft Windows 2003 Server

http://www.microsoft.com/downloads/details.aspx?familyid=8A2643C1-0685-4D89-B655 -521EA6C7B4DB&displaylang=en

Automatic Database Installation

Follow the steps in this chapter to set up and load the P6 Professional databases on a server using the automatic install process.

In This Section

Automatic Database Installation Overview

One database is used to run P6 Professional. It stores data used by all P6 Professional applications.

If you need detailed steps on installing Oracle Database or Microsoft SQL Server, refer to the database documentation included with those products.

P6 Professional supports Oracle and Microsoft SQL Server databases. See **Client and Server Requirements** (on page 18) for details on which versions are supported. The Oracle or Microsoft SQL Server software must be installed on the database servers before you can create the database.

You can run the database wizard to automatically create a database structure and load application data into it; or, you can manually configure the database structures and then run a batch file to load application data. This chapter walks you through the automatic method. See **Manual Database Configuration** (on page 35) for the manual instructions.

> **Note:** See **Automatic Database Upgrade** (on page 47) for details if you have previously installed and configured P6 Professional databases and want to upgrade to the current version.

See **Database Administration** (on page 55) for additional tips and considerations related to database performance along with additional settings.

Microsoft SQL Server considerations

Before installing the P6 Professional database, consider the following:

‣ If you intend to run P6 Professional on a Microsoft SQL Server database server, the required Microsoft SQL Server client files are automatically installed when you install P6 Professional on a client machine.

▸ If you wish to prevent the appearance of duplicate values in P6 Professional modules due to leading or trailing spaces, ensure that the ANSI_PADDING setting in Microsoft SQL Server is set to OFF. For example, if one user enters "Equipment" and another user enters " Equipment" (with a leading space) for resource codes, the database will store both of these as valid values if ANSI_PADDING is set to ON. If ANSI_PADDING is set to OFF, the database will remove the leading space in the second entry and warn the user that a unique ID must be entered. See the documentation included with Microsoft SQL Server for more information.

▸ See *P6 Professional Database Connections Using a Non-Default Microsoft SQL Server Port* (on page 74) if you will be using a non-default port for Microsoft SQL Server for additional configuration instructions after installation.

> **Note:** P6 Professional does not support passwords with multi-byte characters.

To configure the SQL database server for SSL:

Please see instructions for configuring SQL Database Server SSL in the Microsoft Documentation.   Questions and Support for Installation / Configurations should be directed to the database vendor, Microsoft.

About the Database Wizard

The Database wizard guides you through the steps for creating a new database structure and loading the application data into it. You do not need to be an experienced DBA to perform these steps; however, Oracle or Microsoft SQL Server must already be installed on the database server.

You can run the Database wizard to create a new database from a client computer or from the server itself. The Database wizard creates any necessary file structures and database users for you.

For information on how to run the Database wizard from a command line, refer to My Oracle Support's Knowledge Articles.

Automatically Installing a Microsoft SQL Server Database and Loading Application Data

Complete the following steps to automatically create a Microsoft SQL Server database and load application data.

Related Topics

Creating a Microsoft SQL Server Database

To create a Microsoft SQL Server database:

1) Set the JAVA_HOME location:

   In your Windows system environment.

   a. Right-click on **My Computer** and select **Properties**.

   b. In the **System Properties** dialog box, on the **Advanced** tab, click **Environment Variables**.

   c. In the **Environment Variables** dialog box, under **System variables**, click **New**.

   d. In the **New System Variable** dialog box:

      1. In the **Variable name:** field, enter **JAVA_HOME**.

      2. In the **Variable value:** field, enter the location where Java is located (for example, C:\Program Files\Java\jre6).

   e. Click **OK** to exit out of the open dialog boxes.

   For Linux, add the JAVA_HOME Environment variable to the dbsetup.sh (in the Database folder of the P6 Professional physical media or download) file before running it. For example: `export JAVA_HOME=/usr/java/jre1.6.0_24/`

2) Run **dbsetup.bat** (dbsetup.sh for Linux) from the Database folder of the P6 Professional physical media or download.

   > **Note:** Click Next on each wizard dialog box to advance to the next step.

3) On the **Primavera P6** dialog box:

   a. Choose **Install a new database**.

   b. Choose **Microsoft SQL Server** as the server type.

4) On the **Connection Information** dialog box:

   a. In the **DBA user name** field, type the Microsoft SQL Server system administrator name to register to the server.

   b. In the **DBA password** field, type the password for this system administrator.

   c. In the **Database host address** field, enter the server machine name or IP address where Microsoft SQL Server is installed.

   d. In the **Database host port** field, enter the port number that Microsoft SQL Server is using. The default is 1433.

5) On the **Configure Microsoft SQL Server** dialog box, click **Next** to accept the default values, or change them as appropriate for your installation.

   If you change the name of the database, duplicate database names are not permitted—you will be prompted to enter a unique name if a database with the specified name already exists.

   > **Note:** Do not use special characters in the database name, privileged user, or public user name, for example: { } [ ] : ; < > , . ? ! @ # $ % ^ & * ( ) - _ | / \ ~ `

The data file contains the database tables and procedures. The log file contains a record of changes. By default, the Database wizard stores these files in the folder on your server where Microsoft SQL Server is installed. The database name that you specify is used to name the files. If you change the location, the destination folder must exist on the server.

The database code page will default to what is already selected for Microsoft SQL Server. Select a different code page, if necessary.

6) On the **Create SQL Server Users** dialog box, specify the SQL database privileged, and public user names and passwords. If you already have a privileged or public user you want to use, you can select the **Use existing** option.

> **Note:**
>
> - Oracle recommends using strong passwords. Strong passwords in P6 Professional are defined as passwords containing between 8 and 20 characters and at least one numeric and one alpha character. To further strengthen the password, use a mixture of upper and lower case letters.
>
> - Do not use special characters in the database name, privileged user, or public user name, for example: { } [ ] : ; < > , . ? ! @ # $ % ^ & * ( ) - _ | / \ ~ `

7) Click **Next**.

Clicking **Next** will begin the initial creation of the P6 Professional database, so you will no longer be able to click Previous to change your prior selections. However, in *Loading Application Data for SQL* (on page 30), you will have the option to either click Install or Cancel.

Loading Application Data for SQL

To continue installing the SQL database and load application data:

1) On the **Configuration Options** dialog box:

   a. In the **Application User** section, enter the application administrative user name and password. By default, the application administrative user will be granted Admin Superuser access rights.

   > **Notes:**
   >
   > - P6 Professional does not support passwords with multi-byte characters.
   >
   > - Oracle recommends using strong passwords. Strong passwords in P6 Professional are defined as passwords containing between 8 and 20 characters and at least one numeric and one alpha character. To further strengthen the password, use a mixture of upper and lower case letters.

   b. Select the **Load sample data** option if you want to include sample project data in a non-production database. If you do not select the Load sample data option, empty data is loaded in a secure state and includes only the most basic information needed to run the P6 Professional database.

> **Caution:** You must choose the base currency in the following step if you do not want the database to use US dollars ($) as the base currency. It is not possible to change the base currency once projects are in progress. See *The Base Currency* (on page 41) for more information on the base currency.

   c. If you want to use a currency other than US Dollars as the base currency for the database, select a different base currency in the **Currency** field.

   d. Click **Install** to start the process of loading the database tables with application data.

2) On the **Primavera Database Setup Wizard** dialog box, click **Next** after the processes have completed.

> **Note:** If the database creation fails, see PrimaveraDatabaseSetup.log located in the user home directory (for example, C:\Documents and Settings\Administrator). Contact Oracle Global Customer Support if you need further assistance.

3) Click **Finish** to exit the wizard.

> **Note:** When the installation successfully completes, delete the installation log.

Once the application data is installed you can begin to install and configure the client module.

See *Database Administration* (on page 55) for information on configuring database settings to optimize performance.

The Base Currency for Microsoft SQL Server

The base currency is the monetary unit used to store cost data for all projects in the database and is controlled by a global administrative setting in P6. The default base currency for P6 Professional is US dollars ($). The view currency is the monetary unit used to display cost data in P6 Professional and is controlled by a user preference.

The exchange rate for the base currency is always 1.0. When a user selects a different currency than the base currency to view cost data, the base currency value is multiplied times the current exchange rate for the view currency to calculate the values displayed in cost and price fields.

For example, if the base currency is U.S. Dollars, the view currency is Euros, and the exchange rate for Euros is .75, a value of $10 stored in the database is displayed as 7.5 Euros in cost and price fields. Similarly, if you enter 7.5 Euros in a cost or price field, it is stored in the database as $10.

When data is displayed in a view currency that is different than the base currency, some cost and price values can vary slightly (e.g., due to rounding). As long as the correct base currency is selected during database installation, a user can view completely accurate cost and price data by changing the view currency to match the base currency.

See Adding a Currency for information on adding view currencies.

Private Database Logins for P6 Professional

Private database logins are used primarily by administrators to gain direct access to a database. For example, the privileged user login that you use to access the P6 Professional database is a private database login. You can add, modify, or delete existing logins using the Database Logins tool. This can also be accomplished using the Administration Configuration tool.

P6 Professional R8.1 includes an encryption algorithm that provides enhanced security for private database logins; however, the encryption algorithm is not automatically enforced when you manually configure or upgrade your database. If you manually configure or upgrade your database, 🛡 Oracle recommends that you use this encryption algorithm. To do so, you must reset the private database login. See *Resetting Private Database Passwords to Use the New Encryption Algorithm* (on page 43) for instructions. If automatically installing or upgrading your database, no configuration is needed after the upgrade to use the encryption algorithm. User logins and passwords are not affected.

Related Topics

Adding Private Database Logins for P6 Professional

To add private database logins for P6 Professional:

1) Run **databaselogins.bat** (databaselogins.sh for Linux) from the Database folder of the P6 Professional physical media or download.

2) On the **Database Connection** dialog box:

   a. Select the database, Microsoft SQL Server.

   b. Type the user name and password of a privileged database user (for example, privuser). This login should have administrative rights on the database.

   c. Enter the host address, host port, and database name specific to your Microsoft SQL Server installation. The Port field displays the default port for the database type you selected.

   d. Click **Next**.

3) On the **Private Database Logins** dialog box:

   a. Click **Add**.

   b. Enter a user name.

   c. Enter a password.

   d. To reverse a change, click **Undo**. Undo will reverse any changes made during the current session.

   e. Click **Save**.

   f. Click **OK** to exit.

Modifying Private Database Logins for P6 Professional

To modify private database logins:

1) Run **databaselogins.bat** (databaselogins.sh for Linux) from the Database folder of the P6 Professional physical media or download.

2) On the **Database Connection** dialog box:

   a. Select the database, Microsoft SQL Server.

   b. Type the user name and password of a privileged database user (for example, privuser). This login should have administrative rights on the database.

   c. Enter the host address, host port, and database name specific to your Microsoft SQL Server installation. The Port field displays the default port for the database type you selected.

   d. Click **Next**.

3) On the **Private Database Logins** dialog box:

   a. Select the private database user name that you wish to modify.

   b. Enter a new user name.

   c. Highlight the password, and change it.

   d. Click the **Update Password** button.

   e. To reverse a change, click **Undo**. Undo will reverse any changes made during the current session.

   f. Click **Save**.

   g. Click **OK** to exit the Database Logins tool.

Deleting Private Database Logins for P6 Professional

To delete private database logins for P6 Professional:

1) Run **databaselogins.bat** (databaselogins.sh for Linux) from the Database folder of the P6 Professional physical media or download.

2) On the **Database Connection** dialog box:

   a. Select the database, Microsoft SQL Server.

   b. Type the user name and password of a privileged database user (for example, privuser). This login should have administrative rights on the database.

   c. Enter the host address, host port, and database name specific to your Microsoft SQL Server installation. The Port field displays the default port for the database type you selected.

   d. Click **Next**.

3) On the **Private Database Logins** dialog box:

   a. Select the private database user name that you wish to remove.

   > **Note:** You must have at least one private user name for the P6 Professional database at all times.

   b. Click **Delete**.

   c. To reverse a change, click **Undo**. Undo will reverse any changes made during the current session.

   d. Click **Save**.

   e. Click **OK** to exit the Database Logins tool.

Manual Database Configuration

Read this chapter to manually set up the central P6 Professional database on a server running Oracle or Microsoft SQL Server. The steps in this chapter should be performed by your database administrator (DBA).

See *Automatic Database Installation* (on page 27) to use a wizard that automatically creates the database structures and loads the data.

In This Section

Manual Database Configuration Overview

The P6 Professional database stores all P6 Professional data used by all P6 Professional applications.

P6 Professional supports Oracle and Microsoft SQL Server databases. See *Client and Server Requirements* (on page 18) for details on which versions are supported. The Microsoft SQL Server or Oracle server software must be installed on the database servers before you can create the database.

> **Notes:**
>
> See P6 Professional Database Connections Using a Non-Default Microsoft SQL Server Port if you will be using a non-default port for Microsoft SQL Server for additional configuration instructions after database configuration.

P6 Professional R8.1 includes an encryption algorithm that provides enhanced security for private database logins; however, the encryption algorithm is not automatically enforced when you manually configure or upgrade your database. If you manually configure or upgrade your database, Oracle recommends that you use this encryption algorithm. To do so, you must reset the private database login. See Resetting Private Database Passwords to Use the New Encryption Algorithm for instructions. If automatically installing or upgrading your database, no configuration is needed after the upgrade to use the encryption algorithm. User logins and passwords are not affected.

Tips

▶ P6 Professional does not support passwords with multi-byte characters.

▶ When you install the Oracle client, the TNSPING.EXE utility is automatically installed in the \oracle\ora_home\bin folder. This utility must be present for P6 Professional applications. Do not delete it.

▶ See **Automatic Database Upgrade** (on page 47) for instructions on automatically upgrading your databases to the current version if you have manually configured P6 Professional databases for an earlier version. If you want to manually upgrade your databases, refer to the manual database upgrade documents available from the P6 Professional Documentation Center, which you can access from the \Documentation\<language> folder of the P6 Professional physical media or download.

▶ _ For security reasons, Oracle strongly recommends that you replace the default database users' (privuser and pubuser) passwords immediately after a manual database installation or an upgrade from P6 version 7.0 and earlier. Do not use special characters in the database name, privileged user, or public user name for example: { } [ ] : ; < > , . ? ! @ # $ % ^ & * ( ) - _ | / \ ~ ` _

▶ Oracle recommends using strong passwords. Strong passwords in P6 Professional are defined as passwords containing between 8 and 20 characters and at least one numeric and one alpha character. To further strengthen the password, use a mixture of upper and lower case letters.

▶ See **Modifying Private Database Logins for P6 Professional** (on page 33) for instructions on how to replace the private database login. For all other database user names and passwords, use the tools included with Microsoft SQL Server.

▶ For security reasons, Oracle strongly recommends that you replace the default Admin Superuser (admin) immediately after a manual database installation or an upgrade from P6 version 7.0 and earlier.

▶ If you wish to prevent the appearance of duplicate values in P6 Professional modules due to leading or trailing spaces, ensure that the ANSI_PADDING setting in Microsoft SQL Server is set to OFF. For example, if one user enters "Equipment" and another user enters " Equipment" (with a leading space) for resource codes, the database will store both of these as valid values if ANSI_PADDING is set to ON. If ANSI_PADDING is set to OFF, the database will remove the leading space in the second entry and warn the user that a unique ID must be entered. See the documentation included with Microsoft SQL Server for more information.

▶ To configure the SQL database server for SSL, instructions for configuring SQL Database Server SSL can be found within Microsoft Documentation. Questions and Support for Installation / Configurations should be directed to the database vendor, Microsoft.

Creating the Database Structure for Microsoft SQL Server and Loading Application Data

The Microsoft SQL Server DBA creates the P6 Professional database, then runs P6 Professional SQL scripts that create each database's structure (tables, indexes, relationships, and so on).

These instructions assume you are a DBA or are familiar with how to administer Microsoft SQL Server databases. All steps need to be completed in the order specified. If you have any questions about the manual setup process, please contact Oracle Global Customer Support before proceeding.

Before you create the Microsoft SQL Server database structure, you should first register to the server as a system administrator (SA) and review the following server-level configuration changes in the Microsoft SQL Server Management Studio:

▶ **Max Worker Threads** Specify the number of threads used to support the users connected to the server. The default setting (255) might be too high for some configurations, depending on the number of simultaneous users. Each worker thread is allocated, even if it is not in use, which means that if there are fewer simultaneous connections than allocated worker threads, you could be wasting memory resources.

▶ **Memory** Keep the setting as Dynamic. Microsoft SQL Server dynamically acquires and frees memory as needed, up to the maximum available memory on your server.

▶ **Open Objects** Keep the setting as Dynamic. This setting determines the maximum number of objects that can be opened simultaneously on Microsoft SQL Server. The value is set automatically depending on current system needs. You should not need to change this value.

▶ **User Connections** Keep the setting as 0, which designates Microsoft SQL Server to adjust the number of simultaneous user connections allowed based on how many are needed, up to the maximum value.

▶ **Network Packet Size** Set to 16384.

After configuring the server, stop and start Microsoft SQL Server to ensure that the changes take effect.

Related Topics

Creating the P6 Professional Database Structure for Microsoft SQL Server

Complete the following steps to create the P6 Professional database Microsoft SQL Server database structure.

Related Topics

Copying the Script Files to a Local Drive for Microsoft SQL Server

To copy the script files:

1) Copy the Database folder of the P6 Professional physical media or download to a local drive.

2) Use the copy on the local drive for all instructions in this section.

Creating the Database for Microsoft SQL Server

To create the database:

1) Register to the server as SA user.

2) Open Microsoft SQL Server Management Studio. Go to \database\scripts\install\PPM_08_00_00 and execute the **ssppm_init_db.sql** script. This script creates a database called PMDB. If you want to change it, you must modify the **ssppm_init_db.sql** script.

> **Notes:**
>
> - Instead of running the ssppm_init_db.sql script, you can manually create a database named PMDB with a data file of 500 MB or more and a log file of 200 MB or more.

- Do not use special characters in the database name, privileged user, or public user name, for example: { } [ ] : ; < > , . ? ! @ # $ % ^ & * ( ) - _ | / \ ~ `

You can change the initial data file and log file sizes and increase or decrease these amounts depending on how much data you plan to store in the database. You can also select the Automatically Grow File option to specify that these values automatically increase based on need.

> **Note:** Oracle recommends that you use Microsoft SQL Server Management Studio to perform the following steps.

Creating Users and Tables for Microsoft SQL Server

The scripts in this task are located in:

Install scripts: \database\scripts\install\PPM_08_00_00

To create users and tables:

1) Log into the P6 Professional database as SA user.

2) Execute the **ssppm_create_users.sql** script.

> **Notes:**
>
> - Running the ssppm_create_users.sql script creates the following user names: privuser and pubuser. If you have created other user names and wish to use those when running P6 Professional database scripts, make sure to replace the private and public user names with your custom user names in all applicable scripts before running them.
>
> - Do not use special characters in the database name, privileged user, or public user name, for example: { } [ ] : ; < > , . ? ! @ # $ % ^ & * ( ) - _ | / \ ~ `

3) Execute the **ssppm_tables.sql** script in the database you created when you ran the ssppm_init_db.sql

> - **Notes:**
> - If you changed database or user names, you will need to update the **ssppm_tables.sql** script. You will need to update the PMDB name and the privuser and pubuser names.

Installing Sample Data for Microsoft SQL Server

To install sample data:

1) Open a command prompt and change your directory to the location of the rundataloader.bat file, which is on the root of the database folder by default.

2) Execute a statement similar to one of the following:

▸ Use this command if you want to load sample data into a non-production environment.

```
rundataloader.bat sample:ppmdb_mk.zip
sa/password@sqlserver:host:port:instance
```

where *password* is the sa user password, *host* is the server machine name or IP address where Microsoft SQL Server is installed, *port* is the port number that Microsoft SQL Server is using (the default is 1433), and *instance* is the database name (for example, PMDB).

▸ 🛡 Use this command if you do not want to load sample data. Empty data is loaded in a secure state and includes only the most basic information needed to run the P6 Professional database.

```
rundataloader.bat sample:ppmdb_mk_empty.zip
sa/password@sqlserver:host:port:instance
```

where *password* is the sa user password, *host* is the server machine name or IP address where Microsoft SQL Server is installed, *port* is the port number that Microsoft SQL Server is using (the default is 1433), and *instance* is the database name (for example, PMDB).

Creating Remaining Database Objects for Microsoft SQL Server

The scripts in this task are located in:

Install scripts: \database\scripts\install\PPM_08_00_00

Source scripts: \database\scripts\source\PPM_08_00_00

To create remaining database objects:

1) Log on to the P6 Professional database as SA user.
2) Execute the **sspm_querylib.sql** install script.
3) Execute the **sspm_ins_aux.sql** install script.

> **Notes:**
>
> - The sspm_ins_aux.sql script has a grant that reads: GRANT SELECT ON PUBUSER TO PUBUSER. If you changed the default pubuser name, do not change the name of the PUBUSER table, only change the user name. For example: GRANT SELECT ON PUBUSER TO NEW_PUBUSER_USERNAME
> - If you changed the default privuser and pubuser names, you must update the **sspm_ins_aux.sql** script with your custom privuser and pubuser names.
> - Do not use special characters in the database name, privileged user, or public user name, for example: { } [ ] : ; < > , . ? ! @ # $ % ^ & * ( ) - _ | / \ ~ `

4) Execute the **sspm_src.plb** source script.

Notes:

- If you changed the default privuser name, you must update the **sspm_src.plb** script with your custom privuser name.
- Do not use special characters in the database name, privileged user, or public user name, for example: { } [ ] : ; < > , . ? ! @ # $ % ^ & * ( ) - _ | / \ ~ `
- Execute the **sspm_database_version.sql** install script.

5) If you used a non-default privuser name, you must do the following:

   a. Log into the **databaselogins.bat** (on Windows) or **databaselogins.sh** (on Unix) database as privuser (use your custom privuser name if you created a custom user name and password).

   b. Update the privuser name and password to match what you used when you created users in *Creating Users and Tables for Microsoft SQL Server* (on page 39).

Dropping P6 Professional Database Objects for Microsoft SQL Server

If you make a mistake or want to recreate the database objects for the P6 Professional database:

1) Delete the PMDB.
2) Start over at *Creating the Database for Microsoft SQL Server* (on page 38).

Changing the Database Base Currency

Caution: It is not possible to change the base currency once projects are in progress.

After manually creating and configuring the P6 Professional database, you must change the base currency if you do not want the databases to use US dollars ($) as the base currency.

Related Topics

The Base Currency

The base currency is the monetary unit used to store cost data for all projects in the database and is controlled by a global administrative setting in P6. The default base currency for P6 Professional is US dollars ($). The view currency is the monetary unit used to display cost data in P6 Professional and is controlled by a user preference.

The exchange rate for the base currency is always 1.0. When a user selects a different currency than the base currency to view cost data, the base currency value is multiplied times the current exchange rate for the view currency to calculate the values displayed in cost and price fields.

For example, if the base currency is U.S. Dollars, the view currency is Euros, and the exchange rate for Euros is .75, a value of $10 stored in the database is displayed as 7.5 Euros in cost and price fields. Similarly, if you enter 7.5 Euros in a cost or price field, it is stored in the database as $10.

When data is displayed in a view currency that is different than the base currency, some cost and price values can vary slightly (e.g., due to rounding). As long as the correct base currency is selected during database installation, a user can view completely accurate cost and price data by changing the view currency to match the base currency.

See Adding a Currency for information on adding view currencies.

Reviewing Currency Choices

The process to change the base currency involves editing and running a P6 Professional script provided. By default, US dollars is the base currency, and USD is the short name used in the script. To know which short name to use in the script for the currency that you require, review the list of available short names for P6 Professional. To do so, run the following query on the P6 Professional database:

select curr_type, curr_short_name from currtype;

Changing the Base Currency

To change the base currency:

1) On the P6 Professional physical media or download:
   a. Browse to \Database\scripts\common.
   b. Copy one of the following scripts to a local drive:

      For Oracle: **or_set_currency.sql**

2) If the script was copied from physical media, turn off the script file's read-only attribute.

   Since files on physical media are read-only, this attribute is turned on when a file is copied from a CD or DVD.

   a. In Windows Explorer, right-click the file.
   b. Choose Properties.
   c. Clear the Read-Only option.

3) Open the script for editing and locate the line containing **v_new_base_currency: = 'USD'**

4) Replace USD with the currency short name of your choice.

5) Save your changes and run the modified script.

Private Database Logins for P6 Professional

Private database logins are used primarily by administrators to gain direct access to a database. For example, the privileged user login that you use to access the P6 Professional database is a private database login. You can add, modify, or delete existing logins using the Database Logins tool. This can also be accomplished using the Administration Configuration tool.

P6 Professional R8.1 includes an encryption algorithm that provides enhanced security for private database logins; however, the encryption algorithm is not automatically enforced when you manually configure or upgrade your database. If you manually configure or upgrade your database, 🛡 Oracle recommends that you use this encryption algorithm. To do so, you must reset the private database login. See ***Resetting Private Database Passwords to Use the New Encryption Algorithm*** (on page 43) for instructions. If automatically installing or upgrading your database, no configuration is needed after the upgrade to use the encryption algorithm. User logins and passwords are not affected.

Related Topics

Resetting Private Database Passwords to Use the New Encryption Algorithm

To reset private database passwords to use the new encryption algorithm:

1) Run **databaselogins.bat** (databaselogins.sh for Linux) from the Database folder of the P6 Professional physical media or download.

2) On the **Database Connection** dialog box:

   a. Select the database, Microsoft SQL Server.

   b. Type the user name and password of a privileged database user (for example, privuser). This login should have administrative rights on the database.

   c. Enter the host address, host port, and database name specific to your Microsoft SQL Server installation. The Port field displays the default port for the database type you selected.

   d. Click **Next**.

3) On the **Private Database Logins** dialog box:

   a. Select the private database user name that you wish to reset.

   b. Highlight the password, and change it (or simply re-enter the existing password).

   c. Click the **Update Password** button.

   d. To reverse a change, click **Undo**. Undo will reverse any changes made during the current session.

   e. Click **Save**.

   f. Click **OK** to exit the Database Logins tool.

Adding Private Database Logins for P6 Professional

To add private database logins for P6 Professional:

1) Run **databaselogins.bat** (databaselogins.sh for Linux) from the Database folder of the P6 Professional physical media or download.

2) On the **Database Connection** dialog box:

   a. Select the database, Microsoft SQL Server.

   b. Type the user name and password of a privileged database user (for example, privuser). This login should have administrative rights on the database.

   c. Enter the host address, host port, and database name specific to your Microsoft SQL Server installation. The Port field displays the default port for the database type you selected.

   d. Click **Next**.

3) On the **Private Database Logins** dialog box:

   a. Click **Add**.

   b. Enter a user name.

   c. Enter a password.

   d. To reverse a change, click **Undo**. Undo will reverse any changes made during the current session.

   e. Click **Save**.

   f. Click **OK** to exit.

Modifying Private Database Logins for P6 Professional

To modify private database logins:

1) Run **databaselogins.bat** (databaselogins.sh for Linux) from the Database folder of the P6 Professional physical media or download.

2) On the **Database Connection** dialog box:

   a. Select the database, Microsoft SQL Server.

b. Type the user name and password of a privileged database user (for example, privuser). This login should have administrative rights on the database.

c. Enter the host address, host port, and database name specific to your Microsoft SQL Server installation. The Port field displays the default port for the database type you selected.

d. Click **Next**.

3) On the **Private Database Logins** dialog box:

a. Select the private database user name that you wish to modify.

b. Enter a new user name.

c. Highlight the password, and change it.

d. Click the **Update Password** button.

e. To reverse a change, click **Undo**. Undo will reverse any changes made during the current session.

f. Click **Save**.

g. Click **OK** to exit the Database Logins tool.

Deleting Private Database Logins for P6 Professional

To delete private database logins for P6 Professional:

1) Run **databaselogins.bat** (databaselogins.sh for Linux) from the Database folder of the P6 Professional physical media or download.

2) On the **Database Connection** dialog box:

a. Select the database, Microsoft SQL Server.

b. Type the user name and password of a privileged database user (for example, privuser). This login should have administrative rights on the database.

c. Enter the host address, host port, and database name specific to your Microsoft SQL Server installation. The Port field displays the default port for the database type you selected.

d. Click **Next**.

3) On the **Private Database Logins** dialog box:

a. Select the private database user name that you wish to remove.

> **Note:** You must have at least one private user name for the P6 Professional database at all times.

b. Click **Delete**.

c. To reverse a change, click **Undo**. Undo will reverse any changes made during the current session.

d. Click **Save**.

e. Click **OK** to exit the Database Logins tool.

Automatic Database Upgrade

Read this chapter to upgrade your P6 Professional database to R8.1 when version 6.0 or later is already installed. You need to upgrade your database if you want to preserve your project data for use with the new version of P6 Professional. A wizard automatically upgrades your database for you.

Oracle recommends that you upgrade your database automatically as described in this chapter; however, if you want to manually upgrade your database, instructions are included in the \Documentation\<language>\Technical_Documentation\Manual_Upgrades folder of the P6 Professional physical media or download.

In This Section

Database Upgrade Process

You can upgrade your existing P6 Professional database (version v6.2, v6.2.1, or v7) to P6 Professional R8.1. You must upgrade your P6 Professional database so it will work with the new version. Use the Database wizard to upgrade your database automatically. The wizard runs the necessary scripts to upgrade the database structure and an upgrade program to add data required by the new version.

All risk data fields are migrated when upgrading; existing fields are mapped to new fields. See Risks Migration for more information.

Convert Methodologies to Projects

To migrate Methodology Management version 7.0 or earlier data to P6 Professional R8.1 projects, use Project Architect in the Project Management module (version 7.0 or earlier) to convert the data from a methodology to a project.

To convert Methodology Management data to a project:

1) Create a new EPS node in P6 Professional version 7.0 where you can store all your Methodology Management projects.

2) Use Project Architect in P6 Professional version 7.0 to create projects from Methodology Management data. For more information on using Project Architect, see version 7.0 of the *Oracle Primavera P6 Project Management Reference Manual*.

Note: You can create only one project at a time. If you want all of your Methodology Management data moved to projects, contact Oracle Consulting to automate the process.

3) After you have converted all your Methodology Management data to projects, upgrade P6 Professional.

Risks Migration

The following table illustrates the risks data field mapping when upgrading from P6 Professional database (version 6.0 through 7.0 SP3) to P6 Professional R8.1.

Risks Fields Migration Table

Name	P6 Professional database (version 6.0 through 7.0 SP3) Risks Fields	P6 Professional R8.1 Risks Field
Risk ID	risk_id	risk_id
	risk_id	risk_code (PROJRISK appended with risk_id)
Risk Name	risk_name	risk_name
Risk Description	risk_descr	risk_desc
Risk Status	status_code	status_code Open= Open; Closed=Managed (closed)
Risk Category ID	risk_type_id	risk_type_id
Risk Control	risk_control	Appended with 'Risk Control'
Risk UDFs	table_name	table_name
Applies to WBS	wbs_id	Appended with 'Applies to WBS' <WBS name>
Applies to Resource	rsrc_id	rsrc_id
Responsible Manager	obs_id	Appended with 'Responsible Manager' <OBS name>
Priority	priority_type	Appended with 'Priority' <priority_type>
Project ID	proj_id	proj_id

Name	P6 Professional database (version 6.0 through 7.0 SP3) Risks Fields	P6 Professional R8.1 Risks Field
Date Identified	add_date	add_date
Impact Date	impact_date	Appended with 'Impact Date' <add_date in mmm-dd-yyyy format >
Probability	prbly_pct	Appended with 'Probability' <prbly_pct>
Impact - Labor Units	impact_work_qty	Appended with 'Impact - Labor Units' <impact_work_qty> - 2 decimals
Impact - Nonlabor Units	impact_equip_qty	Appended with 'Impact - Nonlabor Units' <impact_equip_qty> - 2 decimals
Impact - Material Units	impact_mat_qty	Appended with 'Impact - Material Units' <impact_mat_qty> - 2 decimals
Impact - Expenses	Impact_expense_cost	Appended with 'Impact - Expenses' <impact_expense_cost> - 2 decimals
Risk Control	risk_control	Appended with 'Risk Control'<risk_control>
Risk Category	risk_type	risk_type
Risk Category Sequence ID	seq_num	seq_num

Upgrading a Microsoft SQL Server Database to P6 Professional

If you want to use the database from Primavera 6.0 and later with P6 Professional R8, you need to upgrade the database by performing the following sets of steps. Although recommended, it is not required that these steps be performed by an experienced database administrator.

The wizard runs the necessary scripts to upgrade the database structure and an upgrade program to add data required by the new version. You must upgrade the P6 Professional database.

Related Topics

Upgrading a Microsoft SQL Server Database

To upgrade a Microsoft SQL Server database:

1) Perform a full backup of the current databases.

   If you are unsure how to back up your Microsoft SQL Server database, do not proceed with the upgrade. Contact your database administrator, your database vendor, or Oracle Global Customer Support for assistance in backing up your database before performing the database upgrade. Also, ensure that you are familiar with the process of restoring the backup copy of the database in case you need to do so.

2) Double-click **dbsetup.bat** in the Database folder of the P6 Professional physical media or download to start the Database wizard.

   > **Note:** Click Next on each wizard dialog box to advance to the next step.

3) On the **Primavera P6** dialog box:
   a. Choose **Upgrade an existing database**.
   b. Choose **Microsoft SQL Server** as the server type.

4) On the **Connection Information** dialog box:
   a. In the **Administrative User Name** field, type the Microsoft SQL Server system administrator name to register to the server. If you chose the defaults during the Microsoft SQL Server installation, leave SA as the system administrator name.
   b. In the **Administrative Password** field, type the password for this system administrator. If you chose the defaults during the Microsoft SQL Server installation, leave the password field blank.
   c. In the **Database host address** field, enter the server machine name or IP address where Microsoft SQL Server is installed.
   d. In the **Database host port** field, enter the port number that Microsoft SQL Server is using. The default is 1433.
   e. In the **Database name** field, enter the name of the existing database that you want to upgrade.

5) On the **Ready to Begin Upgrading Data** dialog box:
   a. Verify that the current version of your existing database is listed correctly.
   b. Choose **Yes, upgrade my database**.
   c. Click **Upgrade**.

   The upgrade process could take several minutes, depending on its size.

6) On the **Primavera Database Setup Wizard** dialog box, click **Next** after the process has completed.

> **Notes:** If the database upgrade fails, see PrimaveraDatabaseSetup.log located in the user home directory (for example, C:\Documents and Settings\Administrator). Contact Oracle Global Customer Support if you need further assistance.

7) On the **Finish** dialog box, click **Finish** to exit the wizard.

Configuring the Microsoft SQL Server Database

To verify that the isolation level setting on the upgraded database has been set to "read committed snapshot":

1) Open Microsoft SQL Server Management Studio.

2) Open a new query window for the updated database and execute the following command:

```
dbcc useroptions
```

3) Look for **isolation level** in the Set Option column and verify that the value is set to **read committed snapshot**.

4) If the value is set to **read committed snapshot**, no further action is needed. If the value is set to **read committed**, proceed to step 5.

> **Caution:** Only the connection executing the alter database command is allowed in the database. There must be no other open connection in the database until the execution of the command is complete.

5) Execute the following command to fix the isolation level setting:

```
alter database database name set read_committed_snapshot on
```

Your database is now ready to use with P6 Professional R8.1.

Private Database Logins for P6 Professional

Private database logins are used primarily by administrators to gain direct access to a database. For example, the privileged user login that you use to access the P6 Professional database is a private database login. You can add, modify, or delete existing logins using the Database Logins tool. This can also be accomplished using the Administration Configuration tool.

P6 Professional R8.1 includes an encryption algorithm that provides enhanced security for private database logins; however, the encryption algorithm is not automatically enforced when you manually configure or upgrade your database. If you manually configure or upgrade your database, 🛡 Oracle recommends that you use this encryption algorithm. To do so, you must reset the private database login. See ***Resetting Private Database Passwords to Use the New Encryption Algorithm*** (on page 43) for instructions. If automatically installing or upgrading your database, no configuration is needed after the upgrade to use the encryption algorithm. User logins and passwords are not affected.

Related Topics

Adding Private Database Logins for P6 Professional

To add private database logins for P6 Professional:

1) Run **databaselogins.bat** (databaselogins.sh for Linux) from the Database folder of the P6 Professional physical media or download.

2) On the **Database Connection** dialog box:
   a. Select the database, Microsoft SQL Server.
   b. Type the user name and password of a privileged database user (for example, privuser). This login should have administrative rights on the database.
   c. Enter the host address, host port, and database name specific to your Microsoft SQL Server installation. The Port field displays the default port for the database type you selected.
   d. Click **Next**.

3) On the **Private Database Logins** dialog box:
   a. Click **Add**.
   b. Enter a user name.
   c. Enter a password.
   d. To reverse a change, click **Undo**. Undo will reverse any changes made during the current session.
   e. Click **Save**.
   f. Click **OK** to exit.

Modifying Private Database Logins for P6 Professional

To modify private database logins:

1) Run **databaselogins.bat** (databaselogins.sh for Linux) from the Database folder of the P6 Professional physical media or download.

2) On the **Database Connection** dialog box:

   a. Select the database, Microsoft SQL Server.

   b. Type the user name and password of a privileged database user (for example, privuser). This login should have administrative rights on the database.

   c. Enter the host address, host port, and database name specific to your Microsoft SQL Server installation. The Port field displays the default port for the database type you selected.

   d. Click **Next**.

3) On the **Private Database Logins** dialog box:

   a. Select the private database user name that you wish to modify.

   b. Enter a new user name.

   c. Highlight the password, and change it.

   d. Click the **Update Password** button.

   e. To reverse a change, click **Undo**. Undo will reverse any changes made during the current session.

   f. Click **Save**.

   g. Click **OK** to exit the Database Logins tool.

Deleting Private Database Logins for P6 Professional

To delete private database logins for P6 Professional:

1) Run **databaselogins.bat** (databaselogins.sh for Linux) from the Database folder of the P6 Professional physical media or download.

2) On the **Database Connection** dialog box:

   a. Select the database, Microsoft SQL Server.

   b. Type the user name and password of a privileged database user (for example, privuser). This login should have administrative rights on the database.

   c. Enter the host address, host port, and database name specific to your Microsoft SQL Server installation. The Port field displays the default port for the database type you selected.

   d. Click **Next**.

3) On the **Private Database Logins** dialog box:

   a. Select the private database user name that you wish to remove.

   > **Note:** You must have at least one private user name for the P6 Professional database at all times.

   b. Click **Delete**.

   c. To reverse a change, click **Undo**. Undo will reverse any changes made during the current session.

d. Click **Save**.

e. Click **OK** to exit the Database Logins tool.

Database Administration

Read this chapter to learn how to configure the job scheduler supplied by your RDBMS, how to optimize performance of your Oracle and SQL P6 Professional databases, and how to configure the native database auditing feature to monitor edits, deletions, and additions to the databases.

In This Section

Background Processes and Clean Up in P6 Professional

Because clean up tasks can be resource intensive and time consuming, in P6 Professional, these tasks are initiated by two background jobs that run on the database server using the background job processes user name:

▸ SYMON (System Monitor), responsible for running procedures that take less than a few seconds to complete.

▸ DAMON (Data Monitor), responsible for running procedures that take longer than a few seconds to complete.

Both of these jobs are pre-configured with default settings. Since the default settings are optimal for most environments, you generally do not need to tune them. However, if further optimization is required, you can use the background job processes user to change the settings to tune the behavior of the background jobs for specific environments.

RDBMS Scheduler Configuration

Since background jobs are initiated by the job scheduler supplied by the RDBMS, you need to ensure that the scheduler for your specific RDBMS is properly configured.

P6 Professional uses the SQL Agent service to automatically schedule background job execution for Microsoft SQL Server. The maintenance of the utilities tables (for example, USESSION and REFRDEL) is handled by the background jobs. As part of background jobs, the SYMON and DAMON stored procedures are run by the agent at specific intervals.

Database Settings Table

Settings Table Overview

The settings table contains name-value pairs that configure the behavior of the background processes.

Namespace

The namespace component is a dot-notation string representing a formal path to the parameter.

Setting Name

The setting name identifies the name of the setting.

Value

Values in the SETTINGS table are case-sensitive. The value portion of the pair can be one of the following types:

▸ String. The string data type is a free text value. The most common string sub-type is interval which represents an interval of time by combining a numeric portion with a unit portion as depicted in the table below.

Table 1: Interval Subtype

	Unit portion	Example	Meaning
Numeric portion +			
	d	'30d'	Thirty day interval
	h	'2h'	Two hour interval
	m	'10m'	Ten minute interval
	s	'30s'	Thirty second interval

▸ Numeric. The numeric data type consists of any number.
▸ Boolean. The boolean data type can have one of two values: true or false, where zero represents false and any non-zero number represents true.
▸ Date.

Setting Example

The following is an example of a setting:

▸ Namespace: database.cleanup.Usession
▸ Setting Name: ExpiredSessionTimeout
▸ Value: 2h (two hour interval)

Reading Setting Values

Settings can be configured through the Settings API Procedures. These procedures are similar to registry or INI file procedure calls.

Reading Settings Values

Use the following SETTINGS_READ_* procedures to determine the current value of specific settings:

▸ `SETTINGS_READ_STRING(ret_val,namespace,settings_name,default)`
▸ `SETTINGS_READ_DATE(ret_val,namespace,settings_name,default)`
▸ `SETTINGS_READ_NUMBER(ret_val,namespace,settings_name,default)`
▸ `SETTINGS_READ_BOOL(ret_val,namespace,settings_name,default)`

Using Code to Read Setting Values for SQL

The following code snippets for the Microsoft SQL Server database demonstrate how the SETTINGS_READ_* procedures are used to read the setting values.

To retrieve the value of the KeepInterval setting in SQL:

1) Use the following code:
```
declare @vset varchar(255)
exec settings_read_string @vset
OUTPUT,'database.cleanup.Usession','ExpiredSessionTimeout'
print @vset
```
2) The following message should appear:
```
PL/SQL procedure successfully completed.
SQL> print vset
```

Writing Setting Values

Use the SETTINGS_WRITE_STRING procedure to set the value of a specific setting:

```
SETTINGS_WRITE_STRING(new value,namespace,settings_name);
```

Using Code to Write Setting Values for Microsoft SQL Server

The following code snippets for Microsoft SQL Server databases demonstrate how the SETTINGS_WRITE_STRING procedure is used to set the value of the ExpiredSessionTimeout setting to twelve hours.

To set the value of the ExpiredSessionTimeout setting to twelve hours in a Microsoft SQL Server database, use the following procedure:

1) Open the Query Analyzer/SSMS and connect as privuser.
2) Select the P6 Professional database, then run the following statement (using 12 hours as an example):

```
exec SETTINGS_WRITE_STRING '12h','database.cleanup.Usession',
'ExpiredSessionTimeout'
```

Tracking Background Job Execution

You can track the execution of background jobs by monitoring the high level status settings or by inspecting the BGPLOG table.

High Level Status Settings

Each time a job is run it will update the SETTINGS table for the setting_name = 'HeartBeatTime.' The job can update this value multiple times during the execution. The maximum difference between this time and the current date can be monitored to assure that the job is running promptly. Refer to the High Level Status Settings table below for information about the HeartBeatTime setting.

High Level Status Settings

Last date and time background job SYMON was executed.	
Namespace	database.background.Symon
Setting Name	HeartBeatTime
Default Setting	N/A

Last date and time background job DAMON was executed.	
Namespace	database.background.Damon
Setting Name	HeartBeatTime
Default Setting	N/A

The BGPLOG Table

You can also track the execution of background jobs by inspecting the BGPLOG table. The BGPLOG table holds detailed entries from the background processes including informational, elapsed time, and error entries. Refer to the BGPLOG Table Descriptions for information about what this table contains.

BGPLOG Table Descriptions

Column	Description	Value
Log_time	Time when log entry was made by background process	Datetime
Source	Program generating log entry	"system_monitor", "data_monitor"
Type	Type of message	INFORMATION, ELAPSED TIME, ERROR
Description	Message from the background process	A variable message followed by a number in parenthesis which represents the number of rows that were processed. As an example, the message "Complete BGPLOG (40)" indicates that forty rows were processed.

SYMON (System Monitor) Procedures

SYMON is meant to run simple P6 Professional tasks on a relatively quick schedule. By default the job is scheduled to run every minute and the tasks assigned to this job should not take more than a few seconds to complete on each run. The default interval of one minute should not be changed for this procedure.

Procedures performed by SYMON

The procedures run by SYMON perform the following tasks:

▸ Processing the PRMQUEUE entries for Project Security by queuing OBSPROJ updates to the PRMQUEUE table.
▸ Marking expired USESSION records as logically deleted.
   Additionally, you can manually run queries to assist you with tracking concurrent usage of P6 Professional.

OBSPROJ_PROCESS_QUEUE Procedure

The OBSPROJ_PROCESS_QUEUE procedure processes the PRMQUEUE entries for Project Security. It is used to defer processing of OBSPROJ updates by queuing the updates to the PRMQUEUE table.

Refer to the following table for information about the settings associated with the OBSPROJ_PROCESS_QUEUE procedure.

OBSPROJ_PROCESS_QUEUE Settings

Setting Description: Maximum project-level queue records to process on each run.	
Namespace	database.obsproj.queue
Setting Name	MaxProjectUpdates
Default Setting	1000
Type	Numeric
Setting Description: Maximum EPS-level queue records to process on each run.	
Namespace	database.obsproj.queue
Setting Name	MaxEpsUpdate
Default Setting	25
Type	Numeric
Setting Description: Maximum times to re-process a failed entry before marking it as an error.	
Namespace	database.obsproj.queue
Setting Name	MaxRetries
Default Setting	50
Type	Numeric

USESSION_CLEANUP_EXPIRED Procedure

The USESSION_CLEANUP_EXPIRED procedure logically deletes USESSION records that have not updated their last_active_time based on the Expired Session settings. Marking expired USESSION records as logically deleted maximizes the number of module access logins that are available. Since it is not cleaning up the underlying data (physically deleting rows), the task completes quickly.

The clean up of expired sessions is controlled by a value in the SETTINGS table. By default, although the clean up of expired sessions occurs every two hours, the SETTINGS table does not contain a value for this setting. Use the SETTINGS_WRITE_STRING (*value*, *namespace*, *setting*) stored procedure to change the default clean up value.

For example, setting the value to "2d" deletes expired sessions older than two days.

> **Note:** Oracle recommends that you set the ExpiredLongSessionTimeout sessions to at least one hour longer than your longest job. For example, if your longest job is a summarizer job that usually takes 12 hours, you should set the value in the SETTINGS table to at least 13.

Refer to the table below for information about the USESSION_CLEANUP_EXPIRED Settings.

USESSION_CLEANUP_EXPIRED Settings

Setting Description: Time-out period for normal sessions.	
Namespace	database.cleanup.Usession
Setting Name	ExpiredSessionTimeout
Default Setting	2h
Type	Interval
Setting Description: Time-out period for long running sessions based on the function preformed in the application (i.e. Scheduling, Leveling, Summarizing, etc.).	
Namespace	database.cleanup.Usession
Setting Name	ExpiredLongSessionTimeout
Default Setting	12h
Type	Interval

Tracking Concurrent Usage of P6 Professional

As an aid in tracking concurrent usage of P6 Professional, you can run queries against the USESSION and USESSAUD tables to perform self-audits. Example queries are provided below.

> **Note:** See ***DAMON (Data Monitor) Procedures*** (on page 62) for information on how to set up the USESSAUD procedure; however, to ensure accuracy of these queries, make sure to run them before physically deleting remaining USESSION records and cleaning up the USESSAUD table.

▸ Against the USESSION table, run the following query to determine how many users are logged in at a given time:

```
select count(*) from usession where delete_session_id is null
```

▸ Against the USESSION table, run the following query to determine how many users are logged into a specific P6 Professional product at a given time:

```
select count (*) from usession where delete_session_id is null and
app_name='P6 Professional product name'
```

where *P6 Professional product name* is the application abbreviation.

> **Note:** You can view all available application abbreviations by running the following query as an administrative database user:
> ```
> select distinct(db_engine_type) from usereng
> ```

▸ Against the USESSAUD table, run a query similar to the following to determine how many users logged into P6 Professional on a specific date during a specified time range. You can alter the date, time range, and P6 Professional product as needed. The following example will search for all users who logged into P6 Professional on February 17, 2010 between 9am and 10am:

```
select * from usessaud where login_date between to_date('17-FEB-10
09:00:00','DD-MON-YY HH:MI:SS') and to_date('17-FEB-10
10:00:00','DD-MON-YY HH:MI:SS') and app_name='Project Management'
```

DAMON (Data Monitor) Procedures

The second database job is the DAMON data monitor job. The DAMON job runs the majority of the background processing and is responsible for running background clean up processes required by the application that can potentially take a relatively long time to run.

Microsoft SQL Server

DAMON runs weekly on every Saturday, by default. It can be set to run every two weeks or on a specific day. To run DAMON every two weeks, use the following command to set the interval: `-eg 2W`

To set DAMON to run on a specific day, use the following setting under namespace: `'Database.background.Damon'` *DayOfWeek*

Procedures performed by DAMON

The procedures run by DAMON perform the following tasks:

▸ Cleaning up the BGPLOG table containing the background logs.

- ▶ Cleaning up the REFRDEL table.
- ▶ Cleaning up the PRMQUEUE table.
- ▶ Physically cleaning up remaining USESSION records.
- ▶ Cleaning up logically deleted records.
- ▶ Cleaning up the PRMAUDIT table.
- ▶ Cleaning up the USESSION audit table (USESSAUD).

Additionally, the functionality of the DAMON process can be dynamically extended via the user-defined procedure, USER_DEFINED_BACKGROUND.

BGPLOG_CLEANUP Procedure

This procedure keeps the BGPLOG table at a reasonable size. The default clean up interval is 5 days which will result in a table size of about 54,000 records.

Refer to the following table for information about the settings associated with the BGPLOG_CLEANUP procedure.

BGPLOG_CLEANUP Settings

Setting Description: The oldest records to keep in the BGPLOG table.	
Namespace	database.cleanup.BackGroundProcessLog
Setting Name	KeepInterval
Default Setting	5d
Type	Interval

REFRDEL_CLEANUP Procedure

This procedure physically deletes records from the REFRDEL table based on the value of the KeepInterval setting. The default setting keeps the REFRDEL records from the last five days.

Refer to the following table for information about the settings associated with the REFRDEL_CLEANUP procedure:

REFRDEL_CLEANUP Settings

Setting Description: The oldest records to keep in the REFRDEL table.	
Namespace	database.cleanup.Refrdel
Setting Name	KeepInterval

Default Setting	5d
Type	Interval
Setting Description: Identifies the maximum number of minutes up to which records are to be deleted from the REFRDEL table.	
Namespace	database.cleanup.Refrdel
Setting Name	DaysToDelete
Default Setting	1d
Type	Interval
Setting Description: Determines the number of minutes for each step interval.	
Namespace	database.cleanup.Refrdel
Setting Name	IntervalStep
Default Setting	15m
Type	Interval

CLEANUP_PRMQUEUE Procedure

This procedure physically deletes records from the PRMQUEUE table based on the value of the KeepInterval setting. The remaining settings are similar to the REFRDEL_CLEANUP.

Refer to the following table for information about the settings associated with the CLEANUP_PRMQUEUE procedure:

CLEANUP_PRMQUEUE Settings

Setting Description: The oldest records to keep in the PRMQUEUE table. Default is five days.	
Namespace	database.cleanup.Prmqueue
Setting Name	KeepInterval
Default Setting	5d

Type	Interval
Setting Description: Determines whether the procedure will delete all of the PRMQUEUE records possible on each pass.	
Namespace	database.cleanup.Prmqueue
Setting Name	DeleteAll
Default Setting	0 (false)
Type	Boolean
Setting Description: Determines whether all of the records are cleaned up. If the total record count is less than this number then all the records are cleaned up.	
Namespace	database.cleanup.Prmqueue
Setting Name	DeleteAllThreshold
Default Setting	1,000
Type	Numeric
Setting Description: Percentage of records to delete on each pass.	
Namespace	database.cleanup.Prmqueue
Setting Name	DeletePercentage
Default Setting	10(%)
Type	Numeric
Setting Description: Maximum rows to delete on each pass.	
Namespace	database.cleanup.Prmqueue
Setting Name	MaxRowsToDelete
Default Setting	10,000
Type	Numeric

USESSION_CLEAR_LOGICAL_DELETES Procedure

This procedure physically deletes all logically deleted USESSION records. There are no settings associated with this procedure: All logically deleted USESSION records are cleared.

CLEANUP_LOGICAL_DELETES Procedure

This procedure removes logically deleted rows based on the value of the KeepInterval setting. Records in the database can be marked as deleted (logically deleted) by setting the DELETE_SESSION_ID column to a non-null value. By default, records that were deleted more than 5 days ago will be physically deleted by this procedure.

> **Note:** The CLEANUP_LOGICAL_DELETES procedure will not physically delete records whose DELETE_SESSION_ID column is set to a negative value.

Refer to the following table for information about the settings associated with the CLEANUP_LOGICAL_DELETES procedure:

CLEANUP_LOGICAL_DELETES Settings

Setting Description: The oldest logically deleted records to keep in tables.	
Namespace	database.cleanup.LogicalDelete
Setting Name	KeepInterval
Default Setting	5d
Type	Interval
Setting Description: Determines whether the procedure will delete all of the logically deleted records possible on each pass.	
Namespace	database.cleanup.LogicalDelete
Setting Name	DeleteAll
Default Setting	0 (false)
Type	Boolean
Setting Description: Maximum rows to delete on each pass.	
Namespace	database.cleanup.LogicalDelete
Setting Name	MaxRowsToDelete
Default Setting	10,000
Type	Numeric

PRMAUDIT_CLEANUP Procedure

If the auditing feature is enabled, this procedure will physically delete records from the table based on the value of the KeepInterval setting.

Refer to the following table for information about the settings associated with the PRMAUDIT_CLEANUP procedure:

PRMAUDIT_CLEANUP Settings

Setting Description: Should the procedure attempt to clean up PRMAUDIT records.	
Namespace	database.cleanup.auditing
Setting Name	Enabled
Default Setting	1 (true)
Type	Boolean
Setting Description: The oldest audit records to keep in PRMAUDIT.	
Namespace	database.cleanup.auditing
Setting Name	KeepInterval
Default Setting	30d
Type	Interval

CLEANUP_USESSAUD Procedure

This procedure physically deletes records from the USESSAUD table based on the KeepInterval. The remaining settings are similar to the REFRDEL_CLEANUP procedure.

Refer to the following table for information about the settings associated with the CLEANUP_USESSAUD procedure:

CLEANUP_USESSAUD Settings

Setting Description: The oldest records to keep in the USESSAUD table.	
Namespace	database.cleanup.Usessaud

Setting Name	KeepInterval
Default Setting	5d
Type	Interval
Setting Description: Determines whether the procedure delete all the REFRDEL records possible on each pass.	
Namespace	database.cleanup.Usessaud
Setting Name	DeleteAll
Default Setting	0 (false)
Type	Boolean
Setting Description: Determines whether all of the records are cleaned up. If the total record count is less than this number then all records are cleaned up.	
Namespace	database.cleanup.Usessaud
Setting Name	DeleteAllThreshold
Default Setting	1,000
Type	Numeric
Setting Description: Percentage of records to delete on each pass.	
Namespace	database.cleanup.Usessaud
Setting Name	DeletePercentage
Default Setting	10 (%)
Type	Numeric
Setting Description: Maximum rows to delete on each pass.	
Namespace	database.cleanup.Usessaud
Setting Name	MaxRowsToDelete
Default Setting	10,000
Type	Numeric

USER_DEFINED_BACKGROUND Procedure

This procedure is an optional customer procedure that is run by DAMON. There are no settings associated with this procedure.

Safe Deletes

The P6 Professional database normally handles restoring select deleted data using a safe delete setting. While using P6 Professional, the Undo command (Edit, Undo) allows users to restore certain types of data that have been deleted. Deleted data remains in the P6 Professional database until the CLEANUP_LOGICAL_DELETES procedure clears it (after 5 days, by default).

See the *P6 Professional Help* for more information about using undo.

Turning Off Safe Deletes

You can turn off safe deletes to save storage space. Turning off safe deletes disables undo functionality and instantly clears deleted data from the P6 Professional database.

To turn off safe deletes:

1) Verify the current state of your safe deletes setting. In the database, if the table ADMIN_CONFIG has the following row, a CONFIG_VALUE of 'N' means turn off safe deletes.

```
CONFIG_NAME = 'SAFEDELETE.ACTIVE' and CONFIG_TYPE = 'SETTINGS'
```

> **Note:** This is only loaded at startup. If you change CONFIG_VALUE while a user is running P6 Professional, the setting will not apply until the user restarts the P6 Professional session.

2) Once you have determined the current state of your safe deletes setting, run one of the following statements.

   ‣ To turn off safe deletes for the first time:

   ```
   INSERT INTO ADMIN_CONFIG (CONFIG_NAME, CONFIG_TYPE, CONFIG_VALUE)
   VALUES ('SAFEDELETE.ACTIVE', 'SETTINGS', 'N')
   ```

   ‣ To turn on safe deletes after it has been turned off:

   ```
   UPDATE ADMIN_CONFIG SET CONFIG_VALUE = 'Y' WHERE CONFIG_NAME =
   'SAFEDELETE.ACTIVE' AND CONFIG_TYPE = 'SETTINGS'
   ```

   ‣ To turn off safe deletes after it has been turned on:

   ```
   UPDATE ADMIN_CONFIG SET CONFIG_VALUE = 'N' WHERE CONFIG_NAME =
   'SAFEDELETE.ACTIVE' AND CONFIG_TYPE = 'SETTINGS'
   ```

Native Database Auditing

Native database auditing permits you to log the edits, additions, and deletions made by users of P6 Professional applications. Native database auditing takes advantage of the fact that every change made by a user results in a Data Manipulation Language (DML) INSERT, UPDATE, or DELETE statement being executed against tables in the database schema. Since every application table in the schema has its own auditing trigger, you can log changes made to each table regardless of who made the change or when the change was made. The database schema owner owns the auditing trigger: trigger execution cannot be bypassed.

Auditing Level Configuration

You can adjust the amount of information that is logged by adjusting the audit level for each table. The granularity of the audit can be refined further by setting the audit level individually for insert, updates and deletes within each table.

Auditing Levels

Level	Description
Level 0	No audit.
Level 1	Row-level audit. Audit only the operation without column details
Level 2	Column-level Audit without blobs. Audit changes to the data at the column level but without blob changes
Level 3	Full Audit. Audit changes to the data at the column level. For Microsoft SQL server, column level changes to blobs are not included.

Simple Configuration

There are two configuration procedures available that provide for the simple control of the auditing feature:

▸ auditing_enable(*table_name*, *level*)
▸ auditing_disable(*table_name*)

These procedures allow for setting the audit level on an individual table or the same audit level for all of the tables. However, the simple configuration procedures do not allow for setting individual auditing levels for insert, update, or delete operations within a table.

Detailed Configuration

You can configure auditing trigger behavior by changing values in the settings table that enable or disable the following auditing features:

▸ The auditing feature itself
▸ The auditing of specific tables
▸ The auditing of table insert, update, or delete operations within each table

Auditing Status

You can enable or disable the auditing feature itself by using the database.audit.Enable setting. Use the settings_write_bool procedure to enable/disable the overall auditing feature.

Microsoft SQL Server Example:

To enable the overall auditing feature in Microsoft SQL Server, use the following code:

```
exec settings_write_bool 1,'database.audit','Enabled'
```

Options Setting

Each individual table's auditing settings are controlled by the Options setting in each table's auditing namespace (for example, database.audit.TASK). The Options setting is a three character string with a numeric value in each character position representing the audit level for insert, update, and delete, respectively.

Auditing Level Options Setting by Table Operation

	Operation			
	Insert	Update	Delete	Description
Level	0	0	0	No audit.
	1	1	1	Row-level audit. Audit only the operation without column details
	2	2	2	Column-level audit without blobs. Audit changes to the data at the column level but without blob changes

	3	3	3	Full Audit. Audit changes to the data at the column level. For Microsoft SQL server, column level changes to blobs are not included.

The following table provides some example uses of the options setting:

Setting the Auditing Level Options Setting by Table Operation Examples

Namespace	Setting	Value	Description
database.audit.TASK	Options	330	Fully audit any insert and update operations. Do not audit any delete operations.
database.audit.PROJWBS		001	Row-level audit on deletes only.
database.audit.TASKRSRC		333	Fully audit.

SETTINGS_WRITE_STRING Procedure

Individual table audit settings can be changed using the settings_write_string procedure.

Microsoft SQL Server Example:

To set the table settings to fully audit insert and update operations but ignore any delete operations, use the following code for Microsoft SQL Server:

```
exec settings_write_string '330','database.audit.TASK','Options'
```

> **Note:** Changes to auditing settings will not necessarily be reflected immediately in the application. In general the program will need to close the database connection and then reconnect to the database to get the new settings.

The Audit Table

Audit records are inserted into the PRMAUDIT table. One record is inserted into the audit table for each row changed in the database.

PRMAUDIT Table

Column	Type	Description
audit_date	Date	Date and time of change
table_name	String(30)	Table Name
pk1, pk2, pk3, pk4	String(255)	Primary key values for audited record
oper	String(1)	I=Insert, U=Update, D=Delete
prm_user_name	String(32)	P6 Professional user name if the change was made in P6 Professional applications
audit_info	String(4000)	Column changes up to 4000 characters (Level 2 and 3 only)
audit_info_extended	BLOB	Blob changes and overflow from audit_info (Level 2 and 3 only)
logical_delete_flag	String(1)	Flag for deletes that are logical (marked) rather that a physical delete
rdbms_user_name*	String(255)	Database user name (usually privuser)
os_user_name*	String(255)	Operating system user name of connected session
program*	String(255)	Name of program connecting to the database
host_name*	String(255)	Computer name of connected session
app_name*	String(25)	Name of application connected to the database
netaddress*	String(24)	IP or MAC address of connected session
* Values will differ from Microsoft SQL Server and Oracle		

Note: Select privileges should be granted to the administrative user on V_$SESSION to assure correct values for several auditing table values.

Session Auditing

Activity for the USESSION table is audited with its own trigger and table. When an application user logs out of the system they logically delete, or mark, their session record in the USESSION table. One record is written to the USESSAUD table for each logout. The format of the USESSAUD table mirrors that of the USESSION table. This audit can be enabled using the usessaud_enable procedure and disabled using the usessaud_disable procedure.

Column Audit Data

The data changes for each audit are stored in the audit_info and audit_info_extended columns. The audit_info column contains all the row changes as long as they do not exceed 4000 characters. Changes over 4000 characters or any edit to a blob will be written to the audit_info_extended BLOB column.

Data in the two audit_info columns has a specific format. Each column audit within the data begins with either ":O" (old data) or ":N" (new data) to distinguish between the audit of the previous (old) or the changed (new) value (for BLOB columns the data starts with :BLOBO or :BLOBN). Directly after this is the name of the column in lowercase. Following the column name is the length of the audited value in a fixed four character field. Finally the actual data is placed in the audit record. Updates will have both an old and new value for each change. Inserts will have only a new value and deletes only an old value.

The following is an example of the audit record for a change to the TASK to change the task_code from 'A1010' to 'B102:'

```
audit_info =>:Otask_code: 5:A1010:Ntask_code: 4:B102
```

P6 Professional Database Connections Using a Non-Default Microsoft SQL Server Port

If you use a port other than the default (1433) to connect to your Microsoft SQL Server P6 Professional database, you might have to perform additional configuration steps to allow users access to functions within P6 Professional that rely on the P6 Integration API (for example, Update Baseline). Not all users will experience access issues. See **Configuring Client Machines for a Non-Default Microsoft SQL Server Port** (on page 83) after installation of P6 Professional to determine if a user will be affected.

Once you have determined which users are affected, you can either globally specify the connection string in the P6 Professional database SETTINGS table or install Microsoft SQL Server 2005 Backward Compatibility Components on each client machine.

See **Database Administrator Settings for a Non-Default Microsoft SQL Server Port** (on page 75) if you choose to specify the connection string. See step 7 in **Configuring Client Machines for a Non-Default Microsoft SQL Server Port** (on page 83) if you choose to configure each client machine.

Database Administrator Settings for a Non-Default Microsoft SQL Server Port

To enable users to utilize P6 Integration API functionality within P6 Professional when using a non-default Microsoft SQL Server port, add an ADMINISTRATOR_SETTINGS row to the SETTINGS table for each Microsoft SQL Server database you use with P6 Professional. The table below summarizes the settings.

ADMINISTRATOR_SETTINGS Settings

Setting Description: Points to the JDBC connection URL for a P6 Professional Microsoft SQL Server database.	
Namespace	Administrator_Settings
Setting Name	JdbcConnectionURL
Setting Value	*jdbc connection url*

When entering a value for *jdbc connection url* for Microsoft SQL Server, use the standard connection string. For example,

jdbc:sqlserver://*servername*:*portnumber*;database=*databasename*;

Installing P6 Professional

Read this chapter to install P6 Professional, the P6 SDK, and Job Service. Run the Setup wizard on the client/desktop computers that will be used by project personnel.

Install P6 Professional only after you install and configure the database server. The Setup wizard needs to connect to the database server when installing P6 Professional.

To install P6 Professional standalone, see the *P6 Professional Standalone Installation and Configuration Guide*.

In This Section

Database Client Software

Before you install P6 Professional, first install the client software for the database you will be using. The database client software enables the client computer to connect over the network to the database on the server computer.

Microsoft SQL Server Database Client Software

When you install P6 Professional on a client computer, the Microsoft SQL Server client files necessary to connect to P6 Professional are automatically installed for you. Or, you can also use your Microsoft SQL Server installation CD to install the client network utility. If you are unfamiliar with this process, please contact your database administrator.

See *Configuring Client Machines for a Non-Default Microsoft SQL Server Port* (on page 83) after you install P6 Professional if you use a port other than the default (1433) to connect to your Microsoft SQL Server P6 Professional database.

Previous Versions of P6 Professional

P6 Professional replaces previous versions. To update to P6 Professional R8.1 from version 6.2, 6.2.1, or 7.0 simply run Setup. Only P6 Professional is replaced; all previous versions of P6 SDK and Job Services must be uninstalled. P6 Professional will run alongside P6 Professional R8 or P6 Optional Client R8.1.

> **Caution** - If you are upgrading the P6 SDK, you must first uninstall the prior version before installing R8.1 of the P6 SDK.

See **Importing Projects from P3 to P6 Professional** (on page 173) in the appendix prior to P6 Professional installation if you plan to transfer data from/to P3. See **Configuring Client Machines to Transfer Data Between P3 and P6 Professional** (on page 83) after installation.

Tip

- Summary-Only projects are not supported in P6 Professional starting with R8. During the P6 Professional database upgrade, existing Summary-Only projects are converted to standard projects, but will lose all summary data. You can import the summary project from Microsoft Project into the converted blank project, and then summarize the data. See the P6 Professional Help.

- For security reasons, Oracle strongly recommends that you replace the default Admin Superuser (admin) immediately after a manual database installation or an upgrade from P6 version 7.0 and earlier.

About the P6 Professional Setup Wizard

Install P6 Professional, P6 SDK, and Job Service by running the Setup wizard. The first several steps of the installation process are the same for these applications. You do not have to install these applications separately; you can install all at the same time. The installation instructions are separated into sections to provide you with information that is relevant only to specific applications.

The Setup wizard displays the amount of disk space required to install P6 Professional, P6 SDK, and Job Service. Administrator rights are required to install these applications on computers running Windows XP, Windows XP SP3, Windows Vista, Windows Vista SP2, or Windows 7. Also, the network protocol TCP/IP must be installed on the client computer.

If you do not want to install P6 Professional manually, you can run an unattended setup. See **Unattended Setup for P6 Professional** (on page 99).

> **Notes**:
>
> - See **Previous Versions of P6 Professional** (on page 78) before running the Setup wizard if version 6.0 or later of P6 Professional is currently installed.
> - The Primavera Timescaled Logic Diagram will be automatically installed when you install P6 Professional.

- The P3 application is required for users with 32-bit operating systems to be able to import and export P3 data. Make sure that P3 is installed PRIOR to running the P6 Professional setup wizard. See **Configuring Client Machines to Transfer Data Between P3 and P6 Professional** (on page 83) after P6 Professional is installed for additional configuration procedures. See **Importing Projects from P3 to P6 Professional** (on page 173) for instructions on how to manually register required files after the installations are complete if you install P3 after you install P6 Professional, if you do not want to install P3 on the same machine where P6 Professional is installed, or if you are using 64-bit operating systems.

Installing P6 Professional

Complete the following steps to install P6 Professional.

Related Topics

Installing the P6 Professional Application for Typical Use

To install the application:

1) Double-click **setup.exe** in the Client_Applications folder of the P6 Professional physical media or download.

   Notes:

   - Click **Next** on each wizard dialog box to advance to the next step. Click **Cancel** at any time to exit the wizard.
   - Click **Disk Usage** to see disk space requirements for the installation of selected features.

2) Microsoft .NET Framework 4.0, Windows Installer 4.5, and JRE 1.6.0_24 are required to run P6 Professional. If they are not installed, follow the prompts to install them and then restart your computer when prompted. Allow setup.exe to run when your computer restarts and follow the prompts to complete installation of the required components.

   Note: Microsoft Windows Imaging Component is required for .NET 4.0 installation on 64-bit Windows XP SP2 systems. This component can be downloaded from Microsoft at **http://www.microsoft.com/downloads/en/details.aspx?FamilyID=F64654AC-6E26-41D9-A90A-0E7783B864EE**

3) On the **Welcome** dialog box, click **Next**.

4) On the **Setup Type** dialog box, choose **Typical** to install P6 Professional.

>   **Note**: By default, the installation location is: *local drive*\Program Files\Oracle\Primavera P6\P6 Professional. Choose **Custom** then **Browse** to set a new destination folder.

5) Click **Install** to begin the installation.

>   **Note**: During installation the Database Configuration wizard will prompt you for your database credentials. If you prefer to supply database credentials later, click **Cancel**. You can run the database configuration tool from the start menu at any time.

6) Click **Finish** to complete the installation.

Configuring the Database Connection for P6 Professional

To configure the database connection and complete the P6 Professional installation process:

1) In the **Select Driver Type** dialog box, select the driver type of your P6 Professional database server, Microsoft SQL Server.

2) In the **Configure SQL Server Connection** dialog box, enter the database connection settings.

   Type the database host name and database name. The host name is the name of the computer or IP address where Microsoft SQL Server is installed. The database name was specified when the database was created; for example, PMDB.

3) In the **Enter Public Login Information** dialog box, enter your public login information that was defined by your administrator.

4) In the **Validate Database Connection** dialog box, click **Next** to test the database connection.

5) If the connection was not successful, click **Back** to revise the database information.

   If the connection was successful, click **Finish** to complete the database connection configuration.

6) Click **Finish** to complete the installation.

Tips

For instructions on how to configure P6 Compression Server, see the *P6 Compression Server Administrator's Guide*.

Set the industry type

The industry type that you choose determines the terminology and default settings that display in P6 Professional.

An upgrade or a new installation of P6 Professional database leaves the industry type field blank and requires the system administrator to set it. So immediately after the installation, the administrator must use the Admin Preferences, Industry tab in P6 Professional to select an appropriate industry type.

Use the following steps to select the industry type.

1) Choose Admin, Admin Preferences.
2) Click the Industry tab.
3) Select the option that most closely aligns with your industry.

Notes

▶ If you set the industry type and later change it, the change will not take effect for users who have logged in since it was last set until you clear their USERDATA; the new industry setting is immediately effective for new users.

▶ The following table lists each industry type and its corresponding terminology and default settings:

Industry Type	Industry Terminology Examples	Default project comparison tool
Engineering and Construction	Budgeted Units Budgeted Cost Original Duration	Claim Digger
Government, Aerospace, and Defense	Planned Units Planned Cost Planned Duration	Schedule Comparison
High-Technology, Manufacturing	Planned Units Planned Cost Planned Duration	Schedule Comparison
Utilities, Oil, and Gas	Budgeted Units Budgeted Cost Original Duration	Claim Digger
Other Industry	Planned Units Planned Cost Planned Duration	Schedule Comparison

About the Database Configuration Wizard for P6 Professional

Use the Database Configuration wizard to change connection settings for the client module if your database server configuration changes. For example, if the database is moved to a new server, run the Database Configuration wizard to configure the connection to the new server.

> **Note:** To be able to change database connection settings, the Database Configuration wizard must access the module's PrmBootStrap.xml file. This file is located the following places:
>
> - In Windows XP, *local drive*\%USERPROFILE%\Local Settings\Application Data\Oracle\Primavera P6\P6 Professional
> - In Windows Vista or Windows 7, *local drive*\%LOCALAPPDATA%\Oracle\Primavera P6\P6 Professional

Changing Database Connection Settings for P6 Professional

To change database connection settings:

1) From the client computer's desktop, click **Start**, then choose **Programs**, **Oracle - Primavera P6**, **P6 Professional R8.1**, **P6 Professional Help and Tools**, **Database Configuration**.

2) On the **Welcome** dialog box, click **Next**.

> **Note:** Click Next on each wizard dialog box to advance to the next step.

3) On the **Select Database Alias Task** dialog box, choose to either **modify an existing database** or **create a new database alias**.

4) On the **Select or Create Alias** dialog box, select the alias and driver type of the database.

   If you are changing the alias or database driver, type the new alias (for example, PMDB) or select the new driver type (Microsoft SQL Server).

> **Note:** For information about the Primavera Compression Server driver type, see the *P6 Compression Server Administration Guide*.

5) On the **Configure SQL Server Connection** dialog box, enter the new database connection settings.

   Type the database host name and database name. The host name is the name of the computer or IP address where Microsoft SQL Server is installed. The database name was specified when the database was created; for example, PMDB.

6) On the **Enter Public Login Information** dialog box, enter your public login information that was defined by your administrator.

7) On the **Validate Database Connection** dialog box, review the settings and click **Next** to test the database connection.

8) If the connection was not successful, click **Back** to revise the database information.

   If the connection was successful, click **Finish** to complete the database connection configuration.

Tips

▶ If you create a new database alias for a module, the module's PrmBootStrap.xml file is updated to reflect the change. If multiple modules are installed on one client computer, changing the database alias for one module does not affect the other modules.

▶ If you change the database connection settings for a database alias and multiple modules share that alias to access the database, your changes affect all the modules that share the alias.

Configuring Client Machines to Transfer Data Between P3 and P6 Professional

In order to use P3 import/export functionality in P6 Professional with 32-bit operating systems, you must have P3 installed on the same machine where P6 Professional resides.

Note: If you install P3 after you install P6 Professional, if you do not want to install P3 on the same machine where P6 Professional is installed, or if you are using 64-bit operating systems, direct your P3 users to use a separate P3/XER import/export utility available from the P6 Professional installation location (by default, the path is *local drive*\Program Files\Oracle\Primavera P6\P6 Professional\Convert). Refer to the My Oracle Support's Knowledge Articles for more information.

Configuring Client Machines for a Non-Default Microsoft SQL Server Port

If you use a port other than the default (1433) to connect to your Microsoft SQL Server P6 Professional database, you might have to perform additional configuration steps. To determine if you need to perform those steps, proceed as follows after installation of P6 Professional:

1) Launch P6 Professional from the client machine.

2) Choose **Help**, **About Primavera P6 Professional.**

3) From the **About Primavera P6 Professional** dialog box, click the **System** tab.

4) Under **BRE Database**, locate the database port number.

5) If the **non-default port number** appears, no further action is necessary.

   If **port number 1433** is listed, the user does not have Microsoft SQL Server 2005 Backward Compatibility Components installed. Proceed to the next step.

6) Choose to either globally specify the connection string in the P6 Professional database SETTINGS table or install Microsoft SQL Server 2005 Backward Compatibility Components on each client machine.

See ***Database Administrator Settings for a Non-Default Microsoft SQL Server Port*** (on page 75) if you choose to specify the connection string. If you choose to configure each client machine, proceed to the next step.

7) Download an updated version of Microsoft SQL Server 2005 Backward Compatibility Components (SQL Server2005_BC.msi for 32-bit operating systems and SQLServer2005_BC_x64.msi for 64-bit operating systems) from the following location: ***http://www.microsoft.com/downloads/details.aspx?FamilyID=d09c1d60-a13c-4479-9b91-9e8b9d835cdc&DisplayLang=en***

Installing the P6 SDK

The P6 SDK makes P6 Professional data available for use by external applications. In addition to data, the P6 SDK provides application business rules and calculated values, and enforces application security. The P6 SDK supports the Open Database Connectivity (ODBC) standard for connecting to the P6 Professional database. ODBC-compliant interfaces, such as OLE DB, are also supported.

Complete the following steps to install the P6 SDK.

Related Topics

Installing the P6 SDK Application

To install the application:

1) Double-click **setup.exe** in the Client_Applications folder of the P6 Professional physical media or download.

> **Notes**:
> - Click **Next** on each wizard dialog box to advance to the next step. Click **Cancel** at any time to exit the wizard.
> - Click **Disk Usage** to see disk space requirements for the installation of selected features.

2) Microsoft .NET Framework 4.0, Windows Installer 4.5, and JRE 1.6.0_24 are required to run P6 Professional. If they are not installed, follow the prompts to install them and then restart your computer when prompted. Allow setup.exe to run when your computer restarts and follow the prompts to complete installation of the required components.

> **Note**: Microsoft Windows Imaging Component is required for .NET 4.0 installation on 64-bit Windows XP SP2 systems. This component can be downloaded from Microsoft at ***http://www.microsoft.com/downloads/en/details.aspx?FamilyID=F64654AC-6E26-41D9-A90A-0E7783B864EE***

3) On the **Welcome** dialog box, click **Next**.

4) On the **Setup Type** dialog box, choose **Custom**.

> **Note**: These instructions assume that you have not already installed P6 Professional, if you have not, P6 Professional will be installed with this component unless you select **Entire feature will be unavailable** under **P6 Professional**. See Installing P6 Professional for instructions on completing P6 Professional installation.

5) Click **Primavera P6 Professional**.

6) Click **Other Components**.

7) Click **Software Development Kit** and select **Will be installed on local hard drive**.

8) On the **Ready to Install the Program** screen, click **Install** to begin the installation.

9) On the **Select or Create Alias** dialog box, select the alias and driver type of the database.

    If you are changing the alias or database driver, type the new alias (for example, PMSDK) or select the new driver type (Microsoft SQL Server).

10) On the **Configure SQL Server Connection** dialog box, enter the new database connection settings.

    Type the database host name and database name. The host name is the name of the computer or IP address where Microsoft SQL Server is installed. The database name was specified when the database was created; for example, PMSDK.

> **Note:** For information about the Primavera Compression Server driver type, see the *P6 Compression Server Administration Guide*.

11) On the **Enter Public Login Information** dialog box, enter your public login information that was defined by your administrator.

12) On the **Validate Database Connection** dialog box, review the settings and click **Next** to test the database connection.

13) Click **Finish** to exit the Setup Wizard.

Installing the Job Service

The Job Service enables you to automate certain functions. You can apply actuals, run a batch report, export projects, schedule projects, and summarize projects. These operations run in the background at specified intervals. The Job Service runs as a Windows 2003/2008 service and can support an unlimited number of jobs, each with its own schedule of execution. Jobs are defined in P6 Professional and stored in the organization's project management database.

Related Topics

Installing the Job Service and Distributed Job Service

To install the application:

1) Double-click **setup.exe** in the Client_Applications folder of the P6 Professional physical media or download.

    Notes:

    ▪ Click **Next** on each wizard dialog box to advance to the next step. Click **Cancel** at any time to exit the wizard.

    ▪ Click **Disk Usage** to see disk space requirements for the installation of selected features.

2) Microsoft .NET Framework 4.0, Windows Installer 4.5, and JRE 1.6.0_24 are required to run P6 Professional. If they are not installed, follow the prompts to install them and then restart your computer when prompted. Allow setup.exe to run when your computer restarts and follow the prompts to complete installation of the required components.

    Note: Microsoft Windows Imaging Component is required for .NET 4.0 installation on 64-bit Windows XP SP2 systems. This component can be downloaded from Microsoft at *http://www.microsoft.com/downloads/en/details.aspx?FamilyID=F 64654AC-6E26-41D9-A90A-0E7783B864EE*

3) On the **Welcome** dialog box, click **Next**.

4) On the **Setup Type** dialog box, choose Custom.

5) On the **Custom Setup** dialog box, expand **Primavera P6 Professional**, expand **Other Components**, click the Job Service icon and select **Will be installed on local hard drive**.

    Notes:

    ▪ These instructions assume that you have not already installed P6 Professional, if you have not, P6 Professional will be installed with this component unless you select **Entire feature will be unavailable** under **P6 Professional**. See Installing P6 Professional for instructions on completing P6 Professional installation.

- If you want to run Job Service jobs in a language other than English, you must install P6 Professional on the Job Service machine. You can install it along with the Job Service, or you can install it at another time.

6) Click **Next** then click **Install.** Setup will verify that the user has administrator rights on the computer. If the user does not have administrator rights, the Setup wizard will end.

7) On the Job Service Alias dialog box:

a. Type the database alias in the DB Alias field; for example, JSDB. Do not use dashes as part of the DB alias; otherwise, an error will occur.

8) Enter or select the program folder.

9) Click Install to begin the installation.

10) On the Select Driver Type dialog box, in the Job Services driver type field, choose the database server type.

▸ If you are connecting to Oracle, on the Configure ORACLE Connection dialog box, use the Oracle EZCONNECT string (*//server name:listen port/service name*) to connect to the P6 Professional database. If you wish to use the TNSNAMES file instead of EZCONNECT, the TNSNAMES file will be in the Oracle home folder on the client machine, not in a shared location. Reference the TNSPING.EXE location in your path environment variable.

▸ If you are connecting to Microsoft SQL Server, on the Configure SQL Server Connection dialog box, type the database name and specify the server computer name.

11) On the Enter Public Login dialog box, enter your public login information that was defined by your administrator; for example, a user name of pubuser, and a group ID of 1.

12) On the Validate Database Connection dialog box, click Next to validate the database connection. The DB alias that you specified is created.

13) On the Connection Successful dialog box, click **Finish**. You are prompted to test the Job Service alias.

> **Caution**: If you are installing on a SERVER machine in a Distributed Job Services environment, DO NOT click the Test button as described in the following step.

14) Click **Yes** to test the database connection. If the test fails, you can still continue the installation.

15) Click **Finish**.

Once the Job Service is installed on your computer and it is able to successfully connect to the database, the service will periodically run any user-defined jobs that are scheduled in P6 Professional. If you are using Windows 2008 Server, refer to required configuration instructions below.

Configuring Windows 2008 Server for Job Services

After installing Job Services, the following configuration steps are required for Windows 2008 Servers:

1) From the command line (or Start, Run utility), run **dcomcnfg**. The Component Services dialog box appears.

2) In the **Component Services** dialog box, expand the tree in the left panel by clicking Component Services, Computers, My Computer, DCOM Config.

3) Right-click on the **{9E521861-5A76-11D5-98F4-00C0F680F1F}** entry in the right panel and select Properties.

4) In the **Properties** dialog box, on the **Identity** tab, select the **This User** option. Enter the Password for a user who has administrative privileges on the machine you are using.

5) Click **OK** to close the dialog box.

Set the Job Service Log On Account

1) From the Windows **Control Panel**, select **Administrative Tools**, **Services**.

2) Double-click the **Primavera P6 Job Service**.

3) On the **Primavera P6 Job Service Properties** dialog box, select the **Log On** tab.

4) Select the **This Account** option and enter the account and password of an administrative user.

5) Click **Apply**, **OK**.

Configure the Job Service to Send Jobs Directly to a Printer

To send jobs directly to a printer, you must run the Job Service using an administrator account that can access a printer rather than the general system account. On the machine running the Job Service, complete the following steps to login to the Job Service using your administrator user name and password.

1) From the Windows **Control Panel**, select **Administrative Tools**, **Services**.

2) Double-click the **Primavera P6 Job Service**.

3) On the **Primavera P6 Job Service Properties** dialog box, select the **Log On** tab.

4) Select the **This Account** option and enter the account and password of an administrative user.

5) Click **Apply**, **OK**.

Specify a Different Language for the Job Service

You can specify the output language for Job Service jobs. Complete the following steps to specify a language other than English:

1) Login to the Job Service using your administrator account rather than the system account.

2) If you did not install P6 Professional when you installed the Job Service install the P6 Professional module on the Job Service machine.

3) After P6 Professional is installed and the database configured, start the module by choosing **Start**, **All Programs**, **Oracle - Primavera P6**, **P6 Professional R8.1** from the Start menu.

4) Login to the P6 Professional using the same administrator account you used to login to the Job Service.

5) If the **Welcome** dialog box appears, choose **Open Global Data Only**.

6) Choose **Tools**, **Set Language**, then select the language.

> **Note**: The Job Service will run jobs in the selected language assuming that the Job Service continues to run using the administrator account you used to login. If, at any time, a different login is specified, you must repeat these steps using the alternate login. You cannot run Job Service jobs in a different language using the local system account.

Configuring Distributed Job Service

Use the Distributed Job Service (DJS) to run jobs independently on multiple Job Service servers at the same time. You can configure a controller server that manages the distributed Job Service by distributing jobs to multiple machines.

Related Topics

Distributed Job Service Overview

The Distributed Job Service (DJS) is an extension of the Job Service that enables a controller machine to manage multiple machines (servers) running job services. Non-distributed job services run jobs on a single machine; installing the non-distributed job service on multiple machines results in each service running independently on each machine.

With distributed job services, each designated server runs jobs as requested by the controller via DCOM communication. This distributes the job service load across multiple machines. The controller can also run jobs.

Prepare the Controller and DJS Servers for Installation and Configuration

Be sure to complete the following before you install and configure DJS on the Controller and servers:

▸ On the Controller and all DJS servers, define the "Temp" and "TMP" variables in Environment variables (both User variables and System variables).

▸ Synchronize the system clocks of the Controller and all DJS servers to have identical time stamps in the log files.

Installing the Distributed Job Service

Before installing the Distributed Job Service, identify the Controller and servers (maximum 10). Install the Job Service on each machine as described in **Installing the Job Service and Distributed Job Service** (on page 86). When you finish the installation, return to this section to configure user access.

> **Note**: Oracle recommends that the controller and all related servers be in the same network domain. Also, each machine should have Windows Server 2003, Windows Server 2008, or Windows XP as the operating system, with Firewall turned off.

Disabling the Windows Firewall

The Windows Firewall, which is enabled by default on Windows 2003 Server and XP, prevents DCOM connections from functioning. You must disable the firewall on the controller and each DJS server.

To disable the Windows Firewall, perform the following steps:

1) From the Windows Control Panel, click Windows Firewall.
2) In the General tab of the Windows Firewall dialog, select Off. then click OK.

Configure Access to the Distributed Job Service

Before configuring DCOM and the DJS, you must create users that have privileges to launch the Job Service, access the registry and path information on the Controller, and access applications across the network.

On the server that controls the domain in which the Controller and DJS servers reside, perform the following steps:

1) Create a user group (for example, PrmAdmins).
2) For the Controller and each DJS server, add a user name to the user group you just created. For example,

   Name of Controller : ControllerUser

Name of Server1 (DCOM Server) : Server1User
Name of Server2 (DCOM Server) : Server2User
Name of Server3 (DCOM Server) : Server3User

3) On the Controller and each DJS server, add the group you created to the Local Administrator Group.

4) In the Security tab of the DCOM Configuration dialog, add the group you created to each Custom permission.

> **Note**: The example above illustrates a multi-user scenario. You can also configure single-user access. For example, you could create a single domain user (e.g., ControllerUser) and add that user to the Local Administrator group on the Controller and each DJS server. Then, when configuring DCOM, you could use the ControllerUser instead of the PrmAdmins user group shown above.

Configure DCOM for the Distributed Job Service

To configure DCOM for the Distributed Job Service on servers running Windows Server 2003, Windows Server 2008, or Windows XP Professional, perform the following steps for the Controller and each DJS server.

1) From the command line (or Start, Run utility), run **dcomcnfg**. The Component Services dialog is displayed.

2) In the **Component Services** dialog, expand the tree in the left panel by clicking **Component Services, Computers, My Computer, DCOM Config**.

3) Right click on the **{9E521861-5A76-11D5-98F4-00C0F680F1F}** entry in the right panel and select Properties.

4) In the **Properties** dialog, **General** tab, set the **Authentication Level** to **Connect**.

> **Note**: Make sure the Controller and all DJS servers are set to the same Authentication Level. You can set Connect as the Default Authentication Level in the Default Properties tab of the Distributed COM Configuration Properties dialog.

5) In the **Properties** dialog, **Location** tab, select the **Run application on this computer** option.

6) In the **Properties** dialog, **Security** tab, ensure that the **Customize** options are selected for all permission types.

7) In the **Properties** dialog, **Security** tab, click the **Edit** button associated with **Launch and Activation Permissions**.

8) In the **Launch Permission** dialog, Security tab, click **Add**.

9) In the **Select Users, Computers, or Groups** dialog, enter the user group name you created previously (for example, PrmAdmins). Click **OK**.

10) In the **Launch Permission** dialog, Security tab, select the user group you added (for example, PrmAdmins), and select **Allow for all permissions**. Click **OK**.

11) In the **Properties** dialog, **Security** tab, click the **Edit** button associated with **Access Permissions**.

12) In the **Access Permission** dialog, Security tab, click **Add**.

13) In the **Select Users, Computers, or Groups** dialog, enter the user group name you created previously (for example, PrmAdmins). Click **OK**.

14) In the **Access Permission** dialog, **Security** tab, select the user group you added (for example, PrmAdmins), and select **Allow for all permissions**. Then click **OK**.

15) In the **Properties** dialog, **Security** tab, click the **Edit** button associated with Configuration Permissions.

16) In the **Change Configuration Permission** dialog, **Security** tab, click **Add**.

17) In the **Select Users, Computers, or Groups** dialog, enter the user group name you created previously (for example, PrmAdmins). Click **OK**.

18) In the **Change Configuration Permission** dialog, **Security** tab, select the user group you added (for example, PrmAdmins), and ensure that permissions are set as shown in the following figure. Then click **OK**.

19) In the **Properties** dialog, **Identity** tab, select the **This User** option. Enter the Password for a user who has administrative privileges on the machine you are using.

20) Click **OK** to close the dialog.

21) On the **Controller**, launch the **Services Control Panel**.

22) In the **Services** dialog, double-click the **P6 Job Service (JSDB)** to open the Properties dialog.

23) In the **Properties** dialog, select **This Account** and enter the password of an administrative user on the Controller.

> **Note**: Steps 21 - 23 enable the DJS to use the name and password of the administrator you specified during DCOM configuration as the launching user for all servers.

24) Click **OK** to close the dialog.

Configure the Controller and DJS Servers

Configure the Controller and DJS servers using the Distributed Job Services Configuration tool. Follow the instructions to access the configuration tool and configure the Controller and DJS servers.

1) On the Controller, run the DistributedJobsAdmin.exe from the following file location: C:\Program Files\Oracle\Primavera P6\P6 Professional\

The Distributed Job Service Configuration dialog opens.

2) In the Distributed Job Service Configuration dialog, click Browse. Navigate to the C:\Program Files\Oracle\Primavera P6\P6 Professional\ folder and select PrmJobSv.exe.

3) In the Distributed Job Service Configuration dialog, click Add. For each server listed, select the equivalent
   PrmJobSv.exe.

> **Note**: If you have already used the configuration tool, all servers you previously configured appear in the list of servers.

4) Set the Status (Enabled/Disabled) for the Controller and each DJS server.

> **Note**: You can disable the DJS on any machine (e.g., if you want to execute jobs only on the servers and not on the Controller). However, a disabled machine may still run jobs if no enabled machine is available (e.g., due to network problems).

5) Click **Test** to verify that the DCOM configuration and PrmJob installation is working correctly on each machine.

6) Click Save Settings, Close.

7) Reboot the Controller and all DJS servers.

> **Note**: When the Controller restarts, its job scheduling actions are listed in the Event Viewer. Log files for all jobs are located in the appropriate folder of the Controller (not on the servers).

> **Note**: After you reboot the Controller and DJS servers, if you modify the DCOM settings you specified in Configure DCOM for the Distributed Job Service, you must reboot the machines on which you made the modifications.

Job Service Registry Settings

You can edit the registry settings that apply to the (Distributed) Job Service and the summarizer service (in both the Job Service and P6 Professional).

Edit (Distributed) Job Service registry settings

Type 'regedit' in the Start, Run utility to open the Registry Editor. In the Registry Editor, navigate to the following directory:

My Computer\HKEY_LOCAL_MACHINE\
SYSTEM\CurrentControlSet\Services\PrmJobSv\Parameters

The following table summarizes the Job Services registry settings.

[Job Service settings]

Setting Name and Description	Default	Valid Ranges/Values
EstablishDBConnectionRetryCount Number of times to try to connect to database on startup.	3	1-10

MaxNumRecurringJobs	4	1-(no maximum)
The maximum number of recurring (Project Management) jobs that can run simultaneously.		
DeleteRemoteLog	1 (true)	0 (false)
[test purposes only] If set to false, log file "Prm*.tmp" will not be deleted.		1 (true)

Edit registry settings for summarizer jobs

Type 'regedit' in the Start, Run utility to open the Registry Editor. In the Registry Editor, navigate to the following directory:

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Primavera.

You can add any of the following settings as D Words and modify the defaults to the recommended value.

> **Note**: The following settings apply to the Job Service and the P6 Professional. You would typically modify them to improve performance.

[Summarizer settings]		
Setting Name and Description	**Default**	**Valid Ranges/Values**
NumProjectsSummarizedAtATime Number of projects that can be summarized at the same time by the Job Service or the P6 Professional. To achieve the best possible performance, Oracle recommends that the value of this setting = 20.	1	1-xx
PreQuerySummarizablePct The percentage threshold that determines how the summarizer will analyze a project's need for summarization. If the value of the equation shown below is less than the threshold, each project is considered for summarization individually. If the value of the following equation is greater than the threshold, all projects to be considered for summarization are analyzed simultaneously. The equation that determines this behavior is: # of projects to be summarized / # of projects user can access*100.	50	0-100

MaxDurationToSummarize	-1	-

The maximum remaining duration or the maximum original duration, in hours, that an activity or activity assignment can have in order to be summarized. If an activity or activity assignment has a remaining duration greater than this threshold, it is ignored during summarization. To ensure that all activities are summarized, Oracle recommends that the value of this setting = 100000.

Note: The following settings are also available. However, you would not typically need to modify their values, unless you are performing tests.

[Summarizer settings]

Setting Name and Description	Default	Valid Ranges/Values
ResourceSummaries If true, resources are summarized. Applies to the Job Service and the P6 Professional.	1 (true)	0 (false) 1 (true)
EnterpriseCommit Controls how frequently to commit EPS summary records to the database, based on the number of rows of data that have been processed. Useful for improving performance when summarizing large jobs. No value commits the EPS summary records when processing is complete. If you assign a value, this value is applied to both the Job Service and P6 Professional.	1000 for the Job Service No value for P6 Professional	1-(no maximum)
PrmJobLogMemoryUsage If true, logs memory usage of PrmJob in megabytes. Applies only to the Job Service.	0 (false)	0 (false) 1 (true)

RetrySleep The time, in milliseconds, to wait between retry attempts when there is a connection failure. Applies only to the Job Service.	60000	-
MaxRetries The maximum number of retry attempts to make when there is a connection failure. Applies only to the Job Service.	10	-
DumpSettings Set to true to log all settings to a Job.txt file for the summarization job. Applies only to the Job Service.	0 (false)	0 (false) 1 (true)
PreLoadTASKSUMFINForEPS Preloads TASKSUMFIN records for all projects before summarizing the entire EPS. Set to false to use a "load on demand" approach that will conserve memory but will be much slower due to an increased number of SQL queries for TASKSUMFIN records. Applies to summarizing Financial Periods in the Job Service and P6 Professional. Does not affect the performance of summarization by Weeks or Months.	1 (true)	0 (false) 1 (true)
PreLoadTASKSUMFINForProject Preloads TASKSUMFIN records for each project before summarizing that project. Set to false to use a "load on demand" approach that will conserve memory but will be much slower due to an increased number of SQL queries for TASKSUMFIN records.	1 (true)	0 (false) 1 (true)

Applies to summarizing Financial Periods in the Job Service and P6 Professional. Does not affect the performance of summarization by Weeks or Months.

PreLoadTRSRCSUMFN	1 (true)	0 (false)
Preloads TRSRCSUMFN records for each project before summarizing any project. Also, during summarization of the entire EPS, it preloads all TRSRCSUMFN records for one resource or role at a time.		1 (true)

Set to false to use a "load on demand" approach that will conserve memory but will be much slower due to an increased number of SQL queries for TRSRCSUMFN records.

Applies to summarizing Financial Periods in the Job Service and P6 Professional. Does not affect the performance of summarization by Weeks or Months.

Unattended Setup for P6 Professional

This chapter provides instructions for performing unattended setup of P6 Professional. An unattended setup enables administrators to run setup in silent mode and ensures that each user receives the same configuration.

As an administrator, you have several options for installing P6 Professional on client machines using the unattended setup. For example, you can physically run the unattended setup on each machine, write scripts that will run the unattended setup on the client machines you specify, or provide these instructions to users with administrator privileges, who can run the unattended setup on his/her computer.

In This Section

Unattended Setup

An unattended setup allows an administrator to install P6 Professional on a client computer without having to answer the configuration prompts of the P6 Professional Setup wizard. All configuration details for the installation are specified in the command line. Unattended installations ensure that the client module is configured identically at setup.

To create an unattended setup, you format a command lines to silently launch setup.

The unattended setup can be run by an administrator on client computers by entering the appropriate command lines. The unattended setup will silently install P6 Professional according to the parameters you specify in the command line.

> **Note:** Unattended setup for P6 SDK or Job Service is not supported.

The following prerequisites, available in the Client_Applications folder of the P6 Professional physical media or download, must be installed on each client computer before running unattended setup:

- Microsoft .NET Framework 4.5
- Windows Installer 4.0
- JRE 1.6.0_24
- DHTML Editing Control in Windows (DHtmlEd.msi) for Vista and Windows 7

An administrator should push these prerequisites to client computers before running unattended setup.

Running Unattended Setup

To run unattended setup:

1) Copy the contents of the files in the Client_Applications folder to a local folder.

   Oracle recommends creating a new folder, such as 'Installer.' Do not include spaces in the folder name.

2) Open a command line by choosing **Start**, **Run**. Type **cmd** and click **OK**.

   > **Notes:**
   >
   > - Ensure you run the command line as Administrator when UAC is on for Vista or Windows 7.
   > - For Windows 64 bit users, run cmd from the SysWOW64 folder.

3) On the command line window, enter the location of the Installer folder. For example,
   `cd c:\Installer`

4) On the command line window, enter the following command:
   `setup /q`

   This runs setup silently and there is no indication of the installer running. This will install to the default location:

   ▸ 32-bit target machines, P6 Professional applications are installed in local drive\Program Files\Oracle\Primavera P6\P6 Professional.

   ▸ 64-bit target machines, P6 Professional applications are installed in local drive\Program Files (x86)\Oracle\Primavera P6\P6 Professional.

To specify a directory other than the default directory use the following command:

`setup.exe /q INSTALLDIR="<Programlocation>"`

To install with a log file use the following command:

`setup.exe /q/l "<LogfileLocation>" INSTALLDIR="<Programlocation>"`

`<Programlocation>` = The location where you want to install the application

`<LogfileLocation>` = The location where you want to save the logfile

Access documentation for for command line parameters by typing `msiexec /help`.

Creating Database Connections for Unattended Setup

The database connection should be set on one administrator computer. After configuring the database connection, push PrmBootStrap.xml from the administrator computer(host computer) with database configuration details to each target client computer.

1) Install P6 Professional R8.1 on one administrator computer (host computer).

2) Create the database connection on the host machine. Follow the instructions in Configuring the Database Connection for P6 Professional.

The default locations of PrmBootStrap.xml for the **host** computers are:

‣ **Windows XP:**
   \%USERPROFILE%\Local Settings\Application Data\Oracle\Primavera P6\P6 Professional

‣ **Windows Vista and 7:**
   \%LOCALAPPDATA%\Oracle\Primavera P6\P6 Professional

The default locations of of PrmBootStrap.xml for the **target** computers are:

‣ **Windows XP**:
   \%ALLUSERSPROFILE%\Application Data\Oracle\Primavera P6\P6 Professional

‣ **Windows Vista and 7:**
   \%PROGRAMDATA%\Oracle\Primavera P6\P6 Professional

Users and Security

In This Section

Security Concepts in P6 Professional

Each person who will be using any module of P6 Professional must be registered as a "user" with the appropriate module access. Additional security privileges determine each user's access to data.

To ensure security at various levels of data, there are two sets of security profiles:

▸ **Global profiles** Define a user's access to application-wide information and settings, such as the enterprise project structure (EPS), resources, roles, and cost accounts. Each user must be assigned a global profile.

▸ **Project profiles** Define a user's access to project-specific information. It is not required that each user be assigned a project profile; however, users cannot access projects unless they are assigned: a project profile, the global profile Admin Superuser, or as a resource assignment when they are a project owner.

You can create a set of profiles that limit access to global information and then assign the appropriate global profile to each user. Similarly, to limit privileges for each project, you assign the appropriate project profile to each user via an organizational breakdown structure (OBS) element. When you create the EPS for your company, you must identify an OBS element, or person responsible, for each node and project within the EPS. This OBS element assignment determines the user's rights to the EPS level (and all levels below it). You can further control access to specific project data by assigning a responsible OBS element to each work breakdown structure (WBS) element within a project. Additionally, you can control user access to activity data via activity editing restrictions in user interface views, and you can control user access to resource data by implementing resource security.

The following diagram illustrates the relationships between a user, the OBS, EPS, and WBS.
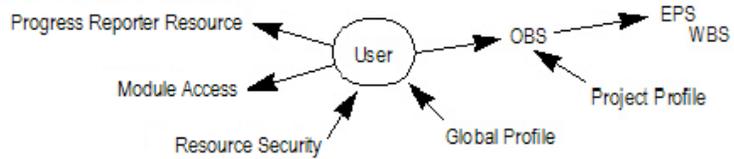
Security Samples

Review the following portions of a sample EPS for Capital Improvement projects in Oak County and its corresponding portion of the OBS.
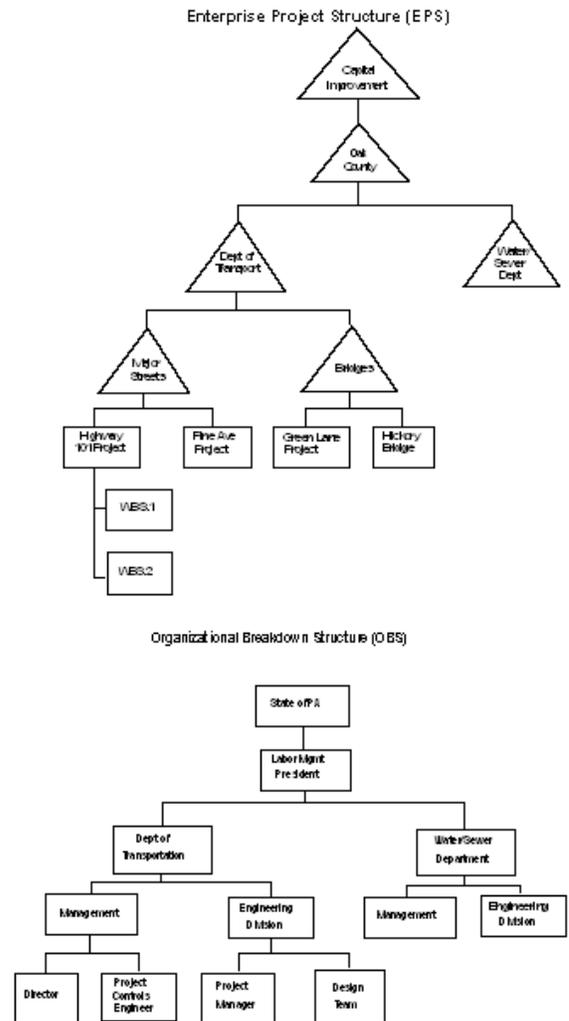
With these structures defined, you can map users to their corresponding roles in the OBS, which in turn can be assigned to each level in the EPS. The EPS level to which you assign the OBS determines the nodes/projects the associated user can access. For example, if you assign an OBS element to the root node of the EPS, the users associated with that OBS element can access the projects in the entire EPS. If you assign an OBS element to one branch of the EPS, the associated users can access only projects within that branch.

The project profile associated with each OBS element determines which data items in the projects the user can access. Only one OBS element can be assigned to each EPS level.

For example, suppose that two project profiles are defined: one that allows edit access to all data, including administration rights (Administrator profile), and one that allows viewing and editing of most, but not all, project data (Project Manager profile). Joe Nolan, the President of Labor Management, is assigned to the P6 Administrator profile. The OBS element, Labor Mgmt President, is assigned as the responsible manager at the Oak County node of the EPS, indicating that Joe Nolan has access to all nodes and projects within Oak County.

If Tim Ryan is the Director of the Department of Transportation (DOT), he can be assigned P6 Administrator rights to all projects under DOT.

OBS Assignments to the EPS
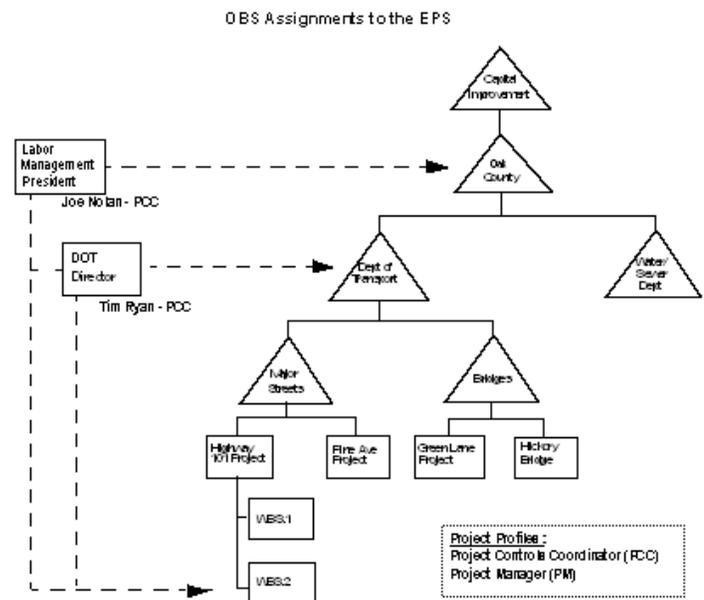
You can further control the access to projects by assigning OBS elements at the project and/or WBS level. In the previous example, if Marie Ross is the Project Manager in the Engineering Division responsible for the Highway 101 project, you can assign her to that OBS element with a Project Manager profile. She would then have editing access to just that project.

As another example, if the Design Team needs access to only the design portion of the Highway 101 Project. You can assign the Design Team to just the WBS branch in the Highway 101 project that involves the project design.

You can assign multiple users to the same OBS element and/or you can assign each user to multiple OBS elements. This flexibility enables you to provide access to the same EPS branch or project to more than one responsible manager (OBS element), and it allows you to control access by the same user across different EPS nodes and projects.

For example, suppose Marie Ross, who is a Project Manager in the Engineering Division responsible for the Highway 101 project, also needs access to the Pine Avenue project; however, you want to limit her access to reviewing and editing financial data only. Also suppose that Jim Harkey, another Project Manager in the Engineering Division, is responsible for the Pine Avenue project. He needs Project Manager access to the Pine Avenue project, but he also needs to review financial information in Marie's Highway 101 project.

You first would create another project profile that specifies viewing/editing rights to just project costs and financial data (Account Manager profile) and then make the following assignments:
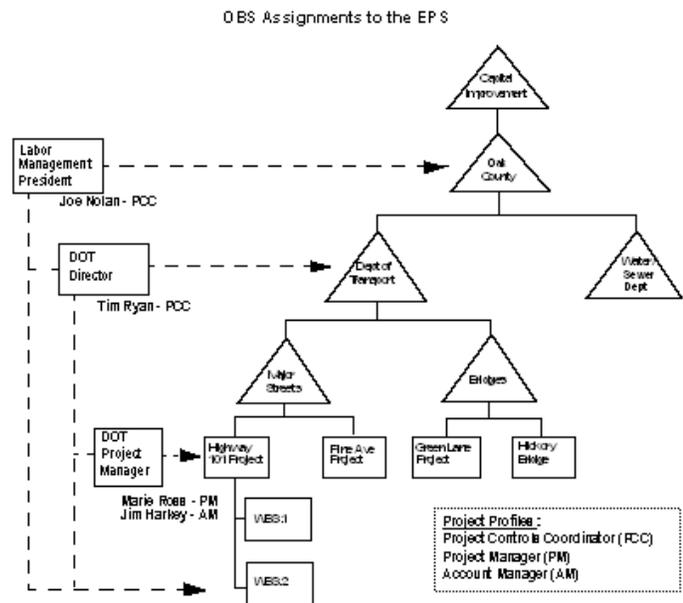
To designate that Jim Harkey has Project Manager rights to the Pine Avenue project and Marie Ross has Account Manager rights to the Pine Avenue project, you would need to add another element to the OBS.

OBS Assignments to the EPS
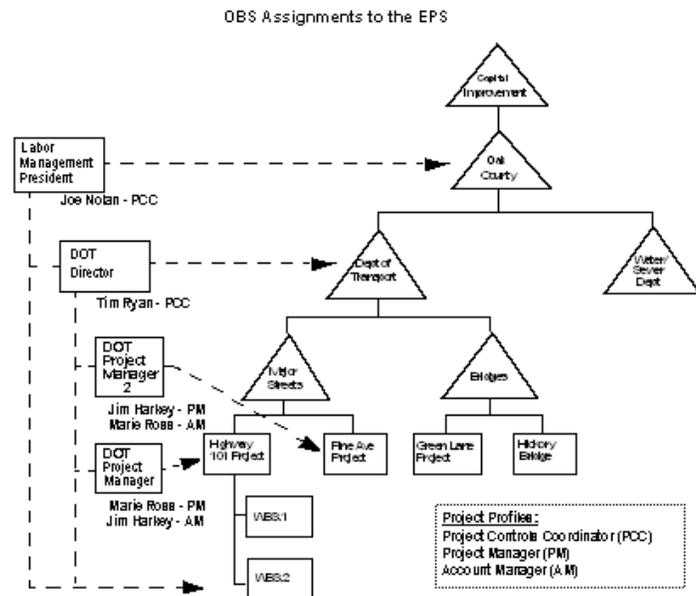
With these assignments, Jim Harkey and Marie Ross now have Project Manager rights to their primary projects and Account Manager rights to their secondary projects.

The following section provides guidelines for setting up users and administering security in P6 Professional.

Security Configuration Process in P6 Professional

Organization-wide project management involves a structured approach to managing several ongoing projects and teams across multiple locations at the same time. To ensure good results, up-front planning and coordination by various members of the organization are essential. Before you can use P6 Professional to manage your projects successfully, you must first administer users and set up structures, including the organizational breakdown structure (OBS), enterprise project structure (EPS), and resource hierarchy. Once users and structures are in place, you can implement security to restrict and/or provide access to project data.

The following bullets provide guidelines and a general process for administering users and security in P6 Professional. Because the structures are global across the company, some processes might require information from many participants. You can vary the order depending on your company's implementation plan. Also, some of these processes, such as defining resource security and user interface views, are optional depending on the needs of your organization.

‣ Create global and project security profiles in P6 Professional.

Define a standard set of profiles that determine access rights to global and project-specific data. Most likely, administrators perform this step.

▸ Add users in P6 Professional.

You must add each user who needs access to any P6 Professional module. At a minimum, each user is assigned a login name, module access, and a global profile.

▸ Set up the OBS for your company.

Identify your company's management structure and include the roles or names of those who will be responsible for the projects and work to be completed.

▸ After setting up the OBS, assign the appropriate users and project profiles to each element of the OBS.

▸ Set up the EPS for your company.

Identify your company's project structure, which is global across the organization.

▸ After setting up the EPS, assign the responsible manager (OBS) to each EPS node.

▸ Define the resources necessary to complete the projects across the organization.

▸ Define user access to resource data.

▸ Add projects to the EPS and define the WBS for each project.

Project managers usually perform this step. They can further control security within their own projects by assigning specific OBS elements to WBS levels.

▸ Set preferences for data in P6 Professional.

Useful P6 Professional Terms

Review the following P6 Professional terms to help you better understand how to administer users and security:

User Any person who needs access to P6 Professional.

Resource The people, materials, and/or equipment that perform the work on activities. You can build a resource hierarchy that includes the required resources across all projects in the organization. Resources are assigned to activities in P6 Professional.

OBS A global hierarchy that represents the managers responsible for the projects in your organization. The OBS usually reflects the management structure of your organization, from top-level personnel down through the various levels constituting your business. The OBS can be role-based or name-based.

EPS A hierarchy that represents the breakdown of projects in the organization. Nodes at the highest, or root, level might represent divisions within your company, project phases, site locations, or other major groupings that meet the needs of your organization, while projects always represent the lowest level of the hierarchy. Every project in the organization must be included in an EPS node.

WBS A hierarchical arrangement of the products and services produced during and by a project. In P6 Professional, the project is the highest level of the WBS, while an individual activity required to create a product or service is the lowest level. Each project in the EPS has its own WBS.

An OBS is not the same as a resource pool. While resources are assigned to activities, OBS elements are associated with EPS nodes and projects. The OBS element corresponding to an EPS node is the manager responsible for all work included in that branch of the hierarchy. In this way, an OBS supports larger projects that involve several project managers with different areas of responsibility.

Admin superuser

A global profile that gives a user read/write privileges for application-wide information and features. This information includes all projects, resources, cost accounts, and users. An Admin superuser always has access to all resources. If resource security is enabled, resource access settings will be ignored.

Defining the OBS

Organizational breakdown structure (OBS) overview

The organizational breakdown structure (OBS) is a global hierarchy that represents the managers responsible for the projects in your enterprise. The OBS usually reflects the management structure of your organization, from top-level personnel down through the various levels constituting your business. You can associate the responsible managers with their areas of the EPS (Enterprise Project Structure) — either nodes or individual projects. When you associate a responsible manager with an EPS node, any projects you add to that branch of the EPS are assigned that manager element by default.

The OBS hierarchy is also used to grant users specific access privileges to projects and the WBS (work breakdown structure) levels within projects.

Setting up the OBS

Because the OBS is maintained as a separate, global hierarchy, you have flexibility in making your OBS assignments as responsibilities change throughout a project life cycle.

You may want to create your OBS to match each EPS node and project set up in the EPS. You could initially match OBS names to the EPS node and project names. You could then assign users, by their login names, to the OBS elements to grant access to the corresponding EPS nodes or projects. The type of access granted to a user is determined by the project security profile assigned to the user. Security profiles are set up in the Security Profiles dialog box (choose Admin, Security Profiles) and then assigned to users in the Users dialog box (choose Admin, Users).

View the OBS

You can view an organizational breakdown structure (OBS) in two ways. You can use the OBS chart to view a graphical display of information, and you can use the OBS table to view information in a column format.

1) Choose Enterprise, OBS.

2) If the Organizational Breakdown Structure dialog box currently displays the Chart View, click the Display Options bar and choose Table View.

   To view the OBS hierarchy, click the OBS Name column label.

   To list and sort OBS elements, click the OBS Name column label again.

OBS security

Project profiles define a user's access to each project according to a specified OBS element. The specified OBS element determines which work breakdown structure (WBS) elements, activities, issues, and thresholds the user can edit in a project.

The OBS is a global hierarchy that represents the management responsible for the projects in your enterprise. The OBS hierarchy is used primarily to grant users specific access privileges to projects and to the WBS levels within projects. To access a project, a user must have access permissions for an OBS element within the project. This provides user access to WBS information for which the specified OBS element is responsible, as well as limits user access to WBS information that may lie beyond the user's scope.

Profiles and corresponding privileges are defined using the Security Profiles dialog box and are associated with the login name of the user. When you assign users to OBS elements using their login names, the security profile is automatically associated.

Note

▸ You can assign a user a security profile for any number of enterprise OBS nodes.

Add an OBS element

1) Choose Enterprise, OBS.

   A root OBS element is automatically assigned to the root EPS node so that a default OBS element can be assigned to each project you add to the EPS root.

2) Click the OBS Name column label to display the OBS hierarchy.

   The outline symbol ☰ in the OBS Name column label indicates a hierarchy display.

3) Select the OBS element immediately above and at the same hierarchy level as the element you want to add, then click Add.

4) Click the General tab, type the OBS Name, then click Modify to type a description of the OBS element in an HTML editor.

   In the editor, you can format text, insert pictures and tables, copy and paste information from other document files (while retaining formatting), and add hyperlinks.

5) Click the Users tab to view the users and corresponding security profiles associated with an OBS element. You can also assign users from this tab, if you have appropriate access rights.

6) Click the Responsibility tab to quickly see where responsible managers (OBS elements) are assigned across the enterprise. Select the OBS name for whom you want to see assignments.

Tip

▸ To change the element's position in the OBS hierarchy, click the appropriate arrow buttons.

Assign an OBS element to a WBS element

1) Choose Project, WBS.
2) Select the WBS element to which you want to assign an OBS element.
3) Click the General tab, then click ⊡ in the Responsible Manager field.
4) Select the OBS element you want to assign, then click the Select button.

Edit an OBS element

1) Choose Enterprise, OBS.
2) Click the OBS Name column label to display the OBS hierarchy.

   The outline symbol ⊟ in the OBS Name column label indicates a hierarchy display.

3) Select the OBS element you want to edit.
4) To change the element's information, click the General tab and enter new information.
5) To change the element's position in the OBS, click the appropriate arrow buttons.

Copy and paste an OBS element

1) Choose Enterprise, OBS.
2) Click the OBS Name column label to display the OBS hierarchy.
3) Select the OBS element you want to copy, then click Copy.

4) Select the OBS element to which you want to add the copied OBS element, then click Paste.

Cut and paste an OBS element

1) Choose Enterprise, OBS.
2) Click the OBS Name column label to display the OBS hierarchy.
3) Select the OBS element you want to cut and paste, then click Cut.
4) Select the OBS element to which you want to add the cut OBS element, then click Paste.

Delete an OBS element

1) Choose Enterprise, OBS.
2) Click the OBS Name column label to display the OBS hierarchy.
3) Select the OBS element you want to delete, then click Del/Merge.

   If the OBS element you want to delete has work breakdown structure (WBS), issue or threshold assignments, you are prompted to merge the element with its parent OBS.

4) Click Yes.

Note

▸ If you delete a parent OBS element, all of the elements contained in the parent element are deleted.

View the OBS chart display

Use the OBS chart to view a graphical display of OBS information.

▸ Choose Enterprise, OBS, then click the Display Options bar and choose Chart View.

Tip

▸ To view the OBS table display again, click the Display Options bar, then choose Table View.

Change the OBS chart display

1) Choose Enterprise, OBS, then click the Display Options bar and choose Chart Font and Colors.
2) To change the appearance of the display's text, click Font, then select a new font.
3) To change the display's background color, click Back Color, then select a new color.
4) To change the display's OBS box color, click Box Color, then select a new color.

Tip

▶ To change the displayed information, click the Display Options bar, choose Chart Box Template, then select Customize.

Move around the OBS chart

You can change the level of detail that appears onscreen.

▶ Click the Display Options bar and choose Zoom. You can zoom in, zoom out, or zoom to best fit.

Tip

▶ You can also use your mouse to control the level of detail that appears onscreen:

To Do This	
Zoom in	Hold down the Alt key, click the background, and then drag the pointer down while holding down the mouse button.
Zoom out	Hold down the Alt key, click the background, and then drag the pointer up while holding down the mouse button.

Change the OBS chart information

1) Choose Enterprise, OBS, then click the Display Options bar and choose Chart Box Template, Customize.
2) Click Add.
3) In the Field Name field, select a template element.
4) Specify a width and height for the template element.
5) Click the up and down arrows to place the element within the OBS box.

Tips

▶ To remove an element from the OBS box, select the element, then click Delete.
▶ To revert to the default OBS box fields, click Default.

Assign responsibility for an issue

1) Choose Project, Issues, then select the issue.
2) Display Issue Details, then click the General tab.
3) In the Responsible Manager field, click ⬚.
4) Select the name of the responsible OBS member, then click the Select button.

Assign responsibility for threshold-generated issues

1) Choose Project, Thresholds.
2) Select the threshold, then click the General tab.
3) In the Responsible Manager field, click ⬚.
4) Select the name of the OBS element, then click the Select button.

Setting up the EPS

Enterprise Project Structure overview

The Enterprise Project Structure (EPS) forms the hierarchical structure of your database of projects. Each EPS node (or folder) can be subdivided into multiple levels to represent the work that needs to be done in your organization. The number of levels and their structure depend on the scope of your projects and how you want to summarize data.

You can use the EPS to

▸ Perform top-down budgeting and resource and cost analysis
▸ Organize work breakdown and organizational breakdown structures into one common structure
▸ Manage multiple projects from the highest levels of the organization to the individuals that perform specific project tasks
▸ Implement coding standards for flexible reporting
▸ Maintain appropriate security throughout the enterprise

Defining the Enterprise Project Structure

All projects in the enterprise exist within the EPS hierarchy, a graphical representation of your project structure. A root node is automatically created for the hierarchy during installation.

The levels and structure of your company's EPS depends on the scope of your projects and how you want to summarize data. You can use the Admin Preferences, Data Limits tab to define one or multiple root nodes, up to 50 combined WBS/EPS levels and as many projects as necessary to complete the required work set forth by the operations executive and project managers in your organization.

Before you begin defining your company's EPS, you should become familiar with the structures and procedures established for your enterprise, such as codes, calendars, and other company-wide standards. Once the EPS hierarchy is defined, you can begin to develop projects by adding information, activities, and resources.

Set up the EPS structure

When you create the enterprise project structure, you must identify an OBS element, or person responsible for each node and project within the EPS. For steps on defining the OBS, see **Setting up the OBS** (on page 109).

1) Choose Enterprise, Enterprise Project Structure.
2) Click the EPS Name column where you want to add a new element.
3) Click Add.
4) Type an ID and name for the EPS node. In the Responsible Manager field, select an OBS element for the new element.
5) If necessary, you can change the hierarchical position of the new element by clicking the arrow keys.
6) Click Close.
7) Choose Enterprise, Projects then specify project details such as dates, resource and budget information, and so on.

Note

▸ A default root node displays in the top left position in the hierarchy. All projects listed below it are part of the same structure. You can also define multiple root nodes to separate various components of your enterprise. For example, you might want to exclude inactive or what-if projects from the main enterprise. To define a root node, click the left arrow key to move an EPS element to the top left position in the hierarchy, then add the hierarchy of projects below this node.

Add a project to the EPS hierarchy

Once you set up the EPS structure, you can add an unlimited number of projects as follows: See **Set up the EPS structure** (on page 115).

1) Choose Enterprise, Projects, then select the EPS node or root element to which you want to add a project.
2) Click ✚ on the Edit Toolbar or choose Edit, Add.
3) Follow the instructions in the Create a New Project Wizard.

   To quickly add a new project using the default settings, click Finish on the Create a New Project Wizard.

4) Use the detail tabs across the bottom of the Project window to add details specific to this project.

Delete an EPS node or project

1) Choose Enterprise, Projects, then select the EPS node or project that you want to delete. Choose Edit, Delete.
2) Click Yes to confirm.

Tip

▸ When you delete an EPS node, all projects in that branch of the hierarchy are also removed. To save projects in a branch before deleting it, first copy and paste those projects to another area of the hierarchy.

Copy an EPS node or project

1) Choose Enterprise, Projects, then select the EPS node or project you want to copy.
2) Choose Edit, Copy.
3) Click the location in the EPS where you want to paste the new EPS node/project.
4) Choose Edit, Paste.
5) Mark the checkboxes beside any optional information you want to include in the copied EPS node or project in the Copy Project Options, Copy WBS Options, and Copy Activity Options dialog boxes.

Notes:

▸ The administrator should not assign any of the following privileges to users who should not have access to view cost information while copying and pasting project/EPS or assigning WBS and Fill Down on the WBS column in the Activities view: View Project Costs/Financials, Edit WBS Costs/Financials, and Edit EPS Costs/Financials.

▸ You must group the projects (to copy) by EPS in order to copy Summary Data.

Tip

▸ When you select an EPS node to copy, all of the selected EPS node's subordinate EPS nodes/projects are also copied, even if you do not select them.

Managing User Security

Setting up user security

For each user, you perform the following steps to implement access to P6 Professional.

1) Choose Admin, Users.
2) Click Add to add a user.
3) On the General tab:
   ▸ Enter the user's login name and personal name.

▸ Click Password to enter the user's password. The minimum password requirements depend on the status of the password policy, and are described in the Change Password dialog box.

4) On the Global Access tab:

▸ Assign a global security profile to the user. Global security profiles determine the global actions the user can perform and are defined in the Security Profiles dialog box (choose Admin, Security Profiles).

▸ Enable or disable resource security for the user. To enable access to all resources, mark the All Resource Access checkbox (Admin Superusers automatically get All Resource Access). To restrict resource access to a specific resource node, select the resource node. To disable access to all resources, clear the All Resource Access checkbox (if necessary), and do not select a resource node.

5) On the Project Access tab, click Assign to assign the user to an OBS element (responsible manager), then select an existing project security profile.

This grants the user access to WBS elements (and associated activities) for which the assigned OBS element is responsible, in all projects. For the projects the user can access based on the user's OBS assignment, the project security profile determines the actions the user can perform for these projects.

6) On the Module Access tab, mark the checkbox for P6 Professional that you want to enable the user to access.

Notes

▸ Only an Admin Superuser can add, edit, delete, cut, copy, or paste Admin Superusers or change an Admin Superusers password.

▸ Only an Admin Superuser can apply the Admin Superuser profile to a user, and only an Admin Superuser can apply the Project Superuser profile to a user.

Module access

P6 Professional controls module access for P6 Professional.

For each defined user, a user with the required security privilege can enable or disable access to the product listed in the Users dialog box (choose Admin, Users, then click the Module Access tab). All users are guaranteed access to the product enabled for them.

Security profiles

Security profiles determine a user's level of access to project information. The security profiles include both global profiles and project profiles. A global profile determines the user's access to application-wide information. A project profile determines the user's level of access to each project within the Enterprise Project Structure (EPS). When you assign a project profile to a user, you also associate the project profile with an OBS element/responsible manager. The user's access privileges, as defined in the project profile, will then apply only to those elements of the EPS that are assigned to the OBS element/responsible manager you selected.

Global profiles

P6 Professional requires that all users have a global profile. A global profile defines a set of privileges for access to global, or application-wide, information such as cost accounts, resources, and roles. To control user access to global information, you create global profiles, and then assign specific profiles to individual users.

To allow complete access to all global information and all projects (assuming all applicable checkboxes are marked on the Users dialog box, Module Access tab), you can assign a global profile called **Admin superuser** (on page 109). You can assign the Admin Superuser profile to as many users as you like. However, since the Admin Superuser profile enables access to all information, you would typically restrict the number of users to whom you assign this profile. You cannot edit the Admin Superuser security profile.

Note: Only an Admin Superuser can apply the Admin Superuser profile to a user.

Global Privilege Definitions

A global profile definition specifies the individual access privileges associated with the profile. For a global profile, access privileges apply to application-wide information and settings. The module requires you to assign a global profile to each user.

Edit Global Change Definitions option

Determines whether the profile will enable users to create, modify, and remove Global Change specifications available to all users in P6 Professional.

Add/Edit/Delete Categories option

Determines whether the profile will enable users to create, modify and remove categories data as defined in the Admin Categories dialog box.

Delete Resources option

Determines whether the profile will enable users to remove resource data. This privilege also selects the 'Add Resources' and 'Edit Resources' global privileges.

Add Resources option

Determines whether the profile will enable users to create resource data. This privilege also selects the 'Edit Resources' global privilege.

Edit Resources option

Determines whether the profile will enable users to modify resource data. This privilege also enables users to assign, modify, and remove role assignments. To display resources' price/unit in reports, users must have this privilege and the 'View Resource and Role Costs/Financials' global privilege assigned to their profile. To display resource skill level (a resource's role proficiency) in the application and in reports, users must have this privilege and the 'View Resource Role Proficiency' global privilege assigned to their profile.

View Resource Role Proficiency option

Determines whether the profile will enable users to display, group/sort, filter, search, and report on resource and role proficiency. To display resource skill level (a resource's role proficiency), users must have this privilege and the Edit Resources global privilege assigned to their profile.

Add/Edit/Delete Cost Accounts option

Determines whether the profile will enable users to create, modify, and remove cost accounts data.

Import Project Management XER, MPP, MPX, and P3 option

Determines whether the profile will enable users to import projects, resources, and roles from XER, MPP, MPX, and P3 formats using P6 Professional. To create new projects when importing, users must also have the 'Create Project' project privilege assigned to their profile. Users must be an Admin or Project Superuser to update a project from XER or P3 formats.

Import XML option

Determines whether the profile will enable users to import projects from P6 Professional and Microsoft Project using XML format. To create new projects when importing, users must also have the 'Create Project' project privilege assigned to their profile.

Note: For Microsoft Project imports, you can only create a new project (not update an existing one) during import. Also, P6 Professional supports imports from Microsoft Project 2002.

Import XLS option

Determines whether the profile will enable users to import projects, resources, and roles from XLS files. Users must also be a Project Superuser to update a project from XLS format.

Add/Edit/Delete Global Reports option

Determines whether the profile will enable users to create, modify, and remove global reports, including editing report groups and global report batches and saving global reports created or modified in P6 Professional.

Edit Global Tracking Layouts option

Determines whether the profile will enable users to create, modify, and remove global tracking layouts in P6 Professional.

Add/Edit/Delete Roles option

Determines whether the profile will enable users to create, modify, and remove roles data.

Edit Global Activity Codes option

Determines whether the profile will enable users to modify global activity codes data. This privilege also enables users to create, modify, and remove global activity code values.

Add Global Activity Codes option

Determines whether the profile will enable users to create global activity codes and code values data. This privilege also selects the 'Edit Global Activity Codes' global privilege.

Delete Global Activity Codes option

Determines whether the profile will enable users to remove global activity codes and code values data. This privilege also selects the 'Add Global Activity Codes' and 'Edit Global Activity Codes' global privileges.

Add/Edit/Delete Global Calendars option

Determines whether the profile will enable users to create, modify, and remove global calendars data.

Add/Edit/Delete Resource Calendars option

Determines whether the profile will enable users to create, modify, and remove resource calendars data. This privilege also enables users to edit Shifts in P6 Professional.

Add/Edit/Delete Security Profiles option

Determines whether the profile will enable users to create, modify, and remove global and project security profiles, which grant access to application-wide and project-specific information.

Add/Edit/Delete Users option

Determines whether the profile will enable users to create, modify, and remove P6 Professional user data. To search the LDAP directory when provisioning, users must also have the Provision Users from LDAP global privilege.

Add/Edit/Delete Global Activity and Assignment Layouts and Filters option

Determines whether the profile will enable users to create, modify, and remove global activity and resource assignment layouts and filters.

Add/Edit/Delete OBS option

Determines whether the profile will enable users to create, modify, and remove hierarchical data for the global Organizational Breakdown Structure.

Edit Project Codes option

Determines whether the profile will enable users to modify project codes data. This privilege also enables users to create, modify, and remove project code values.

Add Project Codes option

Determines whether the profile will enable users to create project codes and code values data. This privilege also selects the 'Edit Project Codes' global privilege.

Delete Project Codes option

Determines whether the profile will enable users to remove project codes and code values data. This privilege also selects the 'Add Project Codes' and 'Edit Project Codes' global privileges.

Edit Resource Codes option

Determines whether the profile will enable users to modify resource codes data. This privilege also enables users to create, modify, and remove resource code values.

Add Resource Codes option

Determines whether the profile will enable users to create resource codes and code values data. This privilege also selects the 'Edit Resource Codes' global privilege.

Delete Resource Codes option

Determines whether the profile will enable users to remove resource codes and code values data. This privilege also selects the 'Add Resource Codes' and 'Edit Resource Codes' global privileges.

Add/Edit/Delete Global Portfolios option

Determines whether the profile will enable users to create, modify, and remove global portfolios.

Administer Global External Applications option

Determines whether the profile will enable users to create, modify, and remove entries in the list of global external applications in P6 Professional.

Add/Edit/Delete Funding Sources option

Determines whether the profile will enable users to create, modify, and remove funding source data.

View Resource and Role Costs/Financials option

Determines whether the profile will enable users to display all values for labor, material, and nonlabor resource costs, price/unit values for roles, and costs for resource and resource assignments User Defined fields. For users who do not have this privilege assigned to their profile, all areas that display monetary values for labor, material, and nonlabor resources and roles will display dashes and cannot be edited. For resources, such areas include resource price/unit, values in resource spreadsheets and histograms in Resource Analysis and Team Usage, and Cost data types for Resource User Defined fields. For roles, the area is the price/unit value in roles data. To display resources' price/unit, users must have this privilege and the 'Edit Resources' global privilege assigned to their profile.

Administer Job Services option

Determines whether the profile will enable users to set up the Apply Actuals, Batch Reports, Export, Schedule, and Summarize services to run at specific time intervals using the Job Service.

Add/Delete Secure Codes option

Determines whether the profile will enable users to create and remove all secure project codes, global and EPS-level activity codes, and resource codes and code values data, as well as all secure issue codes and code values data. This privilege also selects the 'Edit Secure Codes,' 'Assign Secure Codes,' and 'View Secure Codes' global privileges.

Edit Secure Codes option

Determines whether the profile will enable users to modify all secure project codes, global and EPS-level activity codes, and resource codes and code values data, as well as all secure issue codes and code values data. This privilege also selects the 'Assign Secure Codes' and 'View Secure Codes' global privileges.

Assign Secure Codes option

Determines whether the profile will enable users to assign all secure project codes, global and EPS-level activity codes, and resource codes and code values data, as well as all secure issue codes and code values data. This privilege also selects the 'View Secure Codes' global privilege.

View Secure Codes option

Determines whether the profile will enable users to display all secure project codes, global and EPS-level activity codes, and resource codes and code values data, as well as all secure issue codes and code values data.

Add/Edit/Delete Currencies option

Determines whether the profile will enable users to create, modify, and remove currencies data.

Add/Edit/Delete Categories option

Determines whether the profile will enable users to modify administrative categories as defined in the Admin Categories dialog box.

Edit Admin Preferences option

Determines whether the profile will enable users to modify administrative preferences as defined in the Admin Preferences dialog box.

Provision Users from LDAP

Determines whether the profile will enable users to search the LDAP directory when provisioning. For users who do not have this privilege assigned to their profile, the option to load an LDIF file to provision users will still be enabled. To search the LDAP directory, users also must also have the 'Add/Edit/Delete Users' global privilege.

View All Global/Project Data via SDK option

Determines whether the profile will enable users to view All Global and Project Data via P6 SDK. For Admin Superusers, access to the P6 SDK will be read/write. For all other users, access will be read only.

Add/Edit/Delete Resource Curves option

Determines whether the profile will enable users to create, modify, and remove resource distribution curves definitions.

Add/Edit/Delete User Defined fields option

Determines whether the profile will enable users to create, modify, and remove User Defined fields. Even without this privilege, users can still display User Defined fields information.

Add/Edit/Delete Global Project/WBS Layouts option

Determines whether the profile will enable users to create, modify, and remove global project and WBS layouts.

Add/Edit/Delete Microsoft Project Templates option

Determines whether the profile will enable users to create, modify, and remove Microsoft Project templates that are used to import/export data from/to Microsoft Project.

Add/Edit/Delete Activity Step Templates option

Determines whether the profile will enable users to create, modify, and remove Activity Step Templates, which are used to add a set of common steps to multiple activities.

Add/Edit/Delete Financial Period Dates option

Determines whether the profile will enable users to create, modify, and remove financial periods data. To edit period data, users must also have the 'Edit Period Performance' project privilege assigned to their profile.

Tips:

▶ P6 Professional includes a global profile called Admin Superuser. This profile automatically gives a user all of the preceding privileges for all projects and P6 Professional features (assuming all applicable checkboxes are marked on the Users dialog box, Module Access tab). To enable read/write privileges for all projects and features, you can apply the Admin Superuser profile to a user. See **Admin superuser** (on page 109).

▶ The previous table groups each privilege by functionality. The privileges are listed in the same order as displayed in the Security Profiles dialog box. To view the privileges in alphabetical order in the Security Profiles dialog box, click the Privileges bar.

Project profiles

A project profile defines a set of privileges for access to project-specific information. Project profiles are assigned to users based on the OBS hierarchy. To control access to project-specific information, you create project profiles, and then assign specific OBS elements and associated project profiles to individual users.   The assigned OBS element determines the EPS and WBS elements for which the user can access project information. The assigned project profile determines the type of access privileges the user has to that project information.

All WBS elements must have an assigned responsible OBS. If a user's project profile assignment includes a WBS element's responsible OBS, then the user can access all activities and issues related to that WBS element. Similarly, all thresholds and project issues also have an assigned responsible OBS. If a user's project profile assignment includes a threshold or issue's responsible OBS, then the user can access that threshold or issue.

The module does not require that each user have a profile for every project. However, unless a user's global profile is Admin Superuser, that user cannot access a project without a project profile. See **Admin superuser** (on page 109). To allow complete access to a project/OBS assignment, the module includes a project profile called Project Superuser. You can apply the Project Superuser profile to as many users and for as many projects as you like.

Note: Only an Admin Superuser can apply the Project Superuser profile to a user.

Project Privilege Definitions

A project profile definition identifies the specific access privileges that are granted by the profile. Each project profile is associated with an organizational breakdown structure (OBS) element to determine which EPS structure elements an individual user can access.

Add Projects option

Determines whether the profile will enable users to modify EPS budget logs, funding sources, and spending plans.

Delete Projects option

Determines whether the profile will enable users to delete, cut, and paste projects within the EPS node.

Summarize Projects option

Determines whether the profile will enable users to summarize data for all projects in the EPS.

Edit Project Details Except Costs/Financials option

Determines whether the profile will enable users to edit fields in General, Dates, Defaults, Resources, and Settings tabs in Project Details. To assign a project baselines, users must also have the "Assign Project Baselines" project privilege assigned to their profile.

Administer Project External Applications option

Determines whether the profile will enable users to modify entries in the External Applications feature in P6 Professional.

Schedule Projects option

Determines whether the profile will enable users to schedule a project.

Level Resources option

Determines whether the profile will enable users to level resources.

Apply Actuals option

Determines whether the profile will enable users to apply actuals to activities in a project.

Store Period Performance option

Determines whether the profile will enable users to track an actual this period value for actual units and costs in a project. A user must be assigned the Add/Edit Activities Except Relationships project privilege before you can assign this privilege.

Edit Period Performance option

Determines whether the profile will enable users to modify period performance values for labor and nonlabor units as well as labor, nonlabor, material, and expense costs using P6 Professional. The 'Add/Edit Activities Except Relationships' and 'View Project Costs/Financials' project privileges are also required for this functionality.

Maintain Project Baselines option

Determines whether the profile will enable users to create, modify, and remove baselines for projects.

Run Baseline Update option

Determines whether the profile will enable users to update a project's baselines with new project information using the Update Baseline utility.

Assign Project Baselines option

Determines whether the profile will enable users to assign project baselines to projects. To assign project baselines, users must also have the 'Edit Project Details Except Costs/Financials' project privilege assigned to their profile.

Add/Edit/Delete Work Products and Documents option

Determines whether the profile will enable users to create, modify, and remove a project's work products and documents.

View Project Costs/Financials option

Determines whether the profile will enable users to display all monetary values for projects. For users who do not have this privilege assigned to their profile, all areas that display monetary values will display dashes and cannot be edited. To use the Recalculate Assignment Costs feature, users must also have the 'Add/Edit Activities Except Relationships' project privilege assigned to their profile. To display the resource price/unit, users must have the 'View Resource and Role Costs/Financials' global privilege assigned to their profile.

Edit Project Activity Codes option

Determines whether the profile will enable users to modify project activity codes data. This privilege also enables users to create, modify, and remove project activity code values.

Add Project Activity Codes option

Determines whether the profile will enable users to create project activity codes and code values data. This privilege also selects the 'Edit Project Activity Codes' project privilege.

Delete Project Activity Codes option

Determines whether the profile will enable users to remove project activity codes and code values data. This privilege also selects the 'Add Project Activity Codes' and 'Edit Project Activity Codes' project privileges.

Edit EPS Activity Codes option

Determines whether the profile will enable users to modify the name of EPS-level activity codes. This privilege also enables users to create, modify, and remove EPS-level activity code values.

Add EPS Activity Codes option

Determines whether the profile will enable users to create EPS-level activity codes and code values. This privilege also selects the 'Edit EPS Activity Codes' project privilege.

Delete EPS Activity Codes option

Determines whether the profile will enable users to remove EPS-level activity codes and code values data. This privilege also selects the 'Add EPS Activity Codes' and 'Edit EPS Activity Codes' project privileges.

Monitor Project Thresholds option

Determines whether the profile will enable users to run the threshold monitor for a project.

Publish Project Web site option

Determines whether the profile will enable users to publish a project's Web site.

Edit Project Reports option

Determines whether the profile will enable users to edit a project's reports, edit a project's report batches, and export reports.

Add/Edit/Delete Project Calendars option

Determines whether the profile will enable users to create, modify, and remove calendars assigned to projects.

Run Global Change option

Determines whether the profile will enable users to run Global Change to update activity detail information.

Check In/Check Out Projects option

Determines whether the profile will enable users to check projects out to work remotely and then check them back in.

Import/View Contract Management Data option

Determines whether the profile will enable users to import and display data from Contract Management in P6 Professional.

Add/Edit/Delete WBS Except Costs/Financials option

Determines whether the profile will enable users to create, modify, and remove WBS hierarchy nodes, notebook entries, earned value settings, milestones (steps), work products and documents, and dates.

Edit WBS Costs/Financials option

Determines whether the profile will enable users to modify WBS budget logs, funding sources, spending plan, and financial data at the project level. This privilege also enables users to edit cost data at the activity level, including resource assignments. This privilege also selects the 'View Project Costs/Financials' project privilege.

Add/Edit/Delete EPS Except Costs/Financials option

Determines whether the profile will enable users to create, modify, and remove EPS hierarchy nodes, edit EPS notebook, and edit all EPS-related data except financial information.

Edit EPS Costs/Financials option

Determines whether the profile will enable users to modify EPS budget logs, funding sources, and spending plans.

Add/Edit/Delete Expenses option

Determines whether the profile will enable users to create, modify, and remove expenses assigned to projects.

Add/Edit/Delete Issues and Issue Thresholds option

Determines whether the profile will enable users to create, modify, and remove thresholds and issues assigned to projects. The privilege also enables users to assign issue codes to project issues.

Add/Edit/Delete Activity Relationships option

Determines whether the profile will enable users to create, modify, and remove activity relationships assigned to projects.

Add/Edit Activities Except Relationships option

Determines whether the profile will enable users to create and modify all activity information in projects, except activity relationships. To modify activity IDs, users must also have the 'Edit Activity ID' project privilege assigned to their profile. To use the Recalculate Assignment Costs feature, users must also have the 'View Project Costs/Financials' project privilege assigned to their profile.

Delete Activities option

Determines whether the profile will enable users to remove activities from projects.

Edit Contract Management Project Link option

Determines whether the profile will enable users to create, edit, and delete a link to a Contract Management project.

Edit Activity ID option

Determines whether the profile will enable users to modify activity IDs. To modify activity IDs, users must also have the 'Add/Edit Activities Except Relationships' project privilege assigned to their profile.

Edit Future Periods option

Determines whether the profile will enable users to enter, modify, and delete future period assignment values in the Planned Units and Remaining (Early) Units fields of the Resource Usage Spreadsheet using P6 Professional. The 'Add/Edit Activities Except Relationships' project privilege is also required for this functionality.

Add/Edit/Delete Project Level Layouts option

Determines whether the profile will enable users to create, edit, and delete project level layouts in Activities, Assignments, or WBS views.

Add/Edit/Delete Risks option

Determines whether the profile will enable users to assign risks to activities and to create, modify, and remove risks.

Tips:

▸ A project profile, Project Superuser, automatically gives a user all of the above privileges for each project, according to the specified OBS element.

▸ To allow read-write privileges for all aspects of a project, you can assign a user to a project's root OBS element and then apply the Project Superuser profile to the project/OBS assignment.

▸ The previous table groups each privilege by functionality. The privileges are listed in the same order as displayed in the Security Profiles dialog box. To view the privileges in alphabetical order in the Security Profiles dialog box, click the Privileges bar.

Note: To view resources' price/unit in reports, users must have "Edit Resources" and "View Resource and Role Costs/Financials" global privileges assigned to their profile.

Add new users

1) Choose Admin, Users.
2) Click Add.
3) What appears next depends on your security configuration:
   a. If P6 Professional is running in Native authentication mode, the Add User dialog box will appear:
      1. Fill in the Login Name, Personal name, Enter new password, and Confirm new password fields.

2. Click OK.

3. If the ability to edit a personal resource calendar is required, you can select an associated resource from the Resource ID / Resource Name for Personal Calendar field, or you can create the link when you add resources.

4. Click the Contact tab. Enter the user's e-mail address and office phone number.

5. Click Close.

   Notes:

   - Login names must be between 1 and 32 characters long. If the Enable Password Policy check box is cleared in the Admin Preferences dialog box, passwords must be between 1 and 20 characters long. If the Enable password policy check box is selected in the Admin Preferences dialog box, enter a password that is a minimum of 8 characters long, and that contains at least one alpha and one numeric character.

   - If P6 Professional is running in LDAP authentication mode, the Password button does not appear since password management is handled through the directory server.

   - Users you create will not have access to any projects or features until you assign them a security profile.

   - If a user is also a resource, the e-mail address and office phone number you type in the Users dialog box overwrites the e-mail address and office phone number recorded in the Resources window General tab, if that information is different. Likewise, e-mail and phone information you enter in the Resources window overwrites the information in the Users dialog box.

b. If P6 Professional is running in LDAP authentication mode, the Import Domain Users dialog box will appear:

   1. Either click the Load LDIF button, or enter an LDAP query (for example, UID=*) under LDAP User Search Criteria.

   2. If you clicked the Load LDIP button, browse to the location of the LDIF file, and click Open. If you entered an LDAP query, click Search.

   3. A list of users will appear, grouped by category. For example, LDAP repository users that do not exactly match P6 Professional users will be grouped together. If users exist in the LDAP repository, the Login Name, Personal Name, User EMail Address, and Office Phone fields are populated based on the field mappings in the LDAP configuration settings.

   4. Select the Import option next to each Login Name that you with to import. New or modified users are automatically selected.

   5. Click Import Users.

   6. Click Close in the Users dialog box.

Notes:

- You must have the Add/Edit/Delete Users privilege and the Provision Users from LDAP privilege to search the LDAP directory. You do not need the Provision Users from LDAP privilege to import users from the LDIF file.
- The new users will be assigned the default global profile.

Resource Security

Resource security allows the administrator to restrict a user's resource access. By default, new users do not have access to resources. To change the new user resource access click the Global Access tab. See **Introduction to Resource Security** (on page 136).

Notes

▸ Login names must be between 1 and 32 characters long. If the Enable Password Policy check box is cleared in the Admin Preferences dialog box, passwords must be between 1 and 20 characters long. Otherwise, they are required to be a minimum of 8 characters long, including at least one alpha and one numeric character.

▸ If P6 Professional is running in LDAP authentication mode, the Password button does not appear since password management is handled through the directory server.

▸ Users you create will not have access to any projects or features until you assign them a security profile.

▸ If a user is also a resource, the e-mail address and office phone number you type in the Users dialog box overwrites the e-mail address and office phone number recorded in the Resources window General tab, if that information is different. Likewise, e-mail and phone information you enter in the Resources window overwrites the information in the Users dialog box.

▸ Oracle recommends the use of strong passwords. Strong passwords in P6 Professional are defined as passwords containing between 8 to 20 characters and at least one numeric and one alpha character. To further strengthen the password, use a mixture of upper and lower case letters.

List number of users having access to P6 Professional

1) Choose Admin, Users.
2) Click Count.

The Count dialog box displays the number of users and the user name of each user assigned access to P6 Professional. Expand a module to display the user name of each user assigned access to a module.

3) If you want to print the displayed information, click Print. Otherwise, click Close.

Tip

▶ When you click Print, the table prints the same as it appears on the screen. So collapsed nodes are not expanded for printing, and expanded nodes print the entire list of users.

Change user security profiles

1) Choose Admin, Users.
2) Select the user whose security profiles you want to change.
3) To change a global profile, click the Global Access tab and select a new global profile.
4) To change a project profile, click the Project Access tab.

   To remove the user's current access to project information associated with a specific responsible manager, select the manager, then click Remove.

   To grant the user access to project information associated with a specific responsible manager, click Assign. Double-click the OBS element to which you want to grant access, then click Close.

   To change the user's security profile for a project, double-click the security profile you want to change, then select a new project profile.

Change user passwords

1) Depending on your global profile, you may be able to change a user's password or your own.
2) Choose Admin, Users.
3) Select the General tab.
4) Select the user who requires a change of password.
5) Click Password.
6) In the New Password field, enter the new password.
7) In the Confirm New Password field, enter the password again, to verify it.
8) Click OK.

Notes

▶ If the Enable password policy setting is selected in the Password Policy field of the Admin Preferences dialog box, enter a password that is a minimum of 8 characters long, and that contains one alpha and one numeric character.

▶ If the Enable password policy setting is not selected, enter a password up to 20 characters long.

‣ If P6 Professional is running in LDAP authentication mode, password management is handled through the directory server. You cannot change your password through the module and the   Password button does not appear on the Users dialog box General tab.

‣ If P6 Professional is running in LDAP authentication mode, password management is handled through the directory server. You cannot change your password through the module and the Password tab does not appear in the User Preferences dialog box.

‣ Passwords are case-sensitive.

‣ Passwords that were set before the new password policy was enabled are valid and usable.

Enable or disable user access to P6 Professional

1) Choose Admin, Users.
2) Select the user for whom you want to enable or disable module access, then click the Module Access tab.
3) In the Access column, mark or clear the checkbox for the module you want to enable or disable for the selected user.

Remove users

1) Choose Admin, Users.
2) Select the user you want to remove, then click Delete.
3) Click Yes.

Create global profiles

1) Choose Admin, Security Profiles.
2) Choose Global Profiles, then click Add.
3) Type the new profile's name.
4) To make the new profile the default global profile, mark the Default checkbox.
5) Mark the appropriate checkboxes to grant specific privileges to the profile.

Assign global profiles

1) Choose Admin, Users.
2) Select the user to whom you want to assign a global profile.
3) Click the Global Access tab, then select a global security profile.

Tips

▸ A global profile, Admin Superuser, allows complete access to global information, features, and all projects. See **Admin superuser** (on page 109). To grant the user read/write privileges for all projects and features, select Admin Superuser as the global profile. You can apply the Admin Superuser profile to as many users as you like.

▸ Only an Admin Superuser can apply the Admin Superuser profile to a user.

▸ To verify which privileges are associated with a particular global profile, open the Security Profiles dialog box (choose Admin, Security Profiles).

Change global profiles

1) Choose Admin, Security Profiles.
2) Choose Global Profiles.

To change a profile's name, double-click the profile, then type a new name.

To make a profile the default profile, mark its corresponding Default checkbox.

To change a profile's privileges, select the profile, then mark or clear the checkboxes to grant or deny each privilege.

Delete global profiles

1) Choose Admin, Security Profiles.
2) Choose Global Profiles.
3) Select the profile, then click Delete.
4) Click Yes.

Create project profiles

1) Choose Admin, Security Profiles.
2) Choose Project Profiles, then click Add.
3) Type the new profile's name.
4) To make the new profile the default project profile, mark the Default checkbox.
5) Mark the appropriate checkboxes to grant specific privileges to the profile.

Note

▸ Unless a user's global profile is Admin Superuser, a user cannot access any projects without a project profile. See **Admin superuser** (on page 109).

Assign project profiles

1) Choose Admin, Users.
2) Select the user to whom you want to assign a project profile, then click the Project Access tab.
3) Click Assign.
4) Double-click the OBS element/responsible manager whose project information you want to allow the user to access, then click Close.
5) Double-click the Security Profile field, then select a profile.
6) Repeat steps 3 through 5 for all projects to which you want the user to have access.

Tips

▸ A project profile, Project Superuser, allows complete access to a project/OBS assignment. To grant the user read/write privileges for all aspects of a project, select Project Superuser as the user's profile. Only an Admin Superuser can apply the Project Superuser profile to a user.

▸ To verify which privileges are associated with a particular project profile, open the Security Profiles dialog box (choose Admin, Security Profiles).

Note

▸ A user is not required to have a profile for every OBS element. However, unless a user's global profile is Admin Superuser, a user cannot access project information without a project profile. See **Admin superuser** (on page 109).

Change project profiles

1) Choose Admin, Security Profiles.
2) Choose Project Profiles.

To change a profile's name, double-click the profile, then type a new name.

To make a profile the default profile, mark the Default checkbox.

To change a profile's privileges, select the profile, then mark or clear the checkboxes to grant or deny each privilege.

Delete project profiles

1) Choose Admin, Security Profiles.
2) Choose Project Profiles.
3) Select the profile you want to delete, then click Delete.
4) Click Yes.

Managing Resource Security

Introduction to Resource Security

The administrator can restrict a user's access to resource information. The administrator can enable or disable resource security for each user. When resource security is disabled, the user has access to all resources. When resource security is enabled, the user has access to either none of the resources or a selected part of the resource hierarchy.

How does resource security work?

To enable resource security, the administrator assigns each user to a resource node in the resource hierarchy. This is the user's root node. Then, the position of the root node in the resource hierarchy determines the resources to which the user has access. Once assigned to a resource node, the user has access only to the root node and all of its children.

The administrator can give each user access to the following:

▸ All Resources
   The user has access to all resources with no restriction. This option disables resource security.
   For Admin superusers, resource security access settings are ignored; they are always granted All Resources access. See **Admin superuser** (on page 109).

▸ No Resources
   The user has no access to resources. This is the default resource access to new users. Also, if a resource is deleted from the resource hierarchy, users that previously had been assigned to the deleted resource automatically get no access to resources.
   If a user has no resources access, all global resource-related privileges are ignored.

▸ Resource node (Selected Resources)
   The user has access to the assigned resource node and its children. You can assign only one node to a user. Multiple resource nodes are not supported.

Notes

▸ You need Add/Edit/delete Users global privilege to manage resource security.

▸ In the Resource Assignments window you still have access to current project resources.

Example

The following examples illustrate how resource security applies to users assigned to different resource nodes:
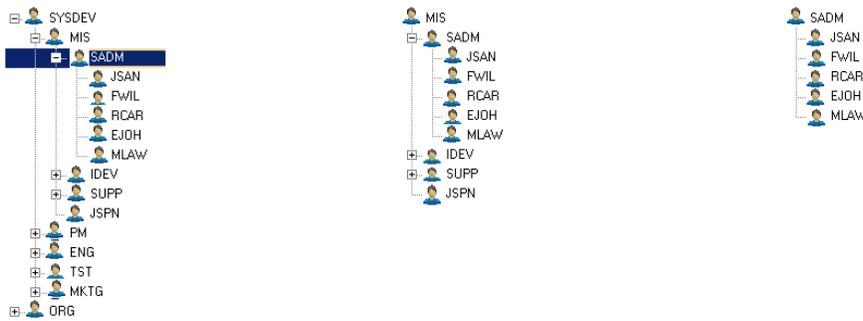
A) User has access to all resources. Resource security is disabled.

B) User is assigned to resource node MIS. This user has access only to root node MIS and its children.

C) User is assigned to resource node SADM. This user has access only to root node SADM and its children.

Implementing Resource Security

Before you implement resource security in your organization, you should know about the impact of restricting resource access in P6 Professional. Users with restricted resource access may experience the impact of the feature in the following major areas:

Resources View

If resource security is enabled, the Resources View's Filter By options display the following resources:

▸ All active resources
   Displays all active resources that you have access to in a hierarchy. Those current project resources that are outside of your resource root node are not displayed.

▸ All resources
   Displays all resources that you have access to in a hierarchy. Those current project resources that are outside of your resource root node are not displayed.

▸ Current Project's Resources
   Displays only those current project resources that you have access to. In other words, those current project resources, who are under your root resource node. (Resources that you do not have access to are not displayed even if they are current project resources.)

Resource Assignments View

In the Resource Assignments View you still have access to all current project resources even if they are not under your root node. If you have the proper privilege, you can modify their assignments or reassign any resource to new activities.

Importing and Exporting Resources/Projects

If you have no resource access, you cannot import new resources or activity resource assignments, or issues associated with new resources. If you have limited resource access, new resources are imported under your root node and you can update existing resources only if you have access to them.

Enable Resource Security

Resource security allows the administrator to restrict a user's resource information access by assigning the user to a resource node in the hierarchy. That resource node is the user's root node. Once assigned to that root node, the user has access only to that resource node and all of its children.

Resource security settings are honored the next time the user logs in. Thus, if you modify your own resource security settings, the changes will not take place until you exit the module and login again.

To enable resource security by assigning the user to a resource node:

1) Choose Admin, Users.
2) Click the Global Access tab.
3) Select a user from the list.

    The bottom of the Global Access tab displays the selected user's current resource access information.

4) To enable resource security, click the browse button in the Resource Access field, and assign a resource node to the current user.

    The current user gets access only to the selected resource and its children after the next login.

To enable resource security by giving the user no access to any resources:

1) Choose Admin, Users.
2) Click the Global Access tab.
3) Select a user from the list.

    The bottom of the Global Access tab displays the selected user's current resource access information.

4) To give the current user no access to resources:

    ‣ Clear the All Resources Access checkbox, if it is marked.

▸ Delete the Resource Access field, if it is not empty.

The current user gets no access to any resources after the next login. This is the default for new users.

Notes

▸ The All Resources Access option disables resource security and gives the user access to all resources.

▸ Admin Superuser always has All Resources access, regardless of the resource security access settings.

▸ If you have restricted or no resource access, you cannot give All Resource access. This option is enabled only for users with all resource access.

Disable Resource Security

Resource security allows the administrator to restrict a user's resource information access by assigning the user to a resource node in the hierarchy. See ***Introduction to Resource Security*** (on page 136). That resource node is the user's root node. Once assigned to that root node, the user has access only to that resource node and all of its children.

To disable resource security:

1) Choose Admin, Users.
2) Click the Global Access tab.
3) Select the user from the list.

The bottom of the Global Access tab displays the selected user's current resource access information.

4) Select All Resources.
   ▸ All Resources
   This option disables resource security for the selected user and gives access to all resources.

Note

▸ Admin Superuser always has All Resources access, regardless of the resource security access settings. See ***Admin superuser*** (on page 109).

Displaying Resource Access Information

The Global Access tab in the Users dialog displays the selected user's resource access settings. The same settings can be displayed as columns as well. To view resource access information, add the Resource Access and All Resources Access columns to display in the Users dialog box. These columns are not displayed by default.

▸ All Resources Access

The All Resource Access column displays a checkbox for each user. If the checkbox is marked, the user has access to all resources. This option disables resource security.

This column is available only for users with all resource access or Admin superusers.

▸ Resource Access

The Resource Access column displays the user's assigned node. The user has access to this resource node and all its children.

If the Resource Access column is empty and the All Resources Access checkbox is unmarked, the user has no access to any resources.

Change Resource Security

You can change each user's resource access in the Users dialog any time. The new settings apply when the user logs in.

To change resource security:

1) Choose Admin, Users.
2) Click the Global Access tab.
3) Select a user from the list.

   The bottom of the Global Access tab displays the selected user's current resource access information.

4) Change the user's resource access settings.

Note

▸ Since a user's resource access depends on the position of the assigned resource in the hierarchy, changing that position also means changing the user's resource access.

Application Settings and Global Data

In This Section

Defining Administrative Preferences

Administrative preferences

Your organization can define a series of application-wide parameters and values that apply to all projects. Your organization can use these settings to customize your project to meet specific project management requirements and standards. While all users can view these settings, a user must have special security privileges to edit them. There are two types of settings: Administrative Preferences and Administrative Categories.

Application administrators use the Admin Preferences dialog box to establish default settings. You can use this dialog box to check the defaults that have been defined.

Change the global code separator

The global code separator is the character that separates cost account and activity codes to indicate hierarchy levels. The global code separator is used to indicate work breakdown structure (WBS) hierarchy levels if you do not specify a code separator for a project.

1) Choose Admin, Admin Preferences.
2) Click the General tab, then type a new code separator character in the Code Separator section.

Set the week start day

You can specify the day on which the calendar week begins.

1) Choose Admin, Admin Preferences.
2) Click the General tab.
3) In the Starting Day of Week section, select the day on which you want the workweek to begin.

Note

▸ This setting applies to all global, project, and resource calendars.

Set a default activity duration

You can specify the default activity duration for new activities added in all projects.

1) Choose Admin, Admin Preferences.
2) Click the General tab.
3) In the Activity Duration section, type a default activity duration in minutes, hours, days, weeks, months, or years.

Note

▸ If you change the default activity duration setting, the new default applies only to activities added after the change; existing activities are not affected.

Define maximum hierarchy levels

1) Choose Admin, Admin Preferences.
2) Click the Data Limits tab.
3) Specify the number of hierarchy levels each hierarchy may have.

Note

▸ If you change maximum hierarchy level settings, your change only applies when you add new elements or edit existing elements.

Define maximum project activity codes

1) Choose Admin, Admin Preferences.
2) Click the Data Limits tab.
3) In the bottom section, specify the maximum number of activity codes per project.

Define maximum baselines

1) Choose Admin, Admin Preferences.
2) Click the Data Limits tab.
3) In the bottom section of the tab, specify the maximum number of baselines per project.

Define maximum ID lengths

1) Choose Admin, Admin Preferences.
2) Click the ID Lengths tab, then specify the number of characters each code may have. Valid values are 1-20.

Note

▸ If you change the maximum number of characters in a code length, your change only applies when you add new codes or edit existing codes.

Set default workhours

P6 Professional calculates and stores time unit values in hourly increments, but users can set preferences to display time units in other increments, such as days or weeks. The values specified for Hours per Time Period are used to convert hours to other time increments for display, and to convert all non-hourly time increments to hours for storage in the database. As an administrator, you can globally specify the conversion factors, or you can enable the Hours per Time Period settings defined for each calendar to control how units and durations are converted and stored.

1) Choose Admin, Admin Preferences.
2) Click the Time Periods tab.
3) If you want to globally specify conversion factors, in the Hours per Time Period section, type the default number of workhours you want to use for each time period.

   If you want to use the Hours per Time Period settings defined in each calendar as conversion factors, mark the "Use assigned calendar to specify the number of work hours for each time period" checkbox.

Set abbreviations for displaying time

1) Choose Admin, Admin Preferences.
2) Click the Time Periods tab.
3) In the Time Period Abbreviations section, type the abbreviations you want to use when displaying each timeperiod.

Define default earned value settings

1) Choose Admin, Admin Preferences.
2) Click the Earned Value tab.
3) In the Technique for Computing Performance Percent Complete section, select the default completion percentage method you want to use for computing earned-value percent complete when calculating an activity's earned value.
4) In the Technique for Computing ETC section, select the default method for computing earned value estimate-to-complete you want to use when calculating an activity's Estimate to Complete (ETC) value.

5) In the Earned Value Calculation section, choose how you want to calculate earned value. Choose to use the baseline's At Completion values and current dates, planned values with planned dates, or planned values with current dates when calculating earned value from a baseline.

The current dates options use the Start/Finish dates for an activity or resource assignment.

Tip

▸ For each project, earned value is calculated using the project baseline or each user's defined primary baseline, depending on a preference setting on the Settings tab of Project Details.

Set global summarization options

In addition to specifying summarization options per project (Project Details, Settings tab), if you have administrator rights, you can specify global summarization options for storing resource spreads at the activity and resource levels.

1) Choose Admin, Preferences.
2) Select the Options tab.
3) In the 'Select summarization periods' section, choose how you want to summarize and store resource data: By calendar, By financial period, or both.

If you choose to summarize and store resource data by calendar intervals, in the WBS Level field, choose the time interval, such as week or month, for storing summarized activity data. Then, in the Resource/Role Assignment Level field, choose the time interval, such as week or month, for storing summarized resource data.

If you choose to summarize and store resource data by financial period intervals, activity and resource data is stored in financial period intervals that correspond to the financial periods defined in the Financial Periods dictionary. Choosing this option enables P6 Professional to display all activity and resource data (including non-past period actual data) in financial period timescale intervals.

Tips:

▸ If you want all project data in the database to be summarized by financial period (including closed projects), you must create financial periods that span the date range of all projects in the database. For example, if the oldest project in your database has a project start date of October 1st, 2001, your financial periods should begin on or before that date.

▶ If you choose to summarize data by financial period, you must summarize closed projects at least once to store project data in financial period intervals. Doing so ensures that data will display accurately in profiles and spreadsheets when users choose to display data for all projects in a financial period timescale interval (rather than open projects only).

Notes:

▶ If you choose to summarize by both calendar and financial period intervals, the runtime of summarizer jobs will increase.

▶ If you summarize projects with the 'By calendar' option selected, then clear the checkbox and summarize projects again, the previously existing summary activity and resource spreads are not removed; you must remove them manually.

▶ If financial periods are not defined in the Financial Periods dictionary, you can select the 'By financial period' option but data will not be summarized by financial period.

Set the industry type

The industry type that you choose determines the terminology and default settings that display in P6 Professional.

An upgrade or a new installation of P6 Professional database leaves the industry type field blank and requires the system administrator to set it. So immediately after the installation, the administrator must use the Admin Preferences, Industry tab in P6 Professional to select an appropriate industry type.

Use the following steps to select the industry type.

1) Choose Admin, Admin Preferences.
2) Click the Industry tab.
3) Select the option that most closely aligns with your industry.

Notes

▶ If you set the industry type and later change it, the change will not take effect for users who have logged in since it was last set until you clear their USERDATA; the new industry setting is immediately effective for new users.

▶ The following table lists each industry type and its corresponding terminology and default settings:

Industry Type	Industry Terminology Examples	Default project comparison tool
Engineering and Construction	Budgeted Units Budgeted Cost	Claim Digger

	Original Duration	
Government, Aerospace, and Defense	Planned Units Planned Cost Planned Duration	Schedule Comparison
High-Technology, Manufacturing	Planned Units Planned Cost Planned Duration	Schedule Comparison
Utilities, Oil, and Gas	Budgeted Units Budgeted Cost Original Duration	Claim Digger
Other Industry	Planned Units Planned Cost Planned Duration	Schedule Comparison

Defining Administrative Categories

Administrative categories

Your organization can define a series of application-wide parameters and values that apply to all projects. Your organization can use these settings to customize your projects to meet specific project management requirements and standards. While all users can view these settings, a user must have the have Add/Edit/Delete Categories global privilege to edit them.

Use the Admin Categories dialog box to define standard categories and values you can apply across all projects, including custom categories and category values for projects, resources, and WBS elements.

Use the following tabs to establish the following default categories and values:

Baseline Types: Create, edit, and delete baseline types. Use these categories to standardize and categorize baselines, and to help benchmark performance across projects.

Expense Categories: Create, edit, and delete expense categories. Use these categories to standardize and categorize project expenses, and organize and maintain expense information.

WBS Category: Create a WBS category and create, edit, and delete WBS category values. Use this category to standardize and categorize WBS elements.

Document Categories: Create, edit, and delete categories for work products and documents. Use these categories to standardize and categorize work products and documents, and organize and maintain work product and document information.

Document Status: Create, edit, and delete document status types. Use these status types to identify the current status of work products and documents within a project.

Risk Categories: Create, edit, and delete risk categories. Use these categories to classify risk types and to organize risks.

Notebook Topics: Create, edit, and delete notebook topics. Use notebook topics to organize related notes about an activity.

Units of Measure: Add, delete, and organize units of measure.

Baseline Types

Create a baseline type

You can create baseline types that you can assign to baselines in any project. You can use baseline types to standardize baselines for all projects.

1) Choose Admin, Admin Categories.
2) Click the Baseline Types tab, then click Add.
3) Type the name of the new baseline type.

Edit a baseline type

1) Choose Admin, Admin Categories.
2) Click the Baseline Types tab.
3) Double-click the baseline type you want to change, then enter a new baseline type.

Tip

▸ To change the order in which baseline types are listed, select the baseline type you want to move, then click Shift Up or Shift Down.

Note

▸ If you change a baseline type, your change applies to all baseline assignments.

Delete a baseline type

1) Choose Admin, Admin Categories.
2) Click the Baseline Types tab.
3) Select the baseline type you want to delete, then click Delete.

4) Click Yes.

Expense Categories

Create expense categories

You can create expense categories that you can assign to expenses in any project. You can use these categories to organize and maintain your expense information.

1) Choose Admin, Admin Categories.
2) Click the Expense Categories tab, then click Add.
3) Type the name of the new expense category.

Rename expense categories

1) Choose Admin, Admin Categories.
2) Click the Expense Categories tab.
3) Double-click the category whose name you want to change, then type the expense category's new name.

Tip

▸ To change the order in which expense categories are listed, select the expense category you want to move, then click Shift Up or Shift Down.

Note

▸ If you change an expense category's name, your change applies to all expense item assignments.

Delete expense categories

1) Choose Admin, Admin Categories.
2) Click the Expense Categories tab.
3) Select the category you want to delete, then click Delete.
4) Click Yes.

WBS Category

Edit the WBS category

You can use a custom work breakdown structure (WBS) category to organize and maintain WBS information in all projects.

1) Choose Admin, Admin Categories.

2) Click the WBS Category tab, which displays the current name of the WBS category, for example Project Phase. Project phase is the default WBS category.

3) In the WBS Category field, type the new WBS category name. (This name will appear in the associated tab on the left side of this dialog box.)

Note

▶ The category's current values and value assignments do not change when you change the WBS category.

Create WBS category values

1) Choose Admin, Admin Categories.
2) Click the tab that displays the name of the current WBS category, then click Add.
3) Type the new value.
4) Use the Shift Up and Shift Down arrows to position the new value in the Category Value list.

Assign WBS Category values

You can assign a WBS category value from the Work Breakdown Structure window.

1) Display a column for the WBS category, if it is not already displayed.

Click the Display Options bar, choose Columns, and then choose Customize. In the Available Options section, under the General subsection, choose the WBS category. Click ▶ , then click OK.

2) In the WBS table, select the WBS element to which you want to assign a WBS category value, then double-click in the WBS category column.
3) Double-click the category value you want to assign.

Change WBS category values

1) Choose Admin, Admin Categories.
2) Click the tab that displays the name of the current WBS category.
3) Double-click the value you want to change, then type the new value.

Note

▶ If you change a category value, your change applies to all WBS assignments.

Delete WBS category values

1) Choose Admin, Admin Categories.
2) Click the tab that displays the name of the current WBS category.

3) Select the value you want to delete, then click Delete.

4) Click Yes.

Document Categories

Create document categories

You can set up categories to assign to work products and documents.

1) Choose Admin, Admin Categories.

2) Click the Document Categories tab, then click Add.

3) Type the name of the new document category.

Tip

▸ To change the order in which document categories are listed, select the document category you want to move, then click Shift Up or Shift Down.

Rename document categories

1) Choose Admin, Admin Categories.

2) Click the Document Categories tab.

3) Double-click the category whose name you want to change, then type the document category's new name.

Tip

▸ To change the order in which document categories are listed, select the document category you want to move, then click Shift Up or Shift Down.

Note

▸ If you change a document category's name, your change applies to all document item assignments.

Delete document categories

1) Choose Admin, Admin Categories.

2) Click the Document Categories tab.

3) Select the category you want to delete, then click Delete.

4) Click Yes.

Document Statuses

Create a document status

You can create status types that you can assign to documents in any project. A document's status helps you determine which documents are approved work products and documents, standards, and deliverables, and if they can be assigned to activities or work breakdown structure elements.

1) Choose Admin, Admin Categories.
2) Click the Document Status tab, then click Add.
3) Type the name of the new status.

Tip

▸ To change the order in which document statuses are listed, select the document status you want to move, then click Shift Up or Shift Down.

Change document status names

1) Choose Admin, Admin Categories.
2) Click the Document Status tab.
3) Double-click the status whose name you want to change, then type the new name.

Tip

▸ To change the order in which document statuses are listed, select the document status you want to move, then click Shift Up or Shift Down.

Note

▸ If you change the name of a document status, your change applies to all document assignments.

Delete a document status

1) Choose Admin, Admin Categories.
2) Click the Document Status tab.
3) Select the status you want to delete, then click Delete.
4) Click Yes.

Risk Categories

Create risk categories

You can create hierarchical risk categories of possible risks that you can assign to risks in any project. Risk categories are a classification of risk types customized to your specific project or business that are used to categorize and organize risks. Categorizing risks enables you to analyze the types of risks occurring and see trends within the project or across multiple projects.

1) Choose Admin, Admin Categories.
2) Click the Risk Categories tab, then click Add.
3) Type the name of the new risk category.

Tip

▸ To change the hierarchical order in which risk categories are listed, select the risk category you want to move, then click Shift up, Shift down, Shift Right, or Shift Left, as applicable.

Edit risk categories

1) Choose Admin, Admin Categories.
2) Click the Risk Categories tab.
3) Double-click the category you want to change, then enter the new risk category name.

Tip

▸ To change the hierarchical order in which risk categories are listed, select the risk category you want to move, then click Shift up, Shift down, Shift Right, or Shift Left, as applicable.

Note

▸ If you change a risk category, your change applies to all risk assignments.

Delete risk categories

1) Choose Admin, Admin Categories.
2) Click the Risk Categories tab.
3) Select the risk category you want to delete, then click Delete.
4) Click Yes.

> **Note**: Deleting a risk category deletes all children and their assignments.

Notebook Topics

Create notebooks

Use notebooks to set up general categories for activity, project, EPS, and WBS notes. You can assign notebooks in any project.

1) Choose Admin, Admin Categories.
2) Click the Notebook Topics tab, then click Add.
3) Type the name of the new notebook.
4) Mark the checkbox in the appropriate column to make the new notebook available in EPS, Project, WBS, or Activity views.

Tip

▸ To change the order in which notebook topics are listed, select the notebook topic you want to move, then click Shift Up or Shift Down.

Change notebook names

1) Choose Admin, Admin Categories.
2) Click the Notebook Topics tab.
3) Double-click the notebook whose name you want to change, then enter the notebook's new name.

Tip

▸ To change the order in which notebook topics are listed, select the notebook topic you want to move, then click Shift Up or Shift Down.

Note

▸ If you change a notebook's name, your change applies to all assignments.

Delete notebooks

1) Choose Admin, Admin Categories.
2) Click the Notebook Topics tab.
3) Select the notebook topic you want to delete, then click Delete.
4) Click Yes.

Units of Measure

Define the units of measure for material resources

A unit of measure describes the quantity of a particular resource. Labor resources are often measured in units of time, such as hours or days; materials can be measured in cubic or linear feet, or perhaps in tons or kilos; items used one-by-one can be measured individually (EA) or as shipped: a box, a case, a pallet. Money is generally measured in monetary units, such as dollars, euros, or yen.

1) Choose Admin, Admin Categories.
2) In the Units of Measure tab, click Add.
3) In the Unit Abbreviation column, type the abbreviation to use as the label for the new unit of measure.
4) In the Unit Name column, type the name of the new unit of measure.

Delete Units of Measure

You can delete any available unit of measure.

1) Choose Admin, Admin Categories.
2) Select the Units of Measure tab, then select a Unit Abbreviation or Unit Name.
3) Click Delete.

Note

▸ If the units of measure you attempt to delete is in use, a message will prompt you that the unit of measure is still in use. Click Yes to continue deleting. The unit of measure is deleted from the resource, but the resource remains.

Defining Currencies

Currencies

You can specify the monetary unit or base currency used to store costs for all projects in the database, as well as the monetary unit or view currency used to display costs in windows and dialog boxes.

The exchange rate for the base currency is always 1.0. If you select a different currency than the base currency to view costs, the base currency value is multiplied times the current exchange rate for the view currency to calculate the values displayed in cost fields.

For example, if the base currency is U.S. Dollars, the view currency is Euros, and the exchange rate for Euros is .75, a value of $10 stored in the database is displayed as 7.5 Euros in cost fields in windows and dialog boxes. Similarly, if you enter 7.5 Euros in a cost field, it is stored in the database as $10.

Notes

▸ Only a user with Admin Superuser privileges can change the base currency and define additional view currency types.

▸ When you enter values in cost fields, they are always displayed in the view currency.

▸ If you are upgrading from a previous version, you should set up the base currency in the new version before you start adding and changing projects.

Add a view currency

1) Choose Admin, Currencies.
2) Click Add.
3) Click the General tab, then type an ID that clearly identifies the currency type.
4) Type the currency's name.
5) Enter the symbol used to identify the currency.
6) Enter the global exchange rate for the currency.
7) Click the Appearance tab, then select the symbol used to separate whole values from decimal values in the currency display, for example, 500.5 or 500,5.
8) Select the symbol used to separate groups of digits in the currency display, for example, 300,000 or 300-000.
9) Select the number of decimal places to display in currency values, for example, none (70), one (70.1), or two (70.14).
10) Select the format used to display positive and negative currency values.

Define a base currency

The base currency, by default, is U.S. dollars.

1) Choose Admin, Currencies.
2) Select the current base currency, then click the General tab.
3) Type the new ID, name, and symbol over the existing values, to define the new base currency.
4) Click the Appearance tab.
5) Select the symbol used to separate whole values from decimal values in the currency display, for example, 500.5 or 500,5.
6) Select the symbol used to separate groups of digits in the currency display, for example, 300,000 or 300-000.

7) Select the number of decimal places to display in currency values, for example, none (70), one (70.1), or two (70.14).

8) Select the format used to display positive and negative currency values.

Tip

▸ If you want to view costs in the old base currency, you will need to add it back to the list of available currencies.

Note

▸ The Base checkbox indicates which currency is used to store cost data. You cannot mark or clear this checkbox.

Setting User Preferences

Define user preferences

1) Choose Edit, User Preferences.

2) Click the Time Units tab and define how to display time information.

3) Click the Dates tab and specify a format for dates.

4) Click the Currency tab and select a view currency. Also, specify how to format currency data.

5) Click the E-Mail tab and enter your e-mail settings.

6) Click the Assistance tab and specify which wizards to use.

7) Click the Application tab and set your startup options. You can also select how you want labels on grouping bands to display and define the range of financial periods that are available for display as columns. In addition, you can set the time interval that P6 Professional polls the database for job alerts, which are created every time a job you submit completes or fails.

8) Click the Password tab and modify your password.

   If P6 Professional is running in LDAP authentication mode, password management is handled through the directory server. You cannot change your password through the module and the Password tab does not appear in the User Preferences dialog box.

9) Click the Resource Analysis tab. Define the parameters for viewing all project data in the Resource Usage profile and how to display and calculate time-distributed data.

10) Click the Calculations tab and choose how you want the units, duration, and units/time calculated when adding or removing multiple resource assignments on activities. You can also choose to always use a resource's or role's units/time, overtime factor, and price/unit when a resource and role share an assignment on the same activity.

11) For Oracle or SQL Server installations, click the Startup Filters tab and choose to display current project data or all data in the enterprise.

Define how to display time information

You can specify how to display time information, such as time units, activity durations, resource rates, and resource availability.

1) Choose Edit, User Preferences.
2) Click the Time Units tab.
3) In the Units Format section, select the unit of time you want to display for work efforts, and resource prices and availability.

   Mark the Sub-unit checkbox to display sub-units in the next smaller time increment.

   Select the number of decimal places to display for time unit values.

   Mark the Show Unit Label checkbox to display the time unit abbreviation with the time value.

   Type an example of the time unit.

4) In the Durations Format section, select the unit of time you want to display for activity duration values.

   Mark the Sub-unit checkbox to display sub-units in the next smaller time increment.

   Select the number of decimal places to display for activity duration values.

   Mark the Show Duration Label checkbox to display the time unit abbreviation with the duration value.

   Type an example of the duration value.

5) Choose how to display resource units per time, either as a percentage or as units per duration.

Tip

▸ If you manually plan future period resource/role allocation in the Resource Usage Spreadsheet, you should set the Units Format and Durations Format according to the timeperiods in which you plan your work. For example, if you plan future work in daily timeperiods, you should set the Units Format to Hour and the Durations Format to Day. Similarly, if you plan future work in weekly timeperiods, you should set the Units Format to Hour or Day, and the Durations Format to Week.

Specify a format for dates

1) Choose Edit, User Preferences.
2) Click the Dates tab.
3) In the Date Format section, select the order in which you want all dates to appear.
4) In the Time section, specify how or whether you want to display time.
5) In the Options section, select the date formatting options you want to apply.

Specify a format for currency

1) Choose Edit, User Preferences.
2) Click the Currency tab.
3) Mark the Show Currency Symbol checkbox to display the currency symbol before currency values.
4) Mark the Show Decimal Digits checkbox to display decimals for currency values.

Select a view currency

1) Choose Edit, User Preferences.
2) Click the Currency tab.
3) Select the currency in which to view cost data.
4) Indicate whether to show the currency symbol and decimal digits for the selected currency.

Enter e-mail settings

You can access your e-mail account to send e-mail messages.

1) Choose Edit, User Preferences.
2) Click the E-Mail tab.
3) Select the mail protocol for your e-mail system.
4) Type the profile name, login, or username you use to access your e-mail server.
5) Click Password, then type your password for the e-mail server.
6) Type the SMTP server name or address to use to send outgoing e-mail.
7) Type the e-mail address to which you want your return e-mail sent.

   If you do not enter a return e-mail address, all e-mail is returned to the address you used to send the e-mail.

Set wizard options

You can specify whether you want wizards to help you add activities and resources.

1) Choose Edit, User Preferences.
2) Click the Assistance tab.
3) To use the New Resource wizard, mark the Use New Resource Wizard checkbox.
4) To use the New Activity wizard, mark the Use New Activity Wizard checkbox.

Change my password

1) Choose Edit, User Preferences.
2) Click the Password tab.
3) Click Password.
4) Type a new password.
5) Type the password again to verify it.
6) Click OK.

Notes

‣ If the Enable password policy setting is selected in the Password Policy field of the Admin Preferences dialog box, you must enter a password that is between 8 and 20 characters and contains at least one number and one letter.

‣ If the Enable password policy setting is not selected, enter a password between 1 and 20 characters long.

‣ If P6 Professional is running in LDAP authentication mode, password management is handled through the directory server. You cannot change your password through the module and the Password tab does not appear in the User Preferences dialog box.

‣ Passwords are case-sensitive.

‣ Passwords that were set before the new password policy was enabled are valid and usable.

‣ Passwords are required.

Set startup options

You can specify the window you want to display each time you start the application.

1) Choose Edit, User Preferences.
2) Click the Application tab.
3) In the Startup Window section, select the window to display each time you start the module.
4) Mark the Show the Issue Navigator Dialog at Startup checkbox to view the Issue Navigator each time you open the module.
5) Mark the Show the Welcome Dialog at Startup checkbox to view the Welcome dialog box each time you open the module.

Create a log of tasks

You can record internal function calls, or the actions you perform, in an ERRORS.LOG file. This file is created in the user's My Documents folder.

1) Choose Edit, User Preferences.
2) Click the Application tab.
3) In the Application Log File section, mark the Write Trace of Internal Functions to Log File checkbox.

Note

▸ You should use this option only when investigating an application error with the assistance of Oracle Customer Support staff.

Define the range of financial periods to display in columns

If your organization stores past period actuals in financial periods, you must define the range of financial periods you want to display when you choose to display financial period columns (for example, in the Activity Table). For example, if your organization stores past period actuals in weekly financial periods and financial periods have been defined for the previous year and the next year, you can choose to display a subset of these weekly financial periods as columns to facilitate easier viewing of past period actual data.

To define the range of financial periods:

1) Choose Edit, User Preferences.
2) Select the Application tab.
3) In the Columns section, click ... to select the financial periods that represent the first and last financial period in the range of financial periods you want to display as columns.
4) Click Close.

Note:

▸ If you do not select a range of financial periods to display, no financial period columns will be available for display.

Set resource analysis options

1) Choose Edit, User Preferences.
2) Click the Resource Analysis tab.

3) In the All Projects section, specify the extent of information you want to gather from closed projects when calculating remaining units and costs for spreadsheet, profiles, and tracking layouts. (Closed projects are any projects in the enterprise project structure (EPS) that are not currently open.)

To include live data from all open projects and stored summary data from all closed projects (excluding those with a what-if status), choose All Closed Projects (Except What-If Projects).

To include live data from all open projects and stored summary data from all closed projects with a specific leveling priority, choose Closed All Projects with Leveling Priority Equal/Higher Than, then specify the leveling priority you want to use. (Specify the leveling priority per project in the General tab of the Projects window.) This value is used to consider applicable external projects' (those not included in the current layout) when deducting from resource availability immediately during leveling.

Choose Open Projects Only to exclude resource data from external (closed) projects in the remaining units and cost values for resource profiles/spreadsheets and tracking layouts.

4) In the Time-Distributed Data section, choose a starting point for calculating remaining units and costs for resource profiles and spreadsheet displays and in tracking layouts.

To focus on the current remaining estimate, choose Remaining Early Dates.

To focus on values calculated from a forecast date, choose Forecast Dates.

Select the interval at which live resource and cost calculations are performed for resource profiles and spreadsheets and in tracking layouts—hour, day, week, or month. Profiles, spreadsheets, and layouts are affected only if their timescale interval is set lower than the interval set in the Interval for Time-Distributed Resource Calculations field.

Choose to display role limits based on custom role limits defined in the Roles dictionary or the calculated limit of each role's primary resource. You can view role limits in spreadsheets, charts, and histograms that display role data in P6 Professional.

Tip

▸ If you manually plan future period resource/role allocation in the Resource Usage Spreadsheet, your selections in the Time-Distributed Data section may affect your planning.

How? If you choose to display time-distributed Remaining Early units and costs according to forecast dates rather than remaining early dates, you can not enter or edit values in the Remaining Units field in the Resource Usage Spreadsheet.

Additionally, if the displayed timescale intervals in the Resource Usage Spreadsheet are smaller than the minimum timescale interval used for time-distributed resource calculations, you can not enter or edit future period values in the Resource Usage Spreadsheet. For example, if this option is set to Week, you can only enter or edit data in weekly, monthly, quarterly, yearly, or financial period future period buckets.

Select Startup Filters

1) Choose Edit, User Preferences.
2) Click the Startup Filters tab.
3) Select the appropriate option for each data element listed. You can choose to view data for your current projects only or all data in the enterprise.

Note:

▸ Startup filters are available for Oracle and SQL Server installations. Startup filters are disabled for stand-alone installations.

Select calculation options for resource and role assignments

1) Choose Edit, User Preferences.
2) Click the Calculations tab.
3) In the Resource Assignments section, specify how to calculate remaining values when new resource assignments are added to or removed from activities.

   Choose Preserve the Units, Duration, and Units/Time for existing assignments if you want units, durations, and units/time to remain constant when additional resources are assigned to an activity.

   Choose Recalculate the Units, Duration, and Units/Time for existing assignments based on the activity Duration Type if you want to calculate a resource assignment's remaining values based on the activity's duration type specified in the Activity Details General tab.

4) In the Assignment Staffing section, specify how you want the module to calculate costs for an assignment when you replace a resource on an existing activity assignment or when you assign both a resource and a role to the same activity assignment.

When replacing a resource on an existing activity assignment, choose to always use the units/time and overtime factor of the current assignment or of the new resource replacing the existing assignment; or, choose to be prompted to select which units/time and overtime factor you want to use each time you replace a resource on an existing activity assignment.

When assigning a resource to an existing role assignment or when assigning a role to an existing resource assignment, choose to always use the price/unit of the resource or role; or, choose to be prompted to select which price/unit you want to use each time you assign a resource and a role to an activity assignment.

Tip

▸ If you manually plan future period resource allocation in the Resource Usage Spreadsheet, your selections on the Calculations tab can affect the values you manually enter in future periods for an assignment. See How - Select calculation options for resource and role assignments topic.

Notes

▸ For Fixed Duration and Units activities P6 Professional will not recalculate the actual units for existing resource assignments if they have negative units/time, units, or cost values.

▸ If you choose to always use the role's price/unit, the Rate Source is set to Role in the Activity Details, Resources tab. If you choose to always use the resource's price/unit, the Rate Source is set to Resource. The price/unit value used to calculate costs for the assignment is determined by the rate type you select in the Rate Type field (rate types are resource- and role-specific)

Authentication in P6 Professional

This chapter describes the authentication modes for P6 Professional and outlines the steps required to implement an authentication scheme. It also details steps on how to import user information from an LDAP server.

In This Section

About User Authentication Modes

The P6 Professional provides support for the following authentication modes to validate user logons. Choose one; your choice applies to all applications in the suite.

▶ **Native**: Native mode is the default user authentication scheme for all Oracle Primavera P6 Professional applications. When a user attempts to log on to a Primavera application, native mode confirms the user's identity in the database.

▶ **LDAP (Lightweight Directory Access Protocol)**: LDAP mode confirms a user's identity in the designated directory server database when a user attempts to log on to an application.

Configuring LDAP Servers

P6 Professional uses native authentication mode by default. Use the Administration Configuration tool to configure one or more LDAP servers.

To configure LDAP servers:

1) Click **Start**, then choose **Programs, Oracle - Primavera P6, P6 Professional R8.1, P6 Professional Help and Tools, Administration Configuration.**

2) Enter a privileged user name and password for the P6 Professional database.

3) Enter the Server Name, Database Name, and Port Number for the P6 Professional database.

4) Click the **LDAP Configuration** tab.

5) Click the **LDAP Servers** row then click the **Add** button.

6) Click the plus sign to expand rows.

Enter the details for your LDAP server by clicking the fields and entering the information in the right column. Specify the LDAP directory server host name or IP address, listening port, and base directory node.

For **Base Directory Node**, specify the location in the directory information tree (DIT) that is the location from which to start the search for module users during login. **Base Directory Node** is also the location where the provisioning function begins the search for directory server users.

SSL protocol is recommended for secure communication to the LDAP server. To use SSL protocol for communication with the LDAP server, select **True** for the **Enable SSL** option.

Referrals chasing allows authentication to extend to another domain.To use referrals, select **True** for the **Chase Referrals** option.

> **Note**: Referral chasing is supported with Oracle Internet Directory and Microsoft Windows Active Directory. For Oracle Internet Directories, referrals chasing only works when the directories are configured to allow anonymous searches.

7) If the LDAP server does not allow anonymous searches, type the user name of an LDAP server user who has search access for the Base Directory Node you specified.

8) Click **Test**. If you entered a user name you are prompted for the user's password.

> **Notes**:
> - The password is encrypted and stored in configuration data. The Administration Configuration tool does not unencrypt the password, so the password must be reentered every time **Test** is clicked.
> - Test must be executed for each LDAP server you configure

9) If you see a message saying Test Passed, your LDAP server is properly configured.

10) Click **Save & Close** to exit the Administration Configuration tool.

Provisioning LDAP User Information for the First Time

1) Follow the instructions in *Add new users* (on page 129) to add a new user (in Native mode) that exactly matches an LDAP server user with rights to read the LDAP directory. Make sure to assign a global profile that contains privileges to add new users and search the LDAP directory and assign the appropriate project profiles and module access. The Admin Super profile has appropriate privledges.

2) Log back into the **Administration Configuration** Tool.

3) From the **LDAP Configuration** tab select **True** for **Enable LDAP Authentication**.

4) Log into P6 Professional as the LDAP user created in step 1.

5) Choose Admin, Users.

6) Click **Add**, the Import Domain Users dialog box will appear:

7) Either click the Load LDIF button, or enter an LDAP query (for example, UID=*) under LDAP User Search Criteria.

8) If you clicked the Load LDIP button, browse to the location of the LDIF file, and click Open. If you entered an LDAP query, click Search.

9) A list of users will appear, grouped by category. For example, LDAP repository users that do not exactly match P6 Professional users will be grouped together. If users exist in the LDAP repository, the Login Name, Personal Name, User EMail Address, and Office Phone fields are populated based on the field mappings in the LDAP configuration settings.

10) Select the Import option next to each Login Name that you with to import. New or modified users are automatically selected.

11) Click Import Users.

12) Click Close in the Users dialog box.

> **Notes:**
>
> - You must have the Add/Edit/Delete Users privilege and the Provision Users from LDAP privilege to search the LDAP directory. You do not need the Provision Users from LDAP privilege to import users from the LDIF file.
> - The new users will be assigned the default global profile

Tip

When you provision users, changed records are updated in the P6 Professional database and new users are added. However, users that have been deleted from the LDAP directory or LDIF file are not automatically removed from the P6 Professional database. You will need to manually delete these users.

Configuring P6 Professional Internal Plug-ins for Authentication

P6 Professional is configured with built in plug-ins (such as Update Baseline, Schedule Comparison, or Claim Digger) and must be configured separately for Single Sign-On or LDAP authentication. These plug-ins are designed to read a configuration stored in the database (called 'Internal_Plugins' by default).

Login Procedures and Authentication in P6 Professional

Login procedures for P6 Professional vary according to the authentication mode selected.

In Native mode

▸ P6 Professional presents a login dialog that prompts for a user name and password. Depending on whether the password policy option in Application Settings is enabled, the use of strong passwords might be required.

In LDAP mode

▸ All P6 Professional applications and the P6 SDK require a login password.

Additionally, because passwords are stored and authenticated against an LDAP directory, the capability for users to change passwords within P6 Professional is disabled.

About the Administration Configuration Tool

The Administration Configuration tool can be installed with P6 Professional. It provides the following capabilities:

▸ Ability to reset private database logins
▸ Ability to reset user passwords
▸ Ability to specify LDAP servers

After installing P6 Professional, use the Administration Configuration tool to set up LDAP servers if you are going to use LDAP authentication.

The Administration Configuration tool is installed using the custom option on the setup wizard.

Installing the Administration Configuration Tool

To install the application:

1) Double-click **setup.exe** in the Client_Applications folder of the P6 Professional physical media or download.

> **Notes**:
>
> ▪ Click **Next** on each wizard dialog box to advance to the next step. Click **Cancel** at any time to exit the wizard.
> ▪ Click **Disk Usage** to see disk space requirements for the installation of selected features.

2) Microsoft .NET Framework 4.0, Windows Installer 4.5, and JRE 1.6.0_24 are required to run P6 Professional. If they are not installed, follow the prompts to install them and then restart your computer when prompted. Allow setup.exe to run when your computer restarts and follow the prompts to complete installation of the required components.

> **Note**: Microsoft Windows Imaging Component is required for .NET 4.0 installation on 64-bit Windows XP SP2 systems. This component can be downloaded from Microsoft at ***http://www.microsoft.com/downloads/en/details.aspx?FamilyID=F 64654AC-6E26-41D9-A90A-0E7783B864EE***

3) On the **Welcome** dialog box, click **Next**.

4) On the **Setup Type** dialog box, choose **Custom**

> **Note**: These instructions assume that you have not already installed P6 Professional, if you have not, P6 Professional will be installed with this component unless you select **Entire feature will be unavailable** under **P6 Professional**. See Installing P6 Professional for instructions on completing P6 Professional installation.

5) Click **Administration Configuration** and select **Will be installed on local hard drive**.

6) On the **Ready to Install the Program** screen, click **Install** to begin the installation.

7) Click **Finish** to exit the Setup Wizard.

Resetting Private User Passwords

You can use the Administration Configuration tool to reset private user passwords.

1) Click **Start,** then choose **Programs, Oracle - Primavera P6, P6 Professional R8.1, P6 Professional Help and Tools, Administration Configuration**.

2) Enter a privileged user name and password for the P6 Professional database.

3) Enter the Server Name, Database Name, and Port Number for the P6 Professional database.

4) Click the **Reset Private User Password** tab.

5) In the **Privileged Database User Name** field, select a user whose password you want to reset.

6) In the **New Password** field, enter a new password for the selected user.

7) In the **Confirm New Password** field, enter the password again, to verify it.

8) In the **Public Group ID** field, change the number if necessary. In a standard configuration, the Public Group ID is 1.

9) Click **Save** to continue working or click **Save and Close** if you are finished.

Resetting Application User Passwords

If P6 Professional is using native authentication mode, you can use the Administration Configuration tool to reset application user passwords.

1) Click **Start,** then choose **Programs, Oracle - Primavera P6, P6 Professional R8.1, P6 Professional Help and Tools, Administration Configuration**.

2) Enter a privileged user name and password for the P6 Professional database.

3) Enter the Server Name, Database Name, and Port Number for the P6 Professional database.

4) Click the **Reset Application User Password** tab.

5) In the **Application User Name** field, select a user whose password you want to reset.

6) In the **New Password** field, enter a new password for the selected user.

7) In the **Confirm New Password** field, enter the password again, to verify it.

8) Click **Save** to continue working or click **Save and Close** if you are finished.

> **Notes**:
>
> - If the Enable password policy setting is selected in the Password Policy field of the Admin Preferences dialog box, enter a password that is a minimum of 8 characters long, and that contains one alpha and one numeric character.
>
> - If the Enable password policy setting is not selected, enter a password up to 20 characters long.
>
> - If P6 Professional is running in LDAP authentication mode, password management is handled through the directory server. You cannot change your password through the Administration Configuration tool and the Reset Application User Password tab is not selectable.
>
> - Passwords are case-sensitive.
>
> - Passwords that were set before the new password policy was enabled are valid and usable.

Appendix

In This Section

Importing Projects from P3 to P6 Professional

Use the steps below to import P3 projects if you have experienced the following:

▸ You cannot import P3 projects due to the option being grayed out.

▸ The option was not grayed out, but you received any of the following error messages:

 ▸ Event Code ICSPI-1034-6 Invalid class string, ProgID: "p3session32" when trying to Import a P3 Project into P6 Professional.

 ▸ COM exception caught. Value = 0 when trying to Import multiple P3 Projects into P6 Professional.

 ▸ Typing REGSVR32 RA32.DLL from the windows command prompt returns "LoadLibrary(ra32.dll) failed- cannot find desired module when P3 or SureTrak are not installed on the workstation.

In This Section

What Causes the P3 Import Option to Be Grayed Our or Send an Error Message?

This issue can occur when any of the following conditions exist:

▸ The workstation which has P6 Professional installed does not have P3 or SureTrak installed.

> **Notes:**
>
> ▪ The P6 Professional installer no longer includes the BTRIEVE database engine files necessary to import P3 file format. These files were removed from the P6 Professional installer due to licensing issues with BTRIEVE software.
>
> ▪ Prior to Project Management version 6.2, users could Import/Export P3 data without having P3 or SureTrak installed on the machine; however, with Project Management version 6.2 and later releases, P3 Import/Export functions are disabled unless P3 or SureTrak is installed on the same computer.

▸ The workstation did not have P3 or SureTrak installed, but P3 or SureTrak was installed **after** P6 Professional was installed.

▸ The workstation is using a 64-bit Operating System.

Importing Projects from P3 if You Own a Licensed Copy of P3 or SureTrak

If you never installed P3 on the workstation hosting the P6 Professional application and you own a licensed copy of P3 or SureTrak:

1) Install P3 or SureTrak on the same machine as P6 Professional.
2) Enable the option to import P3 files using one of the following options:
   ‣ Option 1: Install P3 or SureTrak.
   ‣ Option 2: Uninstall P6 Professional. Reinstall P3 or SureTrak first, then install P6 Professional again (in the listed order).
3) If you choose not to install the entire P3 or SureTrak product, install only the BTRIEVE database engine files. Copy the following files from your P3 installation disk to your '\Windows\System32' Directory. The files are located on P3 install CD \Btrieve\win32 dir:
   - W32MKDE.EXE
   - W32MKRC.DLL
   - WBTRV32.DLL
4) (Optional) For the MicroKernel Setup utility that is used to modify registry settings for the BTRIEVE engine, copy the following files from your P3 installation disk to your '\Windows\System32' Directory. The files are located on P3 install CD \Btrieve\Win32 \Tools dir:
   ‣ W32MKSET.DLL
   ‣ W32MKSET.EXE
   ‣ W32MKSET.HLP

Message when Starting Import or Export

You may see the following message when starting import or export using P6 Optional Client R8.1 when P6 Optional Client R8.1 and P6 Professional R8.1 are installed on the same computer:

```
PM.exe - Unable To Locate Component
This application has failed to start because wbtrv32.dll was not found.
Re-installing the application may fix this problem.
```

If you see this message click OK to ignore it, when the import or export dialog appears, proceed with the import or export process.

Note:
- You may have to click OK several times to dismiss the error.
- Install P3 to avoid this message.