



PRIMAVERA

Integration API Administrator's Guide
Release 8.0

Copyright

Copyright © 2003, 2010, Oracle and/or its affiliates. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

The platform-specific hardware and software requirements included in this document were current when this document was published. However, because new platforms and operating system software versions might be certified after this document is published, review the certification matrix on the My Oracle Support (formerly OracleMetaLink) Web site for the most up-to-date list of certified hardware platforms and operating system versions. The My Oracle Support (formerly OracleMetaLink) Web site is available at the following URL:

<http://metalink.oracle.com/>

or

<http://support.oracle.com/>

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable: U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software -- Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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 P6 Commercial Notices and Disclosures for Documentation, go to the \Documentation\<language>\Notices and Disclosures folder of the P6 physical media or download.

Contents

Copyright.....	2
Preface.....	7
Using this Administrator's Guide	7
Media Packs for P6 EPPM	7
Primavera P6 EPPM R8 Media Pack.....	7
Where to Get Support	9
Install P6 Integration API	11
What is the P6 Integration API?.....	11
System Requirements.....	11
P6 Integration API Installation Process.....	12
Deploying the P6 Integration API for Remote Mode	15
Changing Database Configuration Settings.....	17
Enabling Access.....	18
Java Security Manager.....	18
Using the P6 Administrator application	19
Starting the P6 Administrator application	19
Reviewing and Modifying P6 Integration API Configurations.....	19
Setting up Event Notification	21
P6 Administrator application Settings	22
Configuration Settings for P6 EPPM	22
Localization Settings	22
Session Management Settings.....	23
Database Settings.....	23
Thread Pool Settings	36
Log Settings	37
Directory Services Settings	38
Application Settings.....	39
Services Settings	44
Performance Monitor Settings.....	53
Tracer Settings	53
Integration API Server Settings.....	54
P6 Web Services Settings	55
Authentication Settings for P6 EPPM.....	59
Authentication Settings.....	60
Database instance Settings.....	62
LDAP	65
Authentication Modes	65
Implementing Non-Native Authentication.....	65
Choosing an Authentication Scheme	66
Using the Authentication Tab in the P6 Administrator application	66
Configuring P6 Integration API Authentication	68

Login Procedures and Authentication in P6 EPPM 68

Preface

The P6 Integration API is a Java-based API and server that enables developers to create client code that can seamlessly access P6 EPPM functionality.

In This Chapter

Using this Administrator's Guide	7
Media Packs for P6 EPPM.....	7
Where to Get Support.....	9

Using this Administrator's Guide


This guide describes the steps required to install the P6 Integration API and how to configure it to use one of three authentication modes. It is organized as follows:

Installing the P6 Integration API: Describes how to install the P6 Integration API and explains how to use the P6 Administrator application to review, modify, add, and delete P6 Integration API server configurations.

Configuring Authentication Modes: Describes the authentication modes available in this release and explains how to configure the P6 Integration API to operate using one of three authentication modes.

Media Packs for P6 EPPM

Media packs include all files necessary to install P6 EPPM applications, all manuals and technical documents related to the installation, administration, and use of P6 EPPM components, and the Quick Install Guide.

P6 EPPM Media Packs are delivered via physical media or from the Oracle E-Delivery Web site in zip files.  The E-Delivery site provides instructions for how to perform a secure download.

Primavera P6 EPPM R8 Media Pack

- ▶ **Primavera P6 Enterprise Project Portfolio Management Quick Install Guide:** Includes the Quick Install Guide.
- ▶ **Primavera P6 Documentation:** Includes all manuals and technical documents related to the installation, administration, and use of P6 EPPM components.
- ▶ **Primavera P6 EPPM R8:** Includes all files necessary to install P6 EPPM, sample reports, the BPM Connector, and the BPM sample workflows.
- ▶ **Primavera P6 EPPM Database Setup R8:** Includes all files for both manual and automatic application database setup.

- ▶ **Primavera P6 Professional R8 for EPPM:** Includes all files necessary to install P6 Professional, the optional and always connected Windows Client, P3 converter, and the P6 SDK.

Note: This is not an upgrade for P6 Professional 7.0 standalone.

- ▶ **Primavera P6 Integration API and P6 Web Services R8:** Includes all files necessary to install the P6 Integration API and P6 Web Services (can be licensed separately).

Note: The P6 Integration API and P6 Web Services should be licensed by developers who are not licensed for P6 EPPM, but who need access to applications created using P6 Web Services, P6 Integration API, or both.

- ▶ **Primavera P6 Reporting Database R2.1:** Includes all files necessary to install P6 Reporting Database (must be licensed separately).
- ▶ **Primavera P6 Analytics R1.1:** Includes all files necessary to install P6 Analytics (must be licensed separately). It also includes all files necessary to install P6 Reporting Database R2.1.
- ▶ **Primavera P6 Tools R8:** Includes P6 Compression Server, SharePoint Connector, and the OIM Connector.
- ▶ **Primavera P6 Progress Reporter R8:** Includes all files necessary to install P6 Progress Reporter (can be licensed separately).
- ▶ **Oracle Content Server 10gR3:** Included in the Microsoft Windows and Linux platform versions of the media pack. The one provided is 10.1.3.3.3, and you should apply the 10.1.3.4.1 patch update. Contains all files necessary to install Oracle Universal Content Management for use with the Primavera P6 EPPM R8 Media Pack. For information on installing Oracle Content Server, visit <http://www.oracle.com/technology/documentation/oecm.html>. Please note the following license restrictions for this version of Oracle Content Server:
 - ▶ It is a restricted use license and is only included with a P6 EPPM license. Customers licensed for P6 EPPM under legacy Primavera licensing who would like to take advantage of the restricted use license of Oracle Content Server, should contact their Sales representative to migrate their licenses to the current Oracle offerings.
 - ▶ It is only valid for workspaces or folders that are built from P6 EPPM and repositories that store P6 EPPM documents, artifacts, and work products. Manually creating any workspaces, folders, repositories, etc. outside of P6 EPPM applications will trigger a full-use license.
 - ▶ Only licensed P6 EPPM application users can access the repository.
- ▶ **Oracle WebLogic Server 11gR1 (10.3.3.0):** Included in the Microsoft Windows, Linux, HP-UX, and Sun Solaris platform versions of the media pack. Contains all files necessary to install Oracle WebLogic Server for use with the Primavera P6 EPPM R8 Media Pack. For information on installing Oracle WebLogic Server, visit <http://oracle.com/technology/documentation/bea.html>. Please note the following license restrictions for this version of Oracle WebLogic Server:
 - ▶ It is a restricted use license and is only included with a P6 EPPM license. Customers licensed for P6 EPPM under legacy Primavera licensing who would like to take advantage of the restricted use license of Oracle Weblogic Server, should contact their Sales representative to migrate their licenses to the current Oracle offerings.
 - ▶ P6 is the only application that can be deployed to the WebLogic Server instance. No other applications can be deployed.

- ▶ It does not include the use of features in the Enterprise Edition or Suite version of Oracle WebLogic Server; it is restricted to the use of features included in the Standard version.
- ▶ It does not include the use of clustering, coherence, or Enterprise JavaBeans (EJBs). For example, clustering the P6 EPPM instance will trigger a full-use license.
- ▶ **JRockit Real Time 4.0 for Java SE 6:** Included in the Microsoft Windows and Linux platform versions of the media pack. Contains all files necessary to install JRockit for use with Oracle WebLogic Server 11gR1 (64-bit). For information on installing Oracle WebLogic Server, visit <http://oracle.com/technology/documentation/bea.html>. Please note the following license restrictions for this version of JRockit:
 - ▶ It is a restricted use license and is only included with a P6 EPPM license. Customers licensed for P6 EPPM under legacy Primavera licensing who would like to take advantage of the restricted use license of JRockit, should contact their Sales representative to migrate their licenses to the current Oracle offerings.
 - ▶ It can be used for only P6 EPPM servers.
 - ▶ It is a runtime license that does not allow the use of JRockit for other applications or instances.
- ▶ **Oracle BI Publisher:** Included in the Microsoft Windows and Linux platform versions of the media pack. Contains all files necessary to install Oracle BI Publisher. Valid for users to schedule/execute/run reports within the Primavera application. Any users who need to customize or create new reports will need a full-use license of BI Publisher. You should also apply the following patch update "Patch 10256764: UPDATE FOR BI PUBLISHER ENTERPRISE 10.1.3.4.1 NOVEMBER 2010"

Where to Get Support

If you have a question about using Oracle Primavera 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.

Go to http://download.oracle.com/docs/cd/E17266_01/index.htm for the latest updates to the P6 EPPM 8.0 Documentation library.

Install P6 Integration API

This chapter describes how to install the P6 Integration API. In addition, this chapter explains how to use the P6 Administrator application to review, modify, add, and delete P6 Integration API server configurations.

In This Chapter

What is the P6 Integration API?	11
System Requirements.....	11
P6 Integration API Installation Process.....	12
Deploying the P6 Integration API for Remote Mode.....	15
Changing Database Configuration Settings	17
Enabling Access.....	18
Java Security Manager.....	18
Using the P6 Administrator application.....	19
Starting the P6 Administrator application.....	19
Reviewing and Modifying P6 Integration API Configurations	19
Setting up Event Notification.....	21
P6 Administrator application Settings	22

What is the P6 Integration API?

The P6 Integration API is a Java-based API and server that enables developers to create client code that can seamlessly access P6 EPPM functionality.

System Requirements

The P6 Integration API has the following system requirements for both local mode installations:

Java Runtime Environment

- ▶ Before installing P6 Integration API, you need to install the Java Development Kit (JDK), version 1.6.x, also known as J2SE 6.0. While P6 Integration API is compatible with any 1.6 version, Oracle recommends that you use Update 20. The Integrated Development Environment (IDE) you use to create code must work with this version.
- ▶ You can download the Java JDK from the Sun Microsystems Web site (<http://www.oracle.com/technetwork/java/archive-139210.html>).

Operating Systems

Note: The following summarizes configurations that have been tested with P6 Integration API. For the full list of system requirements, versions, and tested configurations, go to the \Documentation\<language>\Tested_Configurations folder of the P6 EPPM physical media or download.

- ▶ The P6 Integration API is fully supported on Windows, Solaris, and Linux operating systems.

Note: Even though the JRE and JDK are available on additional operating systems, they have not been tested by Oracle Primavera.

Project Management Database

- ▶ A P6 EPPM database (Oracle and SQL Server are supported).

Application Servers

Remote mode installations of the P6 Integration API require one of the following supported application servers:

- ▶ Oracle WebLogic 11g R1 (10.3.3.0)
- ▶ IBM WebSphere 7.0 fp11

P6 Integration API Installation Process

Before installing the P6 Integration API, you need to install P6 EPPM. Additionally, you must uninstall any earlier versions of the P6 Integration API before installing the current version.

Note: For information on installing P6 EPPM, see the P6 EPPM Administrator's Guide, which is provided in the \Documentation\<language> folder on the P6 physical media or download.

The P6 Integration API Installer provides a wizard to guide you through the installation process, which includes:

- ▶ Choosing the installation mode
- ▶ Installing the P6 Integration API client side and server side libraries
- ▶ Setting up and configuring the P6 Integration API database

Notes:

- Before you start the installation, make sure you set the JAVA_HOME environment variable.
 - Due to the global nature of the OUI (Oracle Universal Installer), the OUI online help is not applicable for installing or uninstalling the P6 Integration API or for references to P6 EPPM documentation. Instead, refer to the installation instructions in this section.
-

To install the P6 Integration API

- 1) From the Web_Services\Integration API folder of the physical media or download location, run one of the following depending on your system type:

- ▶ If you are installing on a Microsoft Windows system, navigate to the **win\Disk I\install** directory and then double-click on the **setup.exe** file.
 - ▶ If you are installing on a non-Microsoft Windows system, type the following command:
cd<OperatingSystem>\Disk I\install
 - a. Depending on your operating system, replace **<Operating System>** in the command above with **solaris_64**, **linux**, **hp_64**, or **aix_64-5L**.
 - b. Type the following commands:
chmod 755 runInstaller
chmod 755 unzip
./runInstaller
 - c. Click **Next**.
- 2) On the **Welcome** page, click **Next**.
- 3) On the **Please select the installation type** page, specify the installation mode.
- ▶ **Local Mode Packages Only** - Choose this option to use the P6 Integration API in local mode, without Java RMI.
This option installs client-side and server-side Java libraries, database configuration tools, and javadoc.
 - ▶ **Client Side Packages Only** - Choose this option to use the P6 Integration API in remote mode.
This option installs client-side Java libraries and javadoc.

Note: The maximum number of clients that can access a remote server at one time is approximately 50. This number might be less, depending on multiple factors (e.g., system hardware, network configuration, etc.)

After installing the client-side packages, to complete a remote mode installation, install the P6 Integration API on a separate machine using the following option:

Supported J2EE Compatible Application or Web Servers - This option installs the P6 Integration API application file, **PrimaveraAPI.war**, into the `applications` subdirectory of the destination you specify in the wizard.

The **PrimaveraAPI.war** file contains both client-side and server-side libraries, database configuration tools, and the javadoc. You can deploy the P6 Integration API as a Web application into any J2EE-compatible application or Web server that supports JDK/JRE 1.6.x.

- 4) In the **Specify Home Details. . .** dialog box:
- a. Enter an appropriate name for the P6 Integration API in the **Name** field.
 - b. Specify the installation location for the P6 Integration API files in the **Path** field.

Note: If you setup the `JAVA_HOME` environment variable, the location of the JRE is automatically filled in for you.

- c. Click **Next**.
- 5) In the **Available Product Components** dialog box, select the components to install and click **Next**.
- 6) In the **JDK Home Directory** dialog box, type or browse to the location where JDK is installed.
- 7) In the **Summary** dialog box, click **Install**.

Note: After the P6 files are installed, the **Configuration Assistants** dialog box opens. Do not close this dialog box. After a short time, the **Setup and Configuration of the Primavera Database** dialog box opens.

- 8) In the **Setup and Configuration of the Primavera Database** dialog box, specify the database type.

Note: You can later change the database type through the P6 Integration API Database Configuration Setup.

- 9) In the **Please enter the following information. . .** dialog box, specify the database connection parameters.

Note: The P6 Integration API requires **pubuser** access (in the User Name field) to the database. The database name, host address, and host port are specific to your Oracle or MS SQL Server installation. Database Host Port displays the default port for the database type you selected. You can edit this port.

- 10) In the **The installer has detected an existing. . .** dialog box, choose the appropriate action. The configuration stores server-side settings for the server.

Notes:

- If your site includes P6, you can share a new P6 Integration API configuration with P6. However, an existing configuration for P6 cannot be shared with the P6 Integration API because it will not provide support for new P6 Integration API configuration settings.
 - If there is no existing configuration, the **The installer has detected an existing. . .** dialog box does not appear and the installation process automatically creates a default configuration named Primavera Configuration. You can edit the settings for this configuration through the P6 Administrator application.
 - After installation, you can use the Database Configuration Setup wizard to choose or create a different configuration, if necessary.
 - For more information about configurations, see **Using the P6 Administrator application** (on page 19).
-

- 11) When the message displays to confirm that the database configuration has completed successfully:
- a. Click **OK**.
 - b. Click **Exit** to close the Setup wizard.

You will now have the following shortcuts appended to the P6 Integration API entry in your Start menu:

- ▶ Demo applications
- ▶ Documentation (Java API Documentation, Programmer's Reference, and Readme)
- ▶ Database Configuration
- ▶ P6 Administrator application

Deploying the P6 Integration API for Remote Mode

If you selected **Supported J2EE compatible application or Web servers** when installing the P6 Integration API, you need to then deploy the P6 Integration API into the appropriate application or web server that supports JDK/JRE 1.6.x.

Note: Refer to your application server documentation for detailed deployment instructions.

Deploying into Weblogic

Deploying the P6 Integration API into Weblogic involves two steps:

- 1) Creating a WebLogic domain for the P6 Integration API application.
- 2) Deploying the P6 Integration API into the WebLogic domain.

Creating a WebLogic Domain

- 1) Run the **Oracle WebLogic Configuration Wizard**.
- 2) On the Oracle WebLogic Configuration Wizard **Welcome** page, select **Create a new WebLogic domain** and click **Next**.
- 3) On the **Select Domain Source** page, select one of the options.
 - ▶ If you select **Generate a domain configured automatically to support the following products**, mark products and click **Next**.
 - ▶ If you select **Base this domain on an existing template**, enter a location in the **Template location** field or browse for a location.
- 4) On the **Specify Domain Name and Location** page:
 - a. In the **Domain name** field, enter a domain name.
 - b. In the **Domain location** field, enter or browse for a domain location.
 - c. Click **Next**.
- 5) On the **Configure Administrator Username and Password** page:
 - a. In the **Name** field, enter your user name.
 - b. In the **User password** field, enter your password information.
 - c. In the **Confirm user password** field, reenter your password.
 - d. Click **Next**.
- 6) On the **Configure Server Start Mode and JDK** page:
 - a. In the **WebLogic Domain Startup Mode** pane, select **Production Mode**.
 - b. In the JDK Selection pane, select one of the options.
 - If you select **Available JDKs**, click one of the JDKs and click **Next**.
 - If you select **Other JDK**, enter or browse for a location in the **Location** field and click **Next**.
- 7) On the **Select Optional Configuration** page, click **Next**.
- 8) On the **Configuration Summary** page, click **Create**.
- 9) On the **Creating Domain** page, mark the **Start Admin Server** option and click **Done**.
- 10) When prompted, enter the username and password that you entered above.

Deploying the P6 Integration API into the WebLogic domain

- 1) On the **Welcome** page of the **Administration Console**, log in using the user name and password that you entered above.
- 2) In the **Administration Console**, click **Lock & Edit** in the **Change Center** pane.
- 3) In the **Domain Structure** pane, click **Deployments**.
- 4) In the **Summary of Deployments** pane, click **Install**.
- 5) In the **Path to the new application** pane:
 - a. Click the browse button to navigate to the **<IntegrationAPI installation>\applications** directory.
 - b. Select the **PrimaveraAPI.war** file and click **Next**.
- 6) In the **Install Application Assistant** pane, select **Install this deployment as an application** and click **Next**.
- 7) In the **Install Application Assistant** pane, click **Next** to accept the default options.
- 8) Review the configuration settings you have chosen and click **Finish** to complete the installation.
- 9) On the **Settings for PrimaveraAPI** page, click **Save**.
- 10) In the **Change Center** pane, click **Activate Changes**.
- 11) In the **Domain Structure** pane, click **Deployments**.
- 12) In the **Summary of Deployments** pane, select **PrimaveraAPI**.
- 13) In the **Summary of Deployments** pane, click the down arrow to the right of the **Start** button and click **Servicing all requests**.
- 14) In the **Start Application Assistant** pane, click **Yes**.
- 15) In the **Summary of Deployments** pane, click the **start Running** link in the **State** column of the row that contains PrimaveraAPI.
- 16) In the **Domain Structure** pane, click **Deployments**.

Note: The PrimaveraAPI state column should be **Active**.

Deploying into WebSphere

Follow these steps to deploy the P6 Integration API into WebSphere:

- 1) Start the **WebSphere Application Server**.
- 2) Launch the WebSphere Application Server **Administrative Console**.
- 3) In the **Administrative Console**:
 - a. Expand **Servers** in the navigation pane and click **Server Types**.
 - b. Click **WebSphere Application Servers**.
- 4) On the **Application Servers** page, click the server name link.
- 5) On the **Configuration** tab under **Server Infrastructure**, expand **Java and Process Management** and click **Process Definition**.
- 6) Under **Additional Properties**, click **Java Virtual Machine**.
- 7) Under **Generic JVM arguments**, type:
-Dprimavera.bootstrap.home=c:\apihome
(where 'c:\apihome' is the installation directory).

- 8) Click **OK**.
- 9) Click the **Save** link that appears within the message reporting changes.
- 10) In the left navigation pane, expand **Applications** and click **New Application**.
- 11) Click **New Enterprise Application**.
- 12) On the **Path to the new application** page, specify the path to the war file in the **apihome** folder.
For example:
c:\apihome\applications\primaveraapi.war
- 13) Click **Next**.
- 14) In the **How do you want to install the application** dialog box, select the **Fast Path** option and click **Next**.
- 15) In the **Step 1** section **Select Installation Options**, click **Next**.
- 16) In the **Step 2** section **Map Modules to Servers**, mark the **Primavera Integration API** option, and click **Next**.
- 17) In the **Step 3** section **Map Virtual Host for Web Modules**, mark the **Primavera Integration API** option, and click **Next**.
- 18) In the **Step 4** section **Map context roots for Web module**, for the **Context Root**, type **/PrimaveraAPI** then click **Next**.
- 19) In the **Step 5** screen **Summary**, click **Finish**. Note that the application war file is now deploying and this process can take several minutes.
- 20) To save the master WebSphere configuration, click **Save**. This process can also take several minutes.
- 21) On the **Administrative Console** main window, in the left navigation, expand **Application Types** under **Applications** and click **WebSphere enterprise applications**.
- 22) Mark the **PrimaveraAPI.war** option.
- 23) Click **Start**.

Changing Database Configuration Settings

The P6 Integration API Database Configuration wizard lets you create a new configuration or switch to a different configuration than the one specified during the P6 Integration API installation.

The database you connect to during the installation stores one or more P6 Integration API configurations. Each configuration specifies a set of configurable parameters that determine how the P6 Integration API operates. If no configuration exists in the database the first time you install the P6 Integration API, you must create a new configuration. For subsequent installs, you can choose an existing configuration or create a new one. After installation, you can use the Database Configuration wizard to select a different P6 Integration API configuration or create a new one.

Note: After selecting a different P6 Integration API configuration or creating a new configuration, you must stop and restart the server for the changes to take effect.

Starting the Database Configuration wizard

- ▶ On Windows, from the **Start** menu, choose **Programs > Oracle - Primavera P6 > Primavera P6 API > Database Configuration**.

- ▶ On Solaris/Linux, change to the **PrimaveraAPI** directory under the application server install directory and run the **dbconfig.sh** script.

Enabling Access

Before users can log into the P6 Integration API, they must be granted module access to the P6 Integration API from P6.

Note: For more information on creating users and enabling access to applications, refer to the *P6 EPPM Administrator's Guide*, which is available in the \Documentation\<language> folder of the P6 EPPM physical media or download.

To enable access to the P6 Integration API:

- 1) Login to the P6 as a user with administrative privileges.
- 2) Click the **Administer** menu and choose **User Access**.
- 3) On the **User Access** page, click **Users**.
- 4) On the **Users** page, select the appropriate user and click the **Module Access** tab.
- 5) On the **Module Access** tab, select the **Integration API** option.

Java Security Manager

The Java security manager enables programmers to establish a custom security policy for their Java applications.

Note: The Java security manager is not supported for IBM WebSphere Application Server v 7.0.

Unless it is specifically enabled when the P6 Integration API server is started, the security manager is disabled. To enable/disable the security manager, edit the P6 Integration API server's startup script with a text editor and uncomment/comment the appropriate command (see below).

For Windows platforms, edit **startAppServer.cmd**. For Solaris/Linux, edit **startAppServer.sh**.

WebLogic

Windows:

SET ENABLE_JAVA_SECURITY_MANAGER=-Djava.security.manager

Solaris/Linux:

ENABLE_JAVA_SECURITY_MANAGER=-Djava.security.manager

Note: The P6 Integration API server can use different policy files for different application/web servers.

Using the P6 Administrator application

As the system administrator, you can use the P6 Administrator application to review, modify, add, and delete server configurations. P6 Integration API server configurations are stored in the database specified during installation. These configurations contain all of the settings used to run the P6 Integration API server.

Caution: Only experienced administrators should use the P6 Administrator application to modify configuration settings.

Starting the P6 Administrator application

After launching the P6 Administrator application, you will be prompted for a database level password for the **privuser** account.

Starting the P6 Administrator application

- ▶ On Windows, from the **Start** menu, choose **Programs > Oracle - Primavera P6 > Primavera P6 API > Administration Application**
- ▶ On Solaris/Linux, change to the **PrimaveraAPI** directory under the application server install directory and run the **admin.sh script**.

Reviewing and Modifying P6 Integration API Configurations

The P6 Administrator application presents configuration settings in tabs. Configurations and Authentication views display the current configurations and settings. Log displays a history of configuration changes, additions, or deletions for the current session.

Note: You cannot edit the Factory Default configuration settings. You can only modify custom configurations.

To display brief setting descriptions in the Configurations view, select the Show tool tips option. Then, position the mouse over a setting to read the description.

Add P6 Integration API configurations

To create a new configuration, you can duplicate an existing configuration.

- ▶ To duplicate a configuration:
 1. Select the configuration name in the Configurations tab.
 2. Right-click and choose Duplicate.
 3. Enter a name for the configuration, then click OK.
 4. Edit the settings as needed.
- ▶ To create a new configuration based on factory default settings, right-click on Factory Defaults in the Configurations tab and choose Duplicate.

Add database instances to a configuration

The P6 Integration API enables you to access data from different project manager databases. When you configure the P6 Integration API to support multiple database instances, you can choose the instance you want at login.

To add a new database instance to an P6 Integration API configuration, you can duplicate an existing instance. To duplicate a database instance:

- 1) Select the icon representing the instance.
- 2) Right-click and choose Duplicate.
- 3) Enter a unique name for the new instance.
- 4) Edit other settings as needed.

Delete P6 Integration API configurations and database instances

To delete a configuration or database instance:

- 1) Select the one you want to delete.
- 2) Right-click and choose Delete.

Notes:

- You cannot delete the Factory Defaults configuration. You can delete any custom configuration, but not all of them. There must always be at least one custom configuration.
 - You can delete any database instance associated with a configuration, but not all of them. Each configuration must have at least one database instance.
 - For more information, see `Database.Instance.Driver` and `Database.Instance.URL` in **P6 Administrator application Settings**.
-

Database driver configurations

The following table lists the database drivers the P6 Integration API supports for each application server/database configuration. Use the `Database.Instance.Driver` configuration setting to specify the database driver you are using.

Application Server	Database Type	Database Driver	Default
WebLogic	Oracle	Oracle Thin Client	Y
WebLogic	SQL Server	SQL Server JDBC	Y
WebSphere	Oracle	Oracle Thin Client	Y
WebSphere	SQL Server	SQL Server JDBC	Y

Configure P6 Integration API Authentication

The P6 Integration API uses a single authentication setting to support authentication.

- ▶ `Authentication.Mode`

Because one P6 Integration API server instance can control more than one database, in addition to specifying an authentication mode for a database through the Authentication tab of the P6 Administrator application, you use the `Authentication.Mode` authentication setting to specify the overall mode you want to use for the P6 Integration API server. For LDAP authentication with secure communication (SSL) between the P6 Integration API server and the LDAP server, two additional authentication settings are required.

For more information about each of these settings, refer to ***Authentication Settings for P6 EPPM***.

Note: A P6 Integration API configuration might include database instances that are not set to the same authentication mode as the P6 Integration API server. If a user connects and requests a database that is set to a different authentication mode than the P6 Integration API server, an error message displays. The user must select a database that matches the authentication mode set for the P6 Integration API server.

Configure a Setting for WebLogic on Microsoft SQL Server 2005 Databases

The following instructions apply when using a Microsoft SQL Server 2005 database. If the Microsoft SQL Server database is localized or installed on a localized operating system, it is necessary to use the SET DATEFORMAT setting in the P6 Administrator application. Otherwise, the user will encounter SQL errors when navigating in Resource Planning and Capacity Analysis. Odd behavior might also occur in the Activities view. To avoid these issues:

- 1) In the P6 Administrator application, locate the Database folder for the Microsoft SQL Server database used by P6.
- 2) In that folder, expand the appropriate Instance folder and then the Session Settings folder (choices will be from 1 to 5).
- 3) Use the following syntax to add a Session Setting: **set DATEFORMAT ymd**
- 4) Click **Save Changes**.
- 5) Restart the application server. The change will immediately take effect.

Setting up Event Notification

Depending on the administrative settings, events can be triggered when the P6, P6 Web Services, or P6 Integration API is used to update or create objects in the P6 EPPM database. When a change triggers an event, the P6 EPPM Event Notification system sends the event message to a user configured message queue. If you are planning to use Event Notification with P6 EPPM products, follow the steps below to set up Event Notification to work with your Java Messaging Service (JMS), the application server, and P6 EPPM.

Before you begin: Add the JMS vendor jar files to the application classpath. Refer to the Oracle Primavera Support Knowledgebase for additional information and examples.

Apply the eventing configuration settings as follows:

- 1) Set the "Database/Instance/Eventing/Enabled" setting to true.
- 2) Set additional Database/Instance/Eventing/ settings as appropriate.

Refer to the ***P6 Administrator application Settings*** section for additional information about the database settings.

P6 Administrator application Settings

You can review and modify configuration settings in the Configuration tab and authentication settings in the Authentication tab of the P6 Administrator application. All settings are stored in the database for P6, which you specified during installation.

You can specify durations (time-related values) in several ways:

- ▶ As a simple number, which is always treated as milliseconds.
For example, 240000 would be equivalent to 4 minutes (240000/60000).
- ▶ As a specified time, where "d" is days, "h" is hours, "m" is minutes, and "s" is seconds. All parts are optional.
For example, you can enter:
1d2h30m20s
4m
1h30s

Caution: Only experienced administrators should use the P6 Administrator application of P6 to modify settings.

Note: Localization settings are not applicable for the P6 Integration API or P6 Web Services.

Tips

- ▶ Configurations and database instances are viewable from the **Authentication** tab but can be modified only on the **Configurations** tab.
- ▶ If multiple instances within a configuration point to the same database, the Authentication Mode for the first instance in the list will be used.
- ▶ To enable you to configure more than one LDAP server for each database instance, multiple LDAP Connection Settings are permitted for authentication. Right-click the **LDAP Connection Settings** folder to duplicate, delete, copy, paste, or test a configuration.
- ▶ A configuration for P6 might include database instances that are not set to the same authentication mode as the P6 server. If a user connects and requests a database that is set to a different authentication mode than the P6 server, an error message displays; the user must select a database that matches the authentication mode set for the P6 server.

Configuration Settings for P6 EPPM

The information below details all settings available from the Configuration tab of the P6 Administrator application.

Localization Settings

Setting Name and Description	Default	Valid Ranges/Values
Localization/System Language	en	—

Default language on login page for first-time login.

Localization/System Country	US	—
Country for server string constants		

Session Management Settings

Setting Name and Description	Default	Valid Ranges/Values
Session Management/Maximum Session Timeout The maximum length of time that a user session can remain open, regardless of activity, before P6 EPPM times it out.	1d	1m-24d

Database Settings

Setting Name and Description	Default	Valid Ranges/Values
Database/Instance[n]/Name The name of this database instance. This determines how the database instance name will appear on the P6 login page.	—	up to 32 characters
Database/Instance[n]/Description A description of this database instance.	—	up to 128 characters
Database/Instance[n]/Schema The schema that will be defined for the database.	PMDB	—

Database/Instance[n]/URL

The database URL used to establish a connection to the P6 EPPM database.

Oracle example:

`jdbc:oracle:thin:@xx.xxx.xxx.xx:yyyy:zzzz`

SQL Server example:

`jdbc:sqlserver://xxxx:yyyy;database=zzzz;`

x = IP address or hostname

y = database listen port

z = database name

Database/Instance[n]/Public Group ID

The public group ID used to establish a connection to the database.

Database/Instance[n]/User Name

The name used to establish a connection to the database.

Database/Instance[n]/Password

The password used to establish a connection to the database.

Database/Instance[n]/Timesheet URL

URL for invoking the P6 Progress Reporter module.
To verify that the URL entered for this setting is valid, right-click over the setting, then select 'Test Connection.'

Note: The URL might be case-sensitive, depending on your application server configuration.

Example format:

`http://server name:listen port/pr/`

Database/Instance[n]/User Security/Log Login Attempts

Specifies whether or not login attempts to P6 are tracked in the Web Access logs.

Database/Instance[n]/User Security/Login Lockout Count

The number of times a user can attempt to login before the account is locked. A setting of "0" allows an unlimited number of attempts. The count resets after each

None, Failed Attempts, Successful Attempts, All

0-100000



successful login.

Database/Instance[n]/User Security/Login Lockout Duration	1h	0-24d
<p>The length of time that a user is blocked from logging into P6, starting from the point at which the Logging Lockout Count was exceeded.</p> <p>This setting will be overridden if a user's session is manually reset by an Admin Superuser. For more information, see <i>Reviewing and Modifying Configurations for P6</i>.</p>		
Database/Instance[n]/User Security/Allow Multiple User Sessions	Yes	No, Single Machine, Yes
<p>Specifies whether a single user can be simultaneously logged into Web Access.</p> <p>A setting of "Yes" will allow a single user to login multiple times on any machine.</p> <p>A setting of "No" restricts a user to logging in only once on any machine.</p> <p>A setting of "Single Machine" allows a user to log in multiple times on the same machine, as long as the application server is configured properly to determine the IP address of the machine making the request. For example, if the application server is behind a proxy server, this setting will default to "Yes" instead of "Single Machine."</p>		
Database/Instance[n]/Auto Start Services	true	true/false
<p>Set to true to automatically start all services for this database when the application server starts. When this is true, all services with a concurrent task greater than zero will start when the application server starts. Set this to true if you will use the Summarize or Apply Actuals features in P6 Professional.</p> <p>If set to false, you must manually log into the application before the concurrent services will start.</p> <p>Note: BRE services will not start until someone logs into the application one time.</p>		

Database/Instance[n]/Connection Pool [aaa]/Resize Rate 4m 4m - 12h

The timeout period after which the system will adjust the number of database connections to be equal to the maximum number of database connections simultaneously used during the last period.

[PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine.

[PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs.

[PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.

Database/Instance[n]/Connection Pool [aaa]/Maintenance Frequency 1m 10s - 1h

The run frequency of the maintenance that ensures leases have not exceeded the maximum duration.

[PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine.

[PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs.

[PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.

Database/Instance[n]/Connection Pool [aaa]/Lease Request Wait Timeout 30s 5s - 2h

The amount of time a request for a database connection will wait.

[PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine.

[PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs.

[PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.

Database/Instance[n]/Connection Pool [aaa]/ Maximum Connections	50	5 - 15000
<p>The maximum number of connections the server will have to the database.</p> <p>[PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine.</p> <p>[PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs.</p> <p>[PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.</p>		
Database/Instance[n]/Connection Pool [aaa]/Fetch Size	120	—
<p>A hint to the database driver for how many rows to fetch at a time.</p> <p>[PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine.</p> <p>[PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs.</p> <p>[PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.</p>		
Database/Instance[n]/Connection Pool [aaa]/Trace SQL	false	true/false
<p>Trace all SQL sent to the database.</p> <p>[PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine.</p> <p>[PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs.</p> <p>[PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.</p>		

Database/Instance[n]/Connection Pool [aaa]/
Renewable Free Limit

3

3 - 5

The minimum number of connections that should be available for leases to be renewed.

[PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine.

[PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs.

[PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.

Database/Instance[n]/Connection Pool [aaa]/
Renewable Leases

PMR - false
PML - false
PMT - true

true/false

If false, each connection can be leased only for the MaxLeaseDuration period.

If true, connection leases are renewed if database statements are completed within the MaxLeaseDuration time period. When true, the code can hold onto the connection as long as it needs, provided SQL statements are completed within the MaxLeaseDuration period. When true, the connection is revoked if no SQL statements are issued within the MaxLeaseDuration period or if one statement takes longer to execute than that period.

[PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine.

[PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs.

[PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.

Database/Instance[n]/Connection Pool [aaa]/ Maximum Lease Duration	PMR - 2m PML - 10m PMT - 10m	PMR - 5s - 4h PML - 5s - 6h PMT - 5s - 6h
<p>The maximum amount of time a database connection can be leased before it is revoked.</p> <p>[PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine.</p> <p>[PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs.</p> <p>[PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.</p>		
Database/Instance[n]/Content Repository/Type	None	None, Oracle, SharePoint
<p>The application that will be used to host content repository data in P6 EPPM.</p> <p>After choosing the content repository type, enter the appropriate settings below for the type selected.</p>		
Database/Instance[n]/Content Repository/Oracle Universal Content Management/Host	—	—
<p>The machine name or IP address of the Universal Content Management server.</p>		
Database/Instance[n]/Content Repository/Oracle Universal Content Management/Port	—	—
<p>The IntradocServerPort number of the Universal Content Management server. By default, this is 4444.</p>		
Database/Instance[n]/Content Repository/Oracle Universal Content Management/Oracle Home	—	—
<p>Path to the P6 EPPM content repository files on the Universal Content Management server, as specified in step 2 of Configuring Oracle Universal Content Management. This setting is required.</p> <p>Example:</p> <p>\\Contribution Folders\Production\Oracle Primavera\</p> <p>Note: The slash (\) at the end of the path is required.</p>		
Database/Instance[n]/Content Repository/Oracle Universal Content Management/Oracle Security Group	—	—
<p>The name of the Security Group for P6 EPPM documents, as specified in step 3 of Configuring Oracle Universal Content Management.</p>		

Database/Instance[n]/Content Repository/Oracle
Universal Content Management/Oracle Security Account

The name of the Security Account for P6 EPPM documents, as specified in step 5 of Configuring Oracle Universal Content Management. If the use of security accounts is not enabled in Universal Content Management, this setting should be left blank.

Database/Instance[n]/Content Repository/Oracle
Universal Content Management/Oracle Document Type

The Universal Content Management document type for P6 EPPM documents, which can be either an existing document type or a new one, as specified in step 6 of Configuring Oracle Universal Content Management. If the use of Document Types is enabled in Oracle Universal Content Management, this setting is required.

Database/Instance[n]/Content Repository/Oracle
Universal Content Management/Metadata Prefix

The prefix added to P6 EPPM metadata fields, as specified in step 7 of Configuring Oracle Universal Content Management.

Database/Instance[n]/Content Repository/Oracle
Universal Content Management/Admin User

A Universal Content Management user name with administrative privileges, as specified in step 4 of Configuring Oracle Universal Content Management. This setting is required.

Database/Instance[n]/Content Repository/Oracle
Universal Content Management/Authentication Mode

Multiple User

Single User,
 Multiple
User

The authentication mode used for access to the Universal Content Management server. Content repository functions will not be available to P6 EPPM users if these conditions are not met.

If "Multiple User" is chosen, all P6 EPPM content repository-related user names must match the equivalent Universal Content Management user name. For example, a P6 EPPM user named "Joe" must have an equivalent user named "Joe" in Universal Content Management. If "Single User" is chosen, the administrator user specified in the setting above must have access to all appropriate Security Groups in order to browse to documents outside of the P6 EPPM home folder.

Database/Instance[n]/Content Repository/Oracle
Universal Content Management/Autovue/VueLink URL http://localhost/idc/jsp/ —
autovue/csiApplet.jsp

The URL of the server hosting AutoVue VueLink.

Note: Refer to the Tested Configurations document for the version of AutoVue that is supported for use with P6.

Example format:

http://vuelinkpath/csiApplet.jsp

Database/Instance[n]/Content Repository/Oracle
Universal Content Management/Autovue/Enable false true/false


Set to true to enable the use of AutoVue.

Database/Instance[n]/Content
Repository/SharePoint/Login Name — —

A SharePoint user name with administrative privileges, this setting is required.

Database/Instance[n]/Content
Repository/SharePoint/Password — —

The password for the SharePoint login name.

Database/Instance[n]/Content
Repository/SharePoint/Authentication Mode Multiple User Single User,
 Multiple User

The mode used to connect to the SharePoint content repository database. Content repository functions will not be available to P6 EPPM users if these conditions are not met.

If "Multiple User" is chosen, all P6 EPPM content repository-related user names must match the equivalent SharePoint user name. For example, a P6 EPPM user named "Joe" must have an equivalent user named "Joe" in SharePoint.

If "Single User" is chosen, the administrator user specified in the setting above must have access to all appropriate SharePoint libraries in order to browse to documents outside of the P6 EPPM home folder.

Database/Instance[n]/Content
Repository/SharePoint/Host Name — —

The machine name or IP address of the SharePoint server.

Database/Instance[n]/Content
Repository/SharePoint/Domain — —

The domain in which the SharePoint server resides.

Database/Instance[n]/Content Repository/SharePoint/Document Library URL	—	—
<p>The URL of the P6 EPPM document library on SharePoint created in step 5 in Configuring Microsoft SharePoint. The URL includes the machine name (or IP address) of the content repository server and the path to the content repository library.</p> <p>Example format:</p> <p><i>http://host/library path</i></p>		
Database/Instance[n]/Content Repository/SharePoint/Web Service URL	—	—
<p>The URL of the Web Service used to connect P6 EPPM to SharePoint, as specified in step 4 in Configuring Microsoft SharePoint. The URL includes the machine name (or IP address) of the content repository server, port number of the server, and web service name.</p> <p>Example format:</p> <p><i>http://host:port/virtual_dir</i></p>		
Database/Instance[n]/Content Repository/SharePoint/External Document Library URL	—	—
<p>The URL of an external document library. This is only required if you need to connect to a non-P6 EPPM document library.</p> <p>Example format:</p> <p><i>http://host:port/virtual_dir</i></p>		
Database/Instance[n]/Content Repository/SharePoint/Autovue/VueLink URL	http://localhost/site/_la youts/1033/vue.aspx	—
<p>The URL of the of the server hosting AutoVue VueLink.</p> <p>Note: Refer to the Tested Configurations document for the version of AutoVue that is supported for use with P6.</p> <p>Example format:</p> <p><i>http://vuelinkpath/vue.aspx</i></p>		
Database/Instance[n]/Content Repository/SharePoint/Autovue/Enable	false	true/false
Set to true to enable the use of AutoVue.		
Database/Instance[n]/Session Settings/Setting 1-5	—	alter session set __ = __
<p>"Alter session" commands used to establish cursor sharing, rule-based mode, SQL trace, and more. Invalid settings in these fields are ignored.</p>		

Database/Instance[n]/Cost Based Optimization settings/Enable	false	true/false
If set to true, enables Cost Based Optimization.		
Database/Instance[n]/Cost Based Optimization settings/Dump Matching SQL	false	true/false
Set to true to dump the SQL where a match is found in the QUERYLIB table for a given SQL statement.		
Set to false to dump the SQL where a match is not found in the QUERYLIB table for a given SQL statement.		
You must set your logging level to INFO to see these entries.		
Database/Instance[n]/Eventing/Enabled	false	true/false
Set to true to enable the sending of events for P6, P6 Web Services, and P6 Integration API.		
Database/Instance[n]/Eventing/Interval	5m	1s-10m
The length of time that the Event Notification System uses to determine how often it sends events to the message queue. Specifying a smaller time increases the frequency with which the Event Notification System reports event occurrences to the message queue.		
Database/Instance[n]/Eventing/Max Queue Size	1000	10-5000
The amount of memory allocated to the queue for events. Once exceeded, events will be published immediately.		
Database/Instance/Eventing/Show Costs	false	true/false
Set to true to enable the display of cost fields in event notifications.		
Database/Instance[n]/Eventing/JMS Connection Factory	—	—
Specify the JNDI name of the JMS Connection Factory.		
Database/Instance[n]/Eventing/JMS Destination Name	—	—
Specify the JNDI name of the queue or topic where events are published.		

Database/Instance[n]/Eventing/JMS Destination Security Enabled	true	true/false
--	------	------------

Set to true to use the username and password specified when sending messages to JMS queue.

Database/Instance[n]/Eventing/JMS Destination Username	—	—
--	---	---

Specify the username to use when sending events to the specified JMS destination specified.

Database/Instance[n]/Eventing/JMS Destination Password	—	—
--	---	---

Specify the password to use when sending events to the JMS Destination specified.

Database/Instance[n]/Eventing/Configuration	—	—
---	---	---

Options for which Business Object changes and Special Operation processes trigger event notifications. Right-click to select the node, then choose Configure to select options. For detailed information about these options, refer to the document titled *Using Events with P6* located in the\Documentation\<language>\Technical_Documentation\Event_handling folder of the P6 EPPM physical media or download.

Note: The "Timesheet" business object only has update notification functionality.

Database/Instance[n]/AIA/Enabled	false	true/false
----------------------------------	-------	------------

Set to true to enable integration with AIA components. If set to true, you must set up a Datasource in WebLogic for your connection.

Database/Instance[n]/AIA/Datasource JNDI Name	AIA_ProjP6EPPM_DS
---	-------------------

Setup a datasource in Weblogic to connect to a direct JDBC URL.

Database/Instance[n]/AIA/Username	—	—
-----------------------------------	---	---

The database user name of the AQ queue owner.

Database/Instance[n]/AIA/Context Factory	weblogic.jndi.WLInitialContextFactory	—
--	---------------------------------------	---

Context Factory class for application server.

Database/Instance[n]/AIA/Queue Name	AIA_ProjP6EPPMJMS Queue	—
The name of the AQ queue receiving AIA messages.		
Database/Instance[n]/AIA/System Id	P6EPPM_01	—
The system identification code that AIA will use to identify P6 EPPM.		
Database/Instance[n]/AIA/Target System Id	—	—
The external system identification code that AIA will use to identify a supported Oracle ERP application. Examples: JDE-001 for JDEdwards EBS-001 for E-Business Suite		
Database/Instance[n]/BI Publisher/Server URL	—	—
The URL used to establish a connection to the BI Publisher web service from P6. Example format for WebLogic: <i>http://serverIP:port/BI Publisher domain/services/PublicReportService_v11</i> Example format for WebSphere: <i>http://serverIP:port/BI Publisher domain/services/PublicReportService_v11?WSDL</i>		
Database/Instance[n]/BI Publisher/Folder Paths	—	—
The paths to the BI Publisher folder where P6 will search for reports.		
Database/Instance[n]/BI Publisher/Admin Username	—	—
A BI Publisher web services user name with administrative privileges.		
Database/Instance[n]/BI Publisher/Password	—	—
The password for the administrative user name.		
Database/Instance[n]/BI Publisher/Personal Folders	false	true/false
Set to true to allow the use of BI Publisher personal folders.		
Database/Instance[n]/BI Publisher/Cache Timeout	Id	—
Set how long cached report definitions should appear.		

Database/Instance[n]/BPM Settings/Connector file location	—	—
The file path to the P6 BPM Connector JAR file.		
Database/Instance[n]/BPM Settings/BPM library path	—	—
BPM support library path.		
Database/Instance[n]/BPM Settings/BPM Configuration	—	—
BPM configuration. Right-click on BPM Configuration, then choose Configure to select options from the dialog box.		
For detailed information about these options, refer to the document titled <i>P6 Oracle BPM Integration Administrator's Guide</i> in the \Documentation\<language>\Technical_Documentation\Oracle_BPM folder of the P6 EPPM physical media or download.		
Note: For security guidance information, refer to BPM's documentation.		

Thread Pool Settings

Setting Name and Description	Default
Thread Pool/Number of Threads	25
The number of server threads.	
Thread Pool/Maximum Task Duration	3m
The maximum duration a thread can be used for one task.	
Thread Pool/Maximum Long Running Task Duration	5m
The maximum duration a thread can be used for a long running task.	
Thread Pool/Maintenance Frequency	45s
The frequency at which threads are checked for excess time durations.	

Log Settings

Setting Name and Description	Default	Valid Ranges/ Values
Log/Console Logger/Severity Level Log severity level for the Console Logger. The ranges are inclusive. For example, choose "debug" to log all messages; choose "warning" to log both warning and error level messages.	error	debug, info, warning, error
Log/Console Logger/Enabled Enable the Console Logger	false	true/false
Log/File Logger/Archive Size The minimum size (in Kb) a log file must be before it is archived.	1024	1024 - 2073600000
Log/File Logger/Severity Level Log severity level for the HTML Logger. The ranges are inclusive. For example, choose "debug" to log all messages; choose "warning" to log both warning and error level messages.	error	debug, info, warning, error
Log/File Logger/Number of Archive Files Maximum number of log files to be used. The default files are named WebAccessLog0.html through WebAccessLog5.html.	6	2 - 2073600000
Log/File Logger/HTML Log as HTML.	true	true/false
Log/File Logger/Enabled Enable the HTML Logger. Log files are created in a folder named WebAccessLogs, located as follows: WebLogic on Windows: <i>webaccesshome\WebAccessLogs</i> WebSphere on Windows: <i>webaccesshome\WebAccessLogs</i> WebSphere on Oracle Enterprise Linux: <i>/mount_point/WebSphere/AppServer/WebAccessLogs</i>	true	true/false
Log/Email Logger/SMTP Host SMTP server that will send the email message.	—	—

Log/Email Logger/From Email Address	—	—
Set to the email address from which you would like log messages sent.		
Log/Email Logger/To Email Address	—	—
Set to the email address to which you would like log messages sent.		
Log/Email Logger/Email Subject	P6 Web Access error	—
The subject line for error emails.		
Log/Email Logger/Enabled	false	true/false
Enable the Email logger.		
Log/Asynchronous	true	true/false
Log messages asynchronously for better performance.		

Directory Services Settings

Setting Name and Description	Default	Valid Ranges/Values
Directory Services/Provider URL	—	—
The URL of the JNDI provider used for eventing. Example: t3://localhost:7021		
Directory Services/Initial Context Factory	—	—
The class name of the initial context factory for the JNDI connection for eventing. Example: weblogic.jndi.WLInitialContextFactory		
Directory Services/Security Principal	—	—
Principal used to connect to the JNDI provider for eventing.		
Directory Services/Security Credentials	—	—
Credentials used to connect to the JNDI provider for eventing.		
Directory Services/Security Level	SIMPLE	NONE, SIMPLE, STRONG
Security level used to authenticate to the directory service for eventing.		

Directory Services/Lookup Name primavera —

The lookup used when testing the directory connection for eventing.

Application Settings

Setting Name and Description	Default	Valid Ranges/ Values
<p>Application/Prototype User</p> <p>Prototype user login used to create and store default Dashboards and global preferences for new P6 users. See Prototype User for P6 for details on how to create a prototype user.</p>	—	—
<p>Application/Ignore Daylight Savings Time</p> <p>Set to false to account for daylight savings time. This setting should match the equivalent setting in the P6 Progress Reporter Administrator if P6 and P6 Progress Reporter are deployed in the same domain.</p>	true	true/false
<p>Application/Internet Explorer Java Plugin URL</p> <p>URL for Internet Explorer users to download Java Plug-in (JRE).</p>	Defaults to the plug-in version (1.6.0_20) that is installed during setup.	—
<p>Application/FireFox Java Plugin URL</p> <p>URL for Firefox users to download Java Plug-in (JRE).</p>	Defaults to the plug-in version (1.6.0_20) that is installed during setup.	—
<p>Application/Internet Explorer Java Plugin Version</p> <p>JRE version used by applets in Internet Explorer.</p>	Defaults to the plug-in version (1.6.0_20) that is installed during setup.	—
<p>Application/FireFox Java Plugin Version</p> <p>JRE version used by applets in Firefox.</p>	Defaults to the plug-in version (1.6.0_20) that is installed during setup.	—

Application/Maximum Transactions for Excel Import of Resources	2000	100 - 2000
The maximum number of transactions (activities or resources) that can be imported at once from an .xls or .csv file		
Application/Maximum Excel Import File Size	1048	64 - 4096
The maximum size of the .xls or .csv file uploaded during an import attempt (KB)		
Application/Allow Auto-Summarize Option	true	true/false
Set to true to allow automatic summarization to be available in Resource Staffing user preferences.		
Application/Database Dropdown Key	—	—
Keyword to use for enabling database selection control in the login page. Pass this as a URL parameter db=keyword. Set this to an empty string if you do not want to require the keyword.		
Application/Logout URL	—	—
Directs P6 to a specific URL when the user exits with the Logout/Close icon in the banner of P6. Any valid URL can be used. If no URL is specified, P6 directs the user to the launch page of P6.		
Application/Compress Applet Communication	true	true/false
Set to true to compress communication between applets and the server.		
Application/Compress HTML Content	true	true/false
Set to true to compress HTML-related content generated by P6, including .html, .js, and css files, and Ajax content.		
Application/Filter Portfolio Stale Period	1d	0s - 24d20h31m23s647
Time period of inactivity that indicates a filtered portfolio should be refreshed.		
Application/Maximum Projects in Portfolio	1000	1 - 100000
The maximum number of projects returned when creating a portfolio with a filter.		
Application/Maximum Loaded Resource Planning Projects	100	1 - 1000
The maximum number of projects that can be opened in the Resource Planning spreadsheet.		

Application/Maximum Portlets per Dashboard	12	1 - 50
The maximum number of portlets that can be displayed in a dashboard on the Dashboards Home page.		
Application/Maximum Projects per Portfolio View	5000	1 - 20000
The maximum number of projects that can be displayed in a portfolio view on the Portfolio Analysis tab and in Portfolio View portlets on dashboards.		
Application/Maximum Activities per Activity View	5000	1 - 100000
The maximum number of activities that can be displayed in the Activities tab of the Projects section. If greater than 5000, the Maximum memory allocated to Java Applets setting (below) must be 128 or greater.		
Oracle recommends that the maximum value be set to 5000 (or lower) if users need to display Earned Value or Baseline-related information. Otherwise, database timeouts might occur.		
Application/Maximum Assignments per Assignment View	2000	1 - 15000
The maximum number of assignments that can appear in an assignment view.		
Application/Maximum Projects per EPS View	2000	1 - 15000
The maximum number of projects that can appear in an EPS view.		
Application/Maximum memory allocated to Java Applets	256	64 - 1024
The maximum amount of memory, in megabytes, that can be used by Java Applets. If the Maximum Activities per Activity View setting (above) is greater than 5000, the memory allocation must be set to 128 or greater.		
Application/Maximum MRU List Items	5	1-10
The maximum number of items that can be displayed in a Most Recently Used (MRU) list.		
Application/Maximum Project Activity Codes	350	1-350
The maximum number of projects that can be selected and displayed in the Projects tab of the Activity Codes section.		

Application/Maximum Activity Code Values	100000	1-1m
The maximum number of activity code values that can be created or selected per Activity Code.		
Application/Custom Portlet URL Encryption Key	—	—
Encryption key for custom portlet user password.		
Assigning a key causes the password that is passed as part of the URL for a custom portlet to be encrypted. If you do not assign a value, the password is not encrypted. The value can be any alphanumeric character or string of characters. This encryption uses the Sun/Blowfish algorithm.		
Application/Transaction Monitor Execution Interval	10m	1s - 24d20h31m2 3s647
The frequency at which the transaction monitor job runs, which ensures transactions have not been orphaned.		
Application/Enable Cross Site Scripting Filter	true	true/false
Enable or disable the Cross Site Scripting filter.		
Set to true to allow P6 EPPM to check for unsafe http requests from the browser and unsafe responses from P6, including requested documents. In general, requests and responses that contain Javascript, which was not generated explicitly by P6, are considered unsafe.		
An error message will be displayed for all unsafe page requests. For Internet Explorer 7, an attempt to download an unsafe document will result in an error message. For Internet Explorer 8 and Firefox, users will be prompted to download the document file instead of viewing the document directly in the P6browser.		
It is not necessary to restart the server after changing the value of this setting.		
Application/Notifications/Enable Issue Notifications	false	true/false
Enable or disable automated notifications when Issues are added or modified.		
Application/Notifications/Override Notification Email from User	false	true/false
Set to true to always use the system's From email address. Set to false to use the email address of the user who causes notifications to be sent, if their email address is configured.		
Application/Notifications/Notification from Email User	—	—
The email address from which Notifications will be sent when either NotificationsFromEmailOverride is true or the user's		

email address is not configured

Application/Contract Management Encryption Key

Encryption key for communication between P6 EPPM and Contract Management version 13. The default key is based on the string, "Oracle Primavera." Type a string of your choosing, and it will be converted to a UUID (Universally Unique Identifier). The UUID will be used for encrypting the password needed to connect to Contract Management. This encryption uses the Sun/Blowfish algorithm.

Note: If you change the encryption key value, you must also specify the same value in the Contract Management Administration Application.

Application/Help Server URL

http://localhost:7001/p6help

The URL used to launch P6 Help. Points to the location of the P6 Help file (p6help.war).

Note: The URL might be case-sensitive, depending on your application server configuration.

Example format:

http://server name:listen port/p6help

Application/Tutorials/Enable Tutorials

false

true/false

Set to true to allow tutorials to be available within P6 EPPM.

See the documentation included with Oracle UPK (User Productivity Kit) for details on In-Application Support.

Application/Tutorials/Tutorials URL

The URL used to launch UPK content. Points to the location of the UPK content file (P6Tutorials.war).

Note: The URL might be case-sensitive, depending on your application server configuration.

Example format:

http://server name:listen port/P6Tutorials

Services Settings

Setting Name and Description	Default	Valid Ranges/Values
Services/Enable All Services Allows you to enable or disable all services without having to set concurrent threads on each service. If set to true, the application will use the concurrent threads for all services. This is the recommended value if using the Summarize or Apply Actuals features in P6 Professional. If set to false, the application will treat the concurrent threads of services as equal to zero. When you set to false, the values for the threads will stay the same.	true	true/false
Services/Module Access Service/Update Rate The rate at which a Business Rule Engine synchronizes with the database for license counts.	30s	100 - 1m
Services/Module Access Service/Expiration Check Rate The rate at which licenses are checked to see if they should expire.	2m	500 - 15m
Services/Timestamp Service/Refresh Rate The rate at which the database is queried to determine if a table change notification is necessary.	1m	15s - 1h
Services/Registry Service/Refresh Rate The rate at which the database is updated with the status of the Business Rule Engine.	1m30s	15s - 1h
Services/Registry Service/Stale Period The duration of inactivity that indicates an inoperable Business Rule Engine.	4m	1m - 10m
Services/Registry Service/Port The TCP/IP port on which requests to revive dead Business Rule Engines will be received.	9192	1 - 65535
Services/Next Key Service/Refresh Rate The rate at which next key cache is refreshed.	1m	15s - 1h
Services/Next Key Service/Maximum Cached Keys Maximum next keys to cache per table	10	1 - 100

Services/Performance/Use Enterprise Summary	false	true/false
Use enterprise level summary data for resources and roles.		
This setting specifies whether you want to use EPS level records or Project level records to draw resource or role histograms. If true, performance is better because only one record (EPS record) is used for the histogram. If false, a much larger number of records (Project records) is used to draw the histogram chart, so performance is slower. However, it is important to note that histogram data is more accurate when the setting is false, using Project records.		
Services/Performance/Maximum Summary Node Count	1000	1-50000
The threshold for displaying summarized data in views such as Resource Usage and Resource Analysis. If the number of child elements contained in a node exceeds this number, no data is displayed.		
Services/Job Service Poll Rate	10s	1s-24d20h31m23s647
The rate at which the server polls the database for new Jobs to run.		
Services/ASAP Cleanup Rate	1d	1h-24d
The rate at which completed WebASAP jobs are removed from the database. Once the time is met all ASAP jobs that have a status other than running or delegated will be removed from the table automatically. Running and delegated jobs will be removed if they are older than the cleanup rate or if they are older than one day, whichever is greater.		
Note: Make sure that the cleanup rate is greater than your longest running job.		
Services/Scheduler/Interval	10s	1s - 24d20h31m23s647
Amount of time the Web Scheduler will wait before scheduling the next available job.		
Services/Scheduler/Concurrent Threads	2	0-20
The number of processes (active schedulers) used for scheduling on this server. A value of 0 (zero) indicates that scheduling will not be performed on this server.		

Services/Scheduler/Active Mode	true	true/false
If true, jobs are processed continuously until all jobs are scheduled. If false, each job is processed according to the Scheduling Interval.		
Services/Leveler/Interval	10s	1s - 24d20h31m23s647
Amount of time (in 1d1h1m1s format - specifying no letters implies milliseconds) the Web Leveler will wait before leveling the next available job.		
Services/Leveler/Concurrent Threads	2	0-20
The number of processes (active levelers) used for leveling on this server. A value of 0 (zero) indicates that leveling will not be performed on this server.		
Services/Leveler/Active Mode	true	true/false
If true, jobs are processed continuously until all jobs are leveled. If false, each job is processed according to the Leveling Interval.		
Services/Summarizer/Interval	10s	1s-24d20h31m23s647
Amount of time (in 1d1h1m1s format - specifying no letters implies milliseconds) the Summarizer will wait before summarizing the next available job.		
Services/Summarizer/Concurrent Threads	2	0-20
The number of processes (active summarizers) used for summarizing on this server. A value of 0 (zero) indicates that summarizing will not be performed on this server.		
Services/Summarizer/Active Mode	true	true/false
If true, jobs are processed continuously until all jobs are summarized. If false, each job is processed according to the Summarizing Interval.		
Services/Apply Actuals/Interval	10s	1s - 24d20h31m23s647
Amount of time (in 1d1h1m1s format - specifying no letters implies milliseconds) to wait before running the next available job.		
Services/Apply Actuals/Concurrent Threads	2	0-20
The number of processes used for this service on this server. A value of 0 (zero) indicates that this job will not be run on this server.		

Services/Apply Actuals/Active Mode	true	true/false
Process jobs continuously until all jobs are completed (true) or process each job according to Interval (false).		
Services/Store Period Performance/Interval	10s	1s - 24d20h31m23s647
Amount of time (in 1d1h1m1s format - specifying no letters implies milliseconds) the PeriodPerformance service will wait before running the next available job.		
Services/Store Period Performance/Concurrent Threads	2	0 - 20
The number of processes used for the PeriodPerformance service on this server. A value of 0 (zero) indicates that the service is not available on this server.		
Services/Store Period Performance/Active Mode	true	true/false
Process jobs continuously until all jobs are completed (true) or process each job according to the Interval (false).		
Services/Recalculate Assignment Cost/Interval	10s	1s-24d20h31m23s647
Amount of time (in 1d1h1m1s format - specifying no letters implies milliseconds) the RecalculateAssignmentCost service will wait before scheduling the next available job. When the RecalculateAssignmentCosts service is initiated from P6, it will attempt to run immediately but switch to running as a job service if it takes too long to start.		
Services/Recalculate Assignment Cost/Concurrent Threads	2	0-20
The number of processes used for theRecalculateAssignmentCost service on this server. A value of 0 (zero) indicates that the service is not available on this server.		
Services/Recalculate Assignment Cost/Active Mode	true	true/false
Process jobs continuously until all jobs are completed (true) or process each job according to Interval (false).		

Services/Sync Actual This Period/Enabled	true	true/false
Service for synchronizing actuals and ActualThisPeriod values. If true, recalculates actual units and costs for ThisPeriod.		
Services/Sync Actual This Period/Execution Interval	5m	1s - 24d20h31m23s647
Amount of time the service will wait before checking for any SyncActualThisPeriod jobs. The SyncActualThisPeriod service will poll the job service table, and the execution interval will determine when it starts.		
Services/Sync Actual This Period/ActivityThreshold	8000	1-2147483647
Determines if the SyncActualThisPeriod service will run simultaneously or as a job service. If the number of activities in a project is over the activity threshold, the SyncActualThisPeriod will run as a job service and add an entry to the job service table. The SyncActualThisPeriod service will poll the job service table, and the execution interval will determine when it starts. If the number of activities in a project is under the activity threshold, it will run immediately and will not add an entry to the job service table.		
Services/Sync Actual This Period/Concurrent Threads	2	0 - 20
The number of processes used for the SyncActualThisPeriod service on this server. A value of 0 (zero) indicates that the service is not available on this server.		
Services/Sync Remaining to Planned/Enabled	true	true/false
Set to false to disable the SyncRemainingtoPlanned service.		
Services/Sync Remaining to Planned/Execution Interval	5m	1s-24d20h31m23s647
Amount of time the service will wait before checking for any SyncRemainingtoPlanned jobs. The SyncRemainingtoPlanned service will poll the job service table, and the execution interval will determine when it starts.		

Services/Sync Remaining to Planned/Activity Threshold	8000	1-30000
<p>Determines if the SyncRemainingtoPlanned service will run simultaneously or as a job service. If the number of activities in a project is over the activity threshold, the SyncRemainingtoPlanned will run as a job service and add an entry to the job service table. The SyncRemainingtoPlanned service will poll the job service table, and the execution interval will determine when it starts. If the number of activities in a project is under the activity threshold, it will run immediately and will not add an entry to the job service table.</p>		
Services/Sync Remaining to Planned/Concurrent Threads	2	0-20
<p>The number of processes used for theSyncRemainingtoPlanned service on this server. A value of 0 (zero) indicates that the service is not available on this server.</p>		
Services/Sync Actuals with Duration % Complete/Enabled	true	true/false
<p>Set to false to disable the SyncActualswithDuration%Complete service.</p>		
Services/Sync Actuals with Duration % Complete/Execution Interval	5m	1s-24d20h31m23s647
<p>Amount of time the service will wait before checking for any SyncActualswithDuration%Complete jobs. The SyncActualswithDuration%Complete service will poll the job service table, and the execution interval will determine when it starts.</p>		

Services/Sync Actuals with Duration % Complete/Activity Threshold	8000	I-2147483647
<p>Determines if the SyncActualswithDuration%Complete service will run simultaneously or as a job service. If the number of activities in a project is over the activity threshold, the SyncActualswithDuration%Complete will run as a job service and add an entry to the job service table. The SyncActualswithDuration%Complete service will poll the job service table, and the execution interval will determine when it starts. If the number of activities in a project is under the activity threshold, it will run immediately and will not add an entry to the job service table.</p>		
Services/Sync Actuals with Duration % Complete/Concurrent Threads	2	0-20
<p>The number of processes used for theSyncActualswithDuration%Complete service on this server. A value of 0 (zero) indicates that the service is not available on this server.</p>		
Services/Project Hierarchy Cache/Cache Policy	PRR	FIFO, LRU, JVMM, PRR, PRFIFO, PRLRU, PRCC
<p>The cache policy to use. The cache policy determines how much data is in the cache and which data is removed to reclaim memory.</p> <p>The allowable values are:</p> <p>FIFO (First In First Out-projects are cleared from the cache in the same order they were added to memory)</p> <p>LRU (Least Recently Used projects are cleared from the cache before more recently used ones)</p> <p>JVMM (Java Virtual Machine Managed-uses soft references to cached elements; memory used by soft references is reclaimed by the JVM as required)</p> <p>PRR (Projects are selected at random to be cleared from cache)</p> <p>PRFIFO (Periodic Refresh First In First Out-same as FIFO, except policy is enforced based on MaintenanceFrequency)</p> <p>PRLRU (Periodic Refresh Least Recently Used-same as LRU, except policy is enforced based on MaintenanceFrequency)</p> <p>PRCC (Periodic Refresh Clear Cache-ignores CacheLimit to flush the entire cache, based on MaintenanceFrequency)</p>		

Services/Project Hierarchy Cache/Cache Limit	5000	1000 - 30000
The maximum number of projects stored in memory.		
Services/Project Hierarchy Cache/Maintenance Frequency	5h	1m - 24d
The frequency for applying the specified cache policy. Application of the cache policy might result in memory used by the cache to be reclaimed.		
Services/Collaboration Synchronization Service/Synchronization Interval	1h	1m - 24d20h31m23s647
The interval at which the collaboration synchronization service will run. The synchronization service deletes documents and workflows for projects that have been deleted.		
Services/Asynchronous Jobs/Purge Interval	1h	0 - 24d20h31m23s647
The frequency at which long running job records will be removed from the database.		
Services/Asynchronous Jobs/Grace Time	1d	0 - 24d20h31m23s647
The minimum age of long running job records removed during purge.		
Services/Mail Service/Email Server	—	—
Hostname or IP address of the email notification server for Timesheet Approval.		
Services/Mail Service/SMTP Port	25	1 - 65535
The tcp/ip port of the outgoing SMTP server.		
Services/Mail Service/Send Interval	1m	0 - 24d20h31m23s647
The frequency at which queued mail messages are sent.		
Services/Mail Service/Maximum Queue Length	250	0 - 2147483647
The maximum size of the mail message queue		
Services/Mail Service/Authorized User Name	—	—
The name of the account to use to send mail from this mail server.		
Services/Mail Service/Authorized User password	—	—
The password of the account used to send mail from		

this mail server.

Services/Indexer/Indexing Interval	30s	10s-1d
The frequency that the indexer is run to update global search indices.		
Services/Indexer/Indexing Batch size	1000	10-10000
The number of database records that are indexed at the same time.		
Services/Import/Export Options/Temporary File Location	—	—
The location to store the temporary file during the XML import/export process. If no location is specified, the temporary file is placed in the bootstrap home location, which is in the P6 home directory that was set during installation (for example, c:\p6home).		
Services/Import/Export Options/Maximum file size	102400	1024-2147483647
The maximum file size (in KB) for XML import/export. Limitations on this file size are determined by the JVM settings and available space in the Temporary File Location. Users might need to alter the memory settings in their application server if the import/export file size is greater than the maximum default file size.		
Services/Configuration Management/Configuration Capture Enabled	false	true/false
Allows P6 to collect configuration settings at the configured collection time.		
Services/Configuration Management/Automatic Capture Time	12AM	selection
The time of day that the settings will be captured on a daily basis. Note that the collection time in OCM (Oracle Configuration Management) should be set to occur at least a few minutes AFTER this capture time.		

Performance Monitor Settings

Setting Name and Description	Default	Valid Ranges/Values
Performance Monitor/Enabled Performance monitor packets are sent when true	false	true/false
Performance Monitor/Monitor Host The destination IP or machine name for the performance monitor packets	localhost	—
Performance Monitor/Monitor Port The destination port for the Performance Monitor packets	6990	1 - 65535
Performance Monitor/Update Interval The rate at which the performance monitor packets are sent.	1s	250 - 1m

Tracer Settings

Setting Name and Description	Default	Valid Ranges/Values
Tracer/Enabled If true, debugging messages are sent to Tracer application.	false	true/false
Tracer/Server Name Hostname or IP address of destination for sending tracer information.	localhost	—
Tracer/Port Port to use for Tracer socket connection	9210	1-65535
Tracer/Use Background Send Thread If true, use background thread for sending TCP messages to tracer.	true	true/false

Integration API Server Settings

Setting Name and Description	Default	Valid Ranges/Values
Integration API server/RMI/Registry Port The port for the RMI Registry. This value is usually set to at least 1024.	9099	1 - 65535
Integration API server/RMI/Enable The setting that enables the RMI server.	true	true/false
Integration API server/RMI/Enable Compression The setting that enables compression service mode.	true	true/false
Integration API server/RMI/Enable SSL The setting that enables SSL service mode.	true	true/false
Integration API server/RMI/Enable Standard Service The setting that enables Standard service mode.	true	true/false
Integration API server/RMI/Compression Service Port The port to use for Compression service mode. A setting of 0 indicates that any available port will be used. If the server will be accessed across a firewall, you must set this to a specific port.	0	0 - 65535
Integration API Server/RMI/SSL Service Port The port to use for SSL service mode. A setting of 0 indicates that any available port will be used. If the server will be accessed across a firewall, you must set this to a specific port.	0	0 - 65535
Integration API Server/RMI/Standard Service Port The port to use for Standard service mode. A setting of 0 indicates that any available port will be used. If the server will be accessed across a firewall, you must set this to a specific port.	0	0 - 65535
Integration API Server/Session Timeout The amount of time after which an idle client connection will be terminated.	120	1 - 24d

P6 Web Services Settings

Setting Name and Description	Default	Valid Ranges/Values
Web Services/Security/Authentication/Mode The method clients use for authentication.	Username Token Profile	Username Token Profile, SAML Token Profile, Cookies
Web Services/Security/Authentication/Username Token Profile/Nonce/Require Nonce Set to true to enable nonce.	true	true/false
Web Services/Security/Authentication/Username Token Profile/Nonce/Nonce Cache Timeout Specify a value, in seconds, for the Nonce cache timeout. The value specified indicates how long the nonce remains cached before it is expunged.	600	300-24d
Web Services/Security/Authentication/Username Token Profile/Created/Require Created Set to true to enable the Username token timestamp.	true	true/false
Web Services/Security/Authentication/Username Token Profile/Created/Timeout Specify a value, in seconds, for the timestamp (Created) timeout. You can specify a minimum of 300 seconds. If you do not specify a value, the default is 600 seconds.	600	300-24d
Web Services/Security/Authentication/SAML Token Profile/SAML Version The SAML version of the token.	1.1	1.1
Web Services/Security/Authentication/SAML Token Profile/Require Signed SAML Token Specify whether SAML tokens must be signed or unsigned.	true	true/false
Web Services/Security/Authentication/SAML Token Profile/SAML 1.1 Tokens/Issuer Set the valid issuer for the SAML token. Separate multiple valid issuers with a space.	http://your.saml.issuer.com	—

Web Services/Security/Authentication/SAML Token Profile/SAML 1.1 Tokens/IssueInstant Timeout	300	300-24d
Specify a value, in seconds, for the IssueInstant timeout. The value specified indicates the maximum time allowed between the time the token is issued and the time the token is received by the web service.		
Web Services/Security/Authentication/SAML Token Profile/SAML 1.1 Tokens/AuthenticationInstant Timeout	300	300-24d
Specify a value, in seconds, for the AuthenticationIssueInstant timeout. The value specified indicates the maximum time allowed between the time the user is authenticated and the time the token is received by the web service.		
Web Services/Security/Authentication/SAML Token Profile/Signed SAML tokens/KeyStore Type	JKS	JKS
Keystore type.		
Web Services/Security/Authentication/SAML Token Profile/Signed SAML tokens/File Location	c:\keystore\keystore.jks	—
Absolute path to the key store file. This file must exist on the local filesystem.		
Web Services/Security/Authentication/SAML Token Profile/Signed SAML tokens/Keystore Password	—	—
Keystore password.		
Web Services/Security/Authentication/SAML Token Profile/Signed SAML tokens/Certificate Alias	alias	—
Alias for the client certificate containing the public key.		
Web Services/Security/Message Protection/Require Timestamp	true	true/false
If set to true, incoming SOAP messages must contain the WS-Security Timestamp element.		

Web Services/Security/Message Protection/Require Digital Signatures for Incoming Messages true true/false

Set to true to require that incoming SOAP messages are signed and conform to Web Service Security 1.1 standards. If set to false, incoming SOAP messages must not be signed.

Note: To access Web Services, you must configure all Web Services settings to get encryption and digital signatures to work. If you do not want to use encryption or digital signatures, you must set this setting and the Require Encryption setting to false.

Web Services/Security/Message Protection/Require Encryption for Incoming Messages	true	true/false
---	------	------------

Set to true to require incoming SOAP messages are encrypted and conform to Web Service Security 1.1 standards. When this setting is true, at least one element in each P6 Web Services request message must be encrypted. If set to false, incoming SOAP messages must not be encrypted.

Notes:

To access Web Services, you must configure all Web Services settings to get encryption and digital signatures to work. If you do not want to use encryption or digital signatures, you must set this setting and the Require Encryption setting to false.

When the Encrypt Response setting and the Require Encryption for Incoming Messages setting are both set to true, the server encrypts everything inside of the body element of P6 Web Services response messages.

Web Services/Security/Message Protection/KeyStore Type	JKS	JKS
--	-----	-----

Specify the KeyStore Type.

Web Services/Security/Message Protection/File Location	c:\keystore\keystore.jks
--	--------------------------

Absolute path to key store file. This file must exist on the local filesystem.

Web Services/Security/Message Protection/KeyStore Password	—	—
--	---	---

Password for the KeyStore.

Web Services/Security/Message Protection/Private Key Alias alias

Alias for the private key in KeyStore.

Web Services/Security/Message Protection/Private Key Password — —

Password for the private key.

Web Services/Security/Message Protection/Encrypt Response true

Encrypt outgoing messages. This setting can be used only when encryption is enabled for incoming messages.

Note: When the Encrypt Response setting and the Require Encryption for Incoming Messages setting are both set to true, the server encrypts everything inside of the body element of P6 Web Services response messages.

Authentication Settings for P6 EPPM






The information below details all settings available from the Authentication tab of the P6 Administrator application.

Notes:

If you are upgrading from a previous version of P6 EPPM software, refer to the procedures in Automatic Database Upgrade before modifying the authentication settings.

See Authentication in P6 EPPM for an overview of the authentication configuration process and instructions on how to provision LDAP user information.

Authentication Settings





Setting Name and Description	Default	Valid Ranges/Values
Authentication/Login Mode Determines the page that will display for logging into P6. Must be set to the same value chosen for Authentication Mode for the database instance. For more information on this related setting, see Database instance Settings (on page 62).	NATIVE	NATIVE,  WebSSO,  LDAP
Authentication/Web Single Sign-On/User Name Header Key The name of the HTTP Header you specified in the policy server. The value you specify must match the property of the response you have created under the policy domain/realm, within which the Web server for P6 resides. For example, for Oracle Single Sign-On, the value of this response should be Proxy-Remote-User, where Proxy-Remote-User should match the LDAP server attribute that maps to the P6 EPPM database USER_Name field. For Oracle Access Manager, the value should be OAM_REMOTE_USER.	OAM-Remote-User	— 
Authentication/Web Single Sign-On/Context Path Override The path used to pass web requests from the Single Sign-On Web server to the P6 server. The default listed is the default value for P6.	/p6	— 
Authentication/Web Single Sign-On/Server and Port Override The fully qualified domain name and port for the Web server that the Single Sign-On server is controlling. Example format for Oracle Single Sign-On: http://server name.domain.com:7778 Example format for Oracle Access Manager: http://server name.domain.com:80	http://servername.domain.com:80	— 
Authentication/Web Single Sign-On/Allow Alternate Login Attribute Set to true when using Oracle Single Sign-On and you want to use an SSO login attribute other than the P6 user name. For example, you will enter your email address when	false	true/false

authenticating to Oracle Single Sign-on, but your P6 user name will map to the LDAP's UID field.



Notes:

If you enable the Allow Alternate Login Attribute setting, you must configure the Header Key and LDAP Search Attribute settings. You must also configure the LDAP settings for the appropriate database instance to establish a connection to the LDAP server.

If using P6 Progress Reporter, you must specify the Header Key and LDAP Search Attribute during the P6 Progress Reporter application server configuration. See P6 Progress Reporter Installation for details.

Authentication/Web Single Sign-On/Header Key	Osso-User-Guid		
The HTTP Header Key which contains the global user ID.			
Authentication/Web Single Sign-On/LDAP Search Attribute	orclguid		
The LDAP attribute searched by the Header Key to authenticate users.			
Note: You must configure the LDAP settings for the appropriate database instance to establish a connection to the LDAP server.			
Authentication/LDAP/SSL Certificate Store	—	—	
The full path to the keystore that holds the SSL certificate for the LDAP server.			
Authentication/LDAP/SSL Store Password	—	—	
The password for the keystore that holds the SSL certificate.			
Authentication/HTTPS/Enabled	true		true/false
Set to false to disable SSL redirect for login.			
Caution: If set to false, passwords will be passed to the database as clear text when logging into the application.			
Authentication/HTTPS/Port	443	0-2147483647	
The port number used for SSL.			

Database instance Settings

Setting Name and Description	Default	Valid Ranges/ Values
<p>Database instance/Authentication Mode</p> <p>The authentication method used for the database instance. Must be set to the same value chosen for Login Mode. For more information on this related setting, see Authentication Settings (on page 60).</p> <p>If Native or LDAP is selected, all P6 EPPM applications (with the exception of P6 Web Services) are set to that value. If SSO is selected, P6 and P6 Progress Reporter will be set to SSO and P6 Professional and P6 Integration API will be set to LDAP.</p>	Native	Native,  WebSSO,  LDAP
<p>Database instance/LDAP Connection Settings[n]/Host</p> <p>The connection string for the LDAP server.</p>	—	—
<p>Database instance/LDAP Connection Settings[n]/Port</p> <p>The port number for the LDAP server connection.</p>	636	0-2147483647
<p>Database instance/LDAP Connection Settings[n]/Username</p> <p>The name used to search the LDAP Base Directory Node. The username must be fully qualified (for example, uid=admin). The user must have rights to read the LDAP directory.</p> <p>LDAP username and password are optional when:</p> <ul style="list-style-type: none"> ▶ the installation is not using P6 Professional ▶ the SSO is selected as authentication mode ▶ the LDAP server allows anonymous logins (a prompt for user name and password when attempting to search) ▶ the LDAP is selected as authentication mode and admin does not want to store password in the AdminConfig blob; in this case, if not entered, admins will be prompted to enter LDAP username and password when provisioning users in P6 Web. 	—	—
<p>Database instance/LDAP Connection Settings[n]/Password</p> <p>The password of the name used to search the Base Directory Node.</p>	—	—

LDAP username and password are optional when:

- ▶ the installation is not using P6 Professional
- ▶ when SSO is selected as authentication mode
- ▶ when the LDAP server allows anonymous logins (a prompt for user name and password when attempting to search)
- ▶ when LDAP is selected as authentication mode and admin does not want to store password in the AdminConfig blob; in this case, if not entered, admins will be prompted to enter LDAP username and password when provisioning users in P6 Web.

Database instance/LDAP Connection Settings[n]/Enable SSL	true	true/false
--	------	------------

If set to false, will not connect to LDAP server using SSL. If true, you must populate the settings under the LDAP folder in **Authentication Settings** (on page 60).

Database instance/LDAP Connection Settings[n]/Chase Referrals	true	true/false
---	------	------------

Chasing Referrals allows authentication to extend to another domain. If set to false, searches will be performed only in the domain specified.

Referral chasing is supported with Oracle Internet Directory and Microsoft Windows Active Directory.

For Oracle Internet Directory, referrals chasing only works when the directories are configured to allow anonymous searches.

Database instance/LDAP Connection Settings[n]/Base Directory Node	—	—
---	---	---

Specifies the location in the directory information tree in which to start searches.

Database instance/LDAP Connection Settings[n]/Field Map/USER_NAME	samaccountname	—
---	----------------	---

The name of the LDAP directory field that maps to the P6 USER_NAME field. The LDAP field must be a unique identifier.

Database instance/LDAP Connection Settings[n]/Field Map/EMAIL_ADDR	mail	—
--	------	---

The name of the LDAP directory field that maps to the P6 EMAIL_ADDR field.

Database instance/LDAP Connection Settings[n]/Field name
Map/ACTUAL_NAME

—

The name of the LDAP directory field that maps to
the P6 ACTUAL_NAME field.

Database instance/LDAP Connection Settings[n]/Field telephoneNumber
Map/OFFICE_PHONE

—

The name of the LDAP directory field that maps to
the P6 OFFICE_PHONE field.

LDAP

This chapter describes the authentication modes available and explains how to configure the P6 EPPM to operate using a non-native authentication scheme.

In This Chapter

Authentication Modes.....	65
Implementing Non-Native Authentication.....	65
Choosing an Authentication Scheme	66
Using the Authentication Tab in the P6 Administrator application	66
Configuring P6 Integration API Authentication	68
Login Procedures and Authentication in P6 EPPM	68

Authentication Modes

The P6 Integration API provides support for the following authentication modes to validate user logins:

- ▶ **Native** authentication is the default mode for P6 EPPM. In this mode, when a user attempts to log into a P6 EPPM application, authentication is handled directly through the module with the P6 EPPM database acting as the authority.
- ▶ **LDAP** (Lightweight Directory Access Protocol) is directory-based authentication and is available for all P6 EPPM applications. In this mode, when a user attempts to log into a P6 EPPM application, the user's identity is confirmed in an LDAP-compliant directory server database. Additionally, P6 EPPM supports the use of LDAP referrals with Oracle Internet Directory and Microsoft Windows Active Directory. Referrals chasing allows authentication to extend to another domain.
- ▶ **Single Sign-On** authentication, which provides access control for Web applications, is available for P6 Progress Reporter and P6. In this mode, when a user attempts to log into a P6 EPPM application (protected resource), a Web agent intercepts the request and prompts the user for login credentials. The user's credentials are passed to a policy server and authenticated against a user data store. With Single Sign-On, a user logs on only once and is authenticated for all Web applications for the duration of the browser session (provided that all Web applications authenticate against the same policy server).

Implementing Non-Native Authentication

By default, all P6 EPPM applications are installed using native authentication. Native authentication is handled directly through the module application with the P6 EPPM database acting as the authority.

To implement non-native authentication for P6 EPPM applications:

- ▶ Uninstall current versions of P6 EPPM applications, if you are upgrading.
- ▶ Install the new version of P6 EPPM applications and additional components required for your implementation.

- ▶ Use the Authentication tab in the P6 Administrator application to choose an authentication scheme for the P6 EPPM database (PMDb).
- ▶ Configure administrative settings for the P6 Integration API.

This guide describes the procedures for choosing an authentication scheme and configuring new administrative settings for the P6 Integration API.

For detailed procedures on installing and uninstalling P6 EPPM applications and server components and upgrading the methodology manager database, refer to the *P6 EPPM Administrator's Guide*.

Choosing an Authentication Scheme

To specify the authentication scheme you want to use for P6 EPPM applications, use the P6 EPPM Authentication tab of the P6 Administrator application. Although you specify authentication modes for client/server applications and Web applications separately, you must use a consistent authentication scheme within the P6 EPPM. For example, client/server and Web applications must *both* be configured for either LDAP authentication or native authentication. For Custom mode, which is available only for client/server applications, you can choose LDAP for Web applications.

Authentication mode is database-driven, so the configuration utility enables you to first specify a database connection setting, then choose authentication modes for the applications that access that database.

For LDAP authentication, the configuration utility also enables you to specify LDAP servers, map LDAP attributes to P6 EPPM database fields, and provision users.

Using the Authentication Tab in the P6 Administrator application

Use the Authentication tab in the P6 Administrator application to:

- ▶ Select an authentication mode and configure LDAP servers.
- ▶ Provision LDAP user information to a P6 EPPM database.

To select an authentication mode and configure LDAP servers

Caution: Ensure that all users are logged out of P6 EPPM to avoid a reset of the P6 Administrator application settings.


Note: Verify which global profile is set as the default since this will be assigned to all provisioned users.

- 1) Log into the P6 Administrator application. See About the P6 Administrator application for details.
- 2) From the **Authentication** tab:
 - a. Fill in the appropriate settings under the **Authentication** folder, and make sure that **Login Mode** is set to **NATIVE**. See **Authentication Settings** (on page 60) for details.
 - b. Fill in the appropriate settings under the **Database instance**, and make sure that **Authentication Mode** is set to **NATIVE**. See **Database instance Settings** (on page 62) for details.
 - c. Click **Save Changes**.
- 3) Restart the application server instance.

Note: If you do not restart the application server instance, the settings will be restored to the previous configuration after the next step.

- 4) Log into P6 as a user with privileges to create a new user.
- 5) Follow the instructions in *Creating User Accounts for P6 EPPM* 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. See *Configuring Users in P6 EPPM* for details.
- 6) Log back into the P6 Administrator application.
- 7) From the **Authentication** tab:
 - a. Change **Login Mode** to **LDAP**.
 - b. Change **Authentication Mode** to **LDAP**.
 - c. Right-click the **LDAP Connection Settings** folder and select **Test Connection**.
 - d. Click **Save Changes**.
- 8) Restart the application server instance.

Note: If you do not restart the application server instance, the settings will be restored to the previous configuration after the next step.

- 9) Log into P6 as the LDAP user created in step 5.
 - a. On the **Users** page, click the  **Add** icon. The **Add Users from LDAP** dialog box appears for you to provision users from the LDAP repository:

Note: 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 an LDIF file.

1. Either click the **Load LDIF** button, or enter an LDAP query (for example, `uid=*`) under **Search users**. If a search was previously performed by a user with the privilege to search the LDAP directory, the last query entered by that user will appear.
2. If you clicked the Load LDIF button, browse to the location of the LDIF file, and click **Open**. If you entered an LDAP query, click **Search**.

Note: Depending on your P6 administrative configuration settings, you might be prompted to log into the LDAP server.

3. A list of users will appear, grouped by status. For example, LDAP repository users that do not exactly match P6 EPPM users will be grouped together. If users exist in the LDAP repository, the **User Name**, **Actual Name**, **E-mail**, and **Phone** fields are populated (if you previously mapped those fields through the P6 Administrator application settings).

Note: The User Name field is equivalent to the Login Name field in P6. The Actual Name field is equivalent to the Personal Name field.

4. Select the option next to each user account that you wish to import, or select the option in the fields bar to select all users. New and modified users are automatically selected.

5. Click **Import**.

Note: The new users will be assigned the default global profile.

Tip

When you provision users, changed records are updated in the P6 EPPM 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 EPPM database. You will need to manually delete these users.

Configuring P6 Integration API Authentication

Because one P6 Integration API server instance can control more than one database, in addition to specifying an authentication mode for a database through the Authentication tab of the P6 Administrator application, you use an administrative configuration setting to specify the overall mode you want to use for the P6 Integration API server. The P6 Integration API uses a single P6 EPPM configuration setting, `Authentication.Mode`, to support authentication selection. For LDAP authentication with secure communication (SSL) between the P6 Integration API server and the LDAP server, two additional configuration settings are required.

Use the P6 Administrator application to specify these configuration settings. For more information about the P6 Administrator application and these configuration settings, see ***Using the P6 Administrator application*** (on page 19).

Note: A P6 Integration API configuration might include database instances that are not set to the same authentication mode as the P6 Integration API server. If a user connects and requests a database that is set to a different authentication mode than the P6 Integration API server, an error message displays. The user must select a database that matches the authentication mode set for the P6 Integration API server.

Login Procedures and Authentication in P6 EPPM

Login procedures for P6 EPPM vary according to the authentication mode selected.

In Native mode

- ▶ P6 EPPM 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 EPPM applications (P6 Professional, P6 Progress Reporter, P6, 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 EPPM is disabled.

In Single Sign-On mode

- ▶ For P6 Progress Reporter, the Primavera P6 login dialog box never appears. Instead, login credentials are requested and validated by the Single Sign-On server. Once a user is authenticated, the P6 Progress Reporter launch page appears.
- ▶ For P6, login credentials are requested and validated by the Single Sign-On server. Once a user is authenticated, the launch page for P6 appears so the user can select a database and language.

The capability for users to change passwords within P6 EPPM is disabled because passwords are stored and authenticated against a directory server user store.