ORACLE®

PRIMAVERA

P6 EPPM Post Installation Administrator's Guide
Release 15.1

October 2015

Contents

About the P6 EPPM Post Installation Administrator's Guide

Post Installation and Administrator's Guide Once you have installed and configured your P6 EPPM applications, this guide will tell you how to begin using them. You should complete most of the tasks in this guide before you let your users work with these applications. These tasks include information about configuring your users and security settings and privileges, setting your Primavera P6 Administrator Administrator settings, and finalizing your P6 Team Member, P6 Integration API and P6 EPPM Web Services configurations.

P6 Setup Tasks

This chapter covers the tasks you should complete before you let other users work in P6, including:

- Setting a base currency. (You must set the base currency. You cannot change it once you begin using projects.)
- Adding users.
- Assigning security settings.

This section also has information about using and configuring settings in the Primavera P6 Administrator.

In This Section

Accessing P6 from Client Browsers

Use one of the following for information on accessing P6 from client browsers:

- ***Accessing P6 from Client Browsers using WebLogic*** (on page 13)
- ***Accessing P6 from Client Browsers using WebSphere*** (on page 14)

Accessing P6 from Client Browsers using WebLogic

To access P6 from Client Browsers using WebLogic:

1) Launch a supported browser.
2) Enter the URL using the structure,

   http://*serverIP*:*listenport*/*ContextRoot*/login

   where *listenport* is 7001 (if you manually deployed P6) or 8203 (if you used the wizard to deploy P6) by default and *ContextRoot* is p6 by default.

   Examples:

   http://*serverIP*:7001/p6/login

   http://*serverIP*:8203/p6/login

Tips

▸ HTTPS settings are available in the Primavera P6 Administrator. If you have set the HTTPS/Enabled setting to true, ensure that your application server or front-end Web server is listening on the specified HTTPS port. See **Configuring HTTPS Settings in the Primavera P6 Administrator** (on page 90) for more information on the HTTPS settings.

▸ To select the authentication mode for P6, use the Primavera P6 Administrator. See **About the Authentication Tab in the Primavera P6 Administrator** (on page 89) for information about authentication configuration settings.

▸ On the P6 login window, SSO users can choose to bypass the login window the next time by selecting the appropriate option. See **Configuring Application Settings in the Primavera P6 Administrator** (on page 49) for more information.

▸ You can modify the context root. For information about context root configuration, refer to your application server documentation. Also, URLs might be case-sensitive, depending on your application server configuration.

▸ See the *Planning Your P6 EPPM Implementation* guide for a list of supported application servers with version numbers.

▸ For a full list of tested configurations for P6, see the *Tested Configurations* document.

Accessing P6 from Client Browsers using WebSphere

To access P6 from Client Browsers using WebSphere:

1) Launch a supported browser.
2) Enter the URL using the structure,

   http://*serverIP*:*listenport*/*ContextRoot*/login

   where *listenport* is 9080 by default and *ContextRoot* is p6 by default.

   Example: http://*serverIP*:9080/p6/login

Tips

▶ HTTPS settings are available in the Primavera P6 Administrator. If you have set the HTTPS/Enabled setting to true, ensure that your application server or front-end Web server is listening on the specified HTTPS port. See **Configuring HTTPS Settings in the Primavera P6 Administrator** (on page 90) for more information on the HTTPS settings.

▶ To select the authentication mode for P6, use the Primavera P6 Administrator. See **About the Authentication Tab in the Primavera P6 Administrator** (on page 89) for information about authentication configuration settings.

▶ On the P6 login window, SSO users can choose to bypass the login window the next time by selecting the appropriate option. See **Configuring Application Settings in the Primavera P6 Administrator** (on page 49) for more information.

▶ You can modify the context root. For information about context root configuration, refer to your application server documentation. Also, URLs might be case-sensitive, depending on your application server configuration.

▶ See the *Planning Your P6 EPPM Implementation* guide for a list of supported application servers with version numbers.

▶ For a full list of tested configurations for P6, see the *Tested Configurations* document.

Precompiling P6

Although not required for P6, precompilation helps to reduce the amount of time it takes for users to load P6 pages for the first time. The following instructions apply to all application servers supported by P6 EPPM. You need to perform these instructions while the application server is running.

> **Note**: Your application server must be listening on a HTTP port (non-SSL) for the precompile utility to work. You can later disable the HTTP port after precompilation if you will be using only HTTPS.

To precompile P6:

1) Locate the precompile_utility folder. It will be in the location where you installed P6 EPPM. For example:
   ▸ For Windows, C:\P6EPPM_1\p6\precompile_utility
   ▸ For UNIX, /usr/P6EPPM_1/p6/precompile_utility
2) Run a command similar to the following:

   java -jar JSPPrecompile.jar -u baseURL -f inputfile

   where baseURL is the P6 URL and inputfile is the location of the P6 EAR file.

   > **Note**: The file path of the P6 EAR file cannot contain spaces.

   For example, the command should look similar to the following if you have a standard P6 installation on WebLogic:

   If you deployed P6 in WebLogic:

   ```
   java -jar JSPPrecompile.jar -u http://localhost:7001/p6 -f
   p6home/p6.ear
   ```

   where *p6home* is the location where you installed P6. For example, C:\P6EPPM_1\p6\p6.ear or /usr/P6EPPM_1/p6/p6.ear.

   If you used the P6 EPPM Configuration Wizard to deploy P6:

   ```
   java -jar JSPPrecompile.jar -u http://localhost:8203/p6 -f
   p6home/p6.ear
   ```

   where *p6home* is the location where you installed P6. For example, C:\P6EPPM_1\p6\p6.ear or /usr/P6EPPM_1/p6/p6.ear.

Application Server Plug-Ins for P6 EPPM

Application servers offer a variety of plug-ins that enable you to configure a front-end Web server other than the one provided with the application server. For procedures on configuring a Web server plug-in, refer to the application server's documentation.

About the Database Configuration Wizard for P6

The Database Configuration wizard enables you to change the database connection settings you specified when you installed P6.

The database you select during configuration stores one or more P6 EPPM configurations, each one specifying a set of parameters that determine how P6 operates. During configuration, you select an existing P6 EPPM configuration or create a new one. Later, you can use the Database Configuration wizard to select a different P6 EPPM configuration or create a new one.

> **Notes:**
>
> - After selecting a different P6 EPPM configuration or creating a new configuration, you must stop and restart the P6 application server for the changes to take effect.
> - You should protect the Database Configuration file (dbconfigpv) for security reasons. Depending on which method you used to protect the file, you might have to relocate the file to the production server to run the wizard after implementation. See "Files to Protect after Implementation" in the *P6 EPPM Security Guide*.

Changing Database Connection Settings for P6

To change database connection settings for P6:

1) Do one of the following:

   ▶ On Windows platforms, run **dbconfigpv.cmd** (located in the *p6home* directory that you specified when installing P6).

   ▶ On UNIX platforms, change to the *p6home* directory that you specified when installing P6, and **run dbconfigpv.sh**.

2) On the **Setup and Configuration of the Primavera P6 Database** dialog box, select the database type.

3) On the **Please enter the following information. . .** dialog box:

   a. Specify the database connection parameters. Type your database user name (for example, pubuser) and password, the database name, host address, and host port. The database name, host address, and host port are specific to your database installation. The Database Host Port field displays the default port for the database type you selected. You can edit this port.

   b. To use the SSL protocol to securely communicate between the P6 application server and the database server, select the SSL option. If you select the SSL option, you must specify an SSL-enabled port number in the Database Host Port field.

   > **Notes:**
   >
   > ▪ See the appropriate database server documentation and the My Oracle Support's Knowledge Articles for information on configuring SSL.
   >
   > ▪ Using the SSL protocol will impact database performance.

   c. Ensure that the Public Group ID is 1 for a standard configuration.

4) If there is an existing Primavera configuration, on the **The installer has detected. . .** dialog box, choose whether you want to use it, or create a new configuration.

   > **Note:** If you are upgrading from a previous version of P6 against the same database, choose the option to create a new configuration. This is necessary to accommodate newly added configuration settings.
   > See *About the Primavera P6 Administrator* (on page 21) for more information about configurations.

   If you have not created a Primavera configuration, the **The installer has detected. . .** dialog box does not appear and the installation process automatically creates a default configuration named Primavera P6 Configuration. You can edit the settings for this configuration through the Primavera P6 Administrator.

5) When the message displays to confirm that the database configuration has completed successfully, click **OK**.

6) On the **End of Installation** screen, click **Exit**.

Configuring Settings on Client Machines

Features, such as exporting to Excel and resolving null pointer exceptions, require additional configuration settings on client machines. Some settings are required for a feature to work, while others are only necessary under certain conditions. You must configure your settings on each client machine requiring access to the feature.

Configuring Browser Settings for Internet Explorer

Note: Before you begin, ensure you are using the supported version of Internet Explorer. See the *Tested Configurations* document for more information.

1) Open **Internet Explorer**.
2) Go to **Tools**, **Internet Options**.
3) In the **Internet Options** dialog box, select the **Security** tab:
   a. Select **Trusted sites**.
   b. Click **Sites**.
4) In the **Trusted sites** dialog box:
   a. Ensure the site in the **Add this website to the zone** field is correct. If not change it to the location for P6.
   b. Click **Add**.
   c. Click **Close**.
5) In the **Internet Options** dialog box:
   a. In the **Security level for this zone** section, click **Custom Level**.
   b. In the **Security Settings - Trusted Sites Zone** dialog box:
      1. In the **Reset custom settings** section, select **Medium**.
      2. In the **Run ActiveX controls and plug-ins** section, select **Enable**.
      3. In the **Script ActiveX marked safe for scripting** section, select **Enable**.
      4. In the **Downloads**, **File download** section, select **Enable**.
      5. In the **Downloads**, **Automatic prompting for file downloads** section, select **Enable**.
      6. In the **Miscellaneous**, **Submit non-encrypted form data** section, select **Enable**.
      7. In the **Scripting**, **Active scripting** section, select **Enable**.
      8. Click **Reset....**
      9. Click **Yes** when the warning appears.
      10. Click **OK** to return to the **Internet Options** dialog box.
   c. Select the **Privacy** tab:
      1. In the **Pop-up Blocker** section, deselect the **Turn on Pop-up Blocker** option.
      2. In the **Settings** section, click **Advanced**.
      3. In the **Advanced Privacy Settings** dialog box, deselect the **Overrride automatic cookie handling** option.
      4. Click **OK** to exit all dialog boxes.

6) From the **Windows Control Panel**, select **Java**.
7) Go to the **Advanced** tab:
    a. Expand **Java Plug-in**.
    b. Select the **Enable the next-generation Java Plug-in** option.

> **Note**: Depending on your Java version, this option may already be selected.

Configuring Browser Settings for Mozilla Firefox

> **Note**: Before you begin, ensure you are using the supported version of Mozilla Firefox. See the *Tested Configurations* document for more information.

1) Open **Mozilla Firefox**.
2) Go to **Tools**, **Options**.
3) In the **Options** dialog box:
    a. Select the **Security** tab.
    b. Select the **Warn me when sites try to install add-ons** option.
    c. Select the **Content** tab.
    d. Deselect the **Block pop-up windows** option.
    e. Click **OK** to save your options and close the dialog box.

Configuring Browser Settings for Safari

> **Note**: Before you begin, ensure you are using the supported version of Safari. See the *Tested Configurations* document for more information.

1) Open **Safari**.
2) From the **Settings** drop-down, select **Preferences**.
3) In the **General** dialog box, select **Security**.
4) In the **Web Content** section:
   a. Select the following:
      - **Enable Plug-ins**
      - **Enable Java**
      - **Enable JavaScript**
   b. Deselect **Block pop-up windows**.
5) Select **Advanced**.
6) Select **Press Tab to highlight each item on a webpage**.
7) Close the dialog box.

Tips:

If you're using Safari 7 or later, you must ensure you enable the Java plug-in for P6 to work:

1) From the **Settings** drop-down, select **Preferences**.
2) In the **General** dialog box, select **Security**.
3) In the **Java** section, select **Run in Unsafe Mode** for the P6 URL.

Configuring Client Machines to Export to Excel

If Internet Explorer is not configured properly, the dialog box may not open when you click on the link to export to Excel in P6. If this happens, you need to configure client machines to export to Excel:

1) From the **Windows Control Panel**, select **Internet Options**.
2) Go to the **Security** tab and click on **Trusted Sites**.
3) Click on the **Sites** button and add the application's URL to the zone.
4) Close the **Sites** window.
5) Click on the **Custom level** button.
6) Enable the **Automatic prompting for file downloads** setting.

About the Primavera P6 Administrator

As the system administrator, you can use the Primavera P6 Administrator to review, modify, add, and delete P6 EPPM configurations. P6 EPPM configurations are stored in the database that you specified when you installed P6. These configurations contain all of the settings used to run the application server for P6.

Caution:

- Only experienced administrators should use the Primavera P6 Administrator to modify configuration settings.
- Many of the defaults are set to maximize the performance of your database. You should change them only if you are certain a change is needed.

Launching the Primavera P6 Administrator

You can run the Primavera P6 Administrator locally or remotely through a browser. The installation for P6 sets the default URLs for remote access to the Primavera P6 Administrator. You can use the application server's configuration utility to change the listen port number and context root. After launching the Primavera P6 Administrator, you will need to enter an Admin Superuser name and password.

Launching the Primavera P6 Administrator Locally on Windows Platforms

To launch the Primavera P6 Administrator locally:

1) Go to the P6 home directory (for example, C:\P6EPPM_1\p6).
2) Run the **adminpv.cmd** script.
3) Login as the privileged database user (for example, privuser).

Launching the Primavera P6 Administrator Locally on UNIX Platforms

To launch the Primavera P6 Administrator locally on UNIX platforms:

1) Change to the *p6home* directory that you specified when installing P6.

   The path should look similar to the following:

   `'cd/path/to/p6home'`

   where *p6home* is the P6 home directory you set during installation (for example, /usr/P6EPPM_1/p6).
2) Run the **adminpv.sh** script.
3) Login as the privileged database user (for example, privuser).

Launching the Primavera P6 Administrator Remotely

To launch the Primavera P6 Administrator remotely:

1) Launch a supported browser.
2) Navigate to https://*server IP:listenport*/*ContextRoot*/admin.jsp

   where *serverIP:listenport* is the IP address and listen port for the P6 server, and *ContextRoot* is p6 by default.
3) Login as a user with Admin Superuser privileges.

> **Note:**
>
> - Only users with Admin Superuser privileges can login to the Primavera P6 Administrator remotely. If you are logged into P6 but do not have the appropriate privileges to edit settings in the Primavera P6 Administrator, you will be redirected to the P6 login page.
> - The Privileged database user (e.g., privuser) can still access the local Primavera P6 Administrator, but will not have access to the remote Primavera P6 Administrator.

Tips

To launch the Primavera P6 Administrator remotely on Windows platforms:

1) Go to **Start**, **Programs**, **P6 EPPM**, **Primavera P6 Administrator**.
2) Login as a user with Admin Superuser privileges.

Reviewing and Modifying Configurations for P6

The Primavera P6 Administrator presents configuration settings for your P6 EPPM applications. The Configurations and Authentication tabs display the current configurations and settings. The Log tab displays a history of configuration changes.

Tips

▸ To display brief setting descriptions for configuration and authentication settings, select **Show tool tips** in the **Configurations** tab. Position the mouse over a setting to read the popup description.

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

▸ Configurations highlighted in red are out of date. Oracle recommends that you update these configurations by right-clicking the outdated configuration and select **Update to latest version**.

▸ To find a setting quickly, you can use the search box below the Configurations, Authentication, and Log tabs. Clicking the search button or hitting enter will open every file with that setting name.

▸ If you create a new configuration, you need to click **Update to latest version** before changing your settings in the new configuration.

Changing a Setting in the Primavera P6 Administrator

To change a setting value:

1) Click the **Configurations** or **Authentication** tab to display a hierarchical view of the settings.
2) Expand the folders to display the setting.
3) Triple-click the setting name.

> **Note:** You can also press F2 to change to Edit mode.

4) Type a new value.
5) Click **Save Changes**.

Returning a Primavera P6 Administrator Setting to its Default Value

To return a setting to its default value:

1) Select the setting name.
2) Right-click on the setting name and choose **Revert to default value**.
3) Click **Save Changes**.

Adding Configurations to the Primavera P6 Administrator

Duplicate an existing configuration to create a new 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.
4) Click **OK**.
5) Edit settings as needed.
6) Click **Save Changes**.

Tips

▶ To create a new configuration based on factory default settings, right-click on Factory Defaults in the Configurations tab and choose Duplicate.

▶ If you create a new configuration, you need to click **Update to latest version** before changing your settings in the new configuration.

Adding Database Instances to a Configuration in the Primavera P6 Administrator

To add a new database instance to a configuration, duplicate an existing instance. To duplicate a database instance:

1) Select the folder representing the instance.
2) Right-click and choose **Duplicate**.
3) Enter a unique name for the new instance.
4) Edit settings as needed.
5) Click **Save Changes**.

Deleting Configurations and Database Instances for P6 in the Primavera P6 Administrator

To delete a configuration or database instance:

1) Select it.
2) Right-click and choose **Delete**.

Tips

▶ You cannot delete the Factory Defaults configuration. You can delete any custom configuration, but not all of them. You must always have 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.

▶ You can delete the database that you specified during the database configuration. If you do so, you will need to run the Database Configuration wizard again. See *About the Database Configuration Wizard for P6* (on page 16).

About the Configurations Tab in the Primavera P6 Administrator

Many of the settings in the configurations tab are already set for you. You should change them only if you are certain a change is needed.

Use the configurations tab to:

- ▶ Create new configurations.
- ▶ Delete configurations.
- ▶ Configure your settings for your applications.

Configuring Localization Settings

Your localization settings specify the language you see when you login to P6 and the country for server string constants. The Java application uses this setting to ensure all instances of P6 EPPM will use the same localization settings.

> **Note**:
>
> - The localization used by your operating system will have priority for the language used. The localization setting in P6 ensures P6 EPPM uses your preferred language if the JVM fails to recognize your operating system's localization settings.
> - If you change the localization of P6 on the login page, you will only change the language for your P6 user interface. It does not translate your data or change the convention followed by your region.

To set your language and country:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Localization**.
   a. In the **System Language** field, enter your language. The default is English (en).
   b. In the **System Country** field, enter your country. The default is the US.

Tips

Go to http://download.oracle.com/javase/1.5.0/docs/guide/intl/locale.doc.html or the *Tested Configurations* documentation for a list of supported languages and countries.

Configuring Session Management Settings

The Maximum Session Timeout setting is the maximum length of time that a user can connect to the application server, regardless of activity, before P6 EPPM times it out.

To set your session timeout:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Session Management**.
4) In **Maximum Session Timeout**, enter time a user session can remain open before it times out.

   The default is 1d.

   Enter anything from 1m-24d.

Configuring Database Instance Settings

You will use the database instance settings to specify information about your database, such as name, description, schema.

To set your database instance settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]**.
   a. In the **Name** field, enter the name of this database instance.

      > **Notes**:
      > - This determines how the database instance name will appear on the P6 login page.
      > - The name can be a maximum of 32 characters.

   b. In the **Description** field, enter a description of this database instance.

      > **Note**: The description can be a maximum of 128 characters.

   c. In the **Public Group ID** field, enter the database group ID of the privileged user account that will access the database.

      The default is 1.
   d. In the **User Name** field, enter the name used to establish a connection to the database.

      The default is pubuser, but if you created a custom Public User name, you should use your custom name.
   e. In the **Password** field, enter the Public User password used to establish a connection to the database.
   f. In the **Auto Start Services** field, choose **true** to automatically start all services for this database when the application server starts. When this is true, all job services with a Concurrent Threads setting greater than zero will start when the application server starts.

      Set to true if you will use the Summarize or Apply Actuals features in P6 Professional.

If set to false, you must manually log into the application before the services will start.

> **Note**: If you set **Auto Start Services** to false, job services will not start until someone logs into the application for the first time.

About Database Instance Settings

If you have more than one database instance for your configurations, you will see them all under the database folder for your configuration. You can configure these settings for a database instance:

- Database information, such as name, schema, and public group ID
- Driver Class and URL
- User Security
- Connection Pool
- Content Repository, such as Oracle WebCenter Content Core Capabilities (formerly Universal Content Management), Microsoft SharePoint, or custom
- Session Settings
- Cost Based Optimization settings
- Eventing
- AIA
- Fusion Projects
- BI Publisher
- BPM Settings

Configuring Driver Class and URL for Database Instance Settings

The Driver Class and URL settings are where you configure the Java class and database URL that will connect to P6 EPPM.

To set your Driver Class and URL settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/Driver Class & URL**.
   a. In the **Java Class** field, enter the database driver class used for communicating with the database. Your options are:
      - oracle.jdbc.driver.OracleDriver
      - com.microsoft.sqlserver.jdbc.SQLServerDriver
   b. In the **URL** field, enter the database URL used to establish a connection to the P6 EPPM database.
      Oracle example:
      jdbc:oracle:thin:@xxx:yyyy:zzzz
      Microsoft SQL Server example:
      jdbc:sqlserver://xxx:yyy;database=zzz;

Where:

x = IP address or hostname

y = database listen port

z = database name or SID

Notes:

- If you upgrade your database and this database connection gets disconnected, you can right-click on the **Driver Class & URL** node to reconfigure your database connection. When you right-click on the node, click **Configure** and the **Configure URL** dialog box will appear.

- You can also define a custom Oracle/MSSQL driver class from the **Configure URL** dialog box. The jar file for your custom driver class should exist in the application server classpath. Oracle recommends copying the driver jar file to the *weblogic_home*\user_projects\domains*your_domain*\lib file if you use WebLogic, or creating a shared lib reference if you use WebSphere.

Configuring User Security for Database Instance Settings

These settings let you specify how many times users can login before they are locked out and for how long the users will stay locked out. You can also specify whether to allow multiple user or single machine sessions.

To set your database instance settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/User Security**.
   a. In the **Log Login Attempts** field, choose whether login attempts to P6 are tracked in the logs. You can choose to log the following:
      - None
      - Failed Attempts
      - Successful Attempts
      - All
   b. In the **Login Lockout Count** field, enter the number of times a user can attempt to login before the account locks.

      The default is 5.

      Enter anything from 0-100000.

Notes:

- A setting of "0" allows an unlimited number of attempts.
- The count resets after each successful login.

---

   c. In the **Login Lockout Duration** field, enter the length of time that a user is blocked from logging into P6; starts when the user exceeds the Login Lockout Count.

The default is 1h.

Enter anything from 0-24d.

> **Note**: The Admin Superuser can override this setting if they manually reset a user's session. See *Resetting User Sessions* (on page 144) for more information.

d. In the **Allow Multiple User Sessions** field, choose whether a single user can simultaneously log into P6 on different machines.

The default is Yes.

You can choose one of the following:

- Selecting "Yes" allows a single user to log in multiple times on the same machine or different machines.

> **Notes**: The following restrictions apply when you select "Yes" for multiple user sessions:
>
> - Users must use Microsoft Internet Explorer 8 or higher when logging in more than once on the same machine.
> - If you want users to log in multiple times on the same machine (either with the same user name or with different user names), you must set the **Allow Multiple User Sessions** setting to **Yes**. The other settings will not allow the user to login multiple times.
> - When you create a second Internet Explorer Session you must either: (1) Launch an **InPrivate** session by selecting **Tools, InPrivate Browsing** from the IE menu; or (2) Run a new browser session from your first browser session by selecting **File**, **New Session**.

- Selecting "No" allows a single user to log in only once with the same user name. If the user tries to login again while another session is active, the login will fail. A session can still be active if the user has closed the browser without logging out of P6. The user will have to wait until the session resets before they can login again.
- Selecting "Single Machine" allows a user to log in once on a machine. The user can login again on the same machine if they close their browser without logging out; they will not have to wait for the session to reset. If they close their browser without logging out, they can immediately login again on the same machine they were using; the user won't be able to login on a different machine unless they wait for the session to reset.

Configuring Connection Pool for Database Instance Settings

The connection pools create and open database connections when they are first needed. When you start the P6 EPPM server, it will allocate one or two connections for initialization routines. The server will allocate and open more connections when the pool cannot satisfy requests from the current pool. You can set the connection pool settings for:

▶ **Regular** Used for the regular connection pool. Regular is the most used connection pool and has 90%+ of database access.

▶ **Long Running** Used for the long running connection pool. Use this connection pool for services that will run for a long time.

▶ **Transactional** Used for the transactional connection pool. Use this connection pool when you have several types of objects saved at one time.

> **Note**: Gantt applets will use the Regular pool when loading data and the Transactional pool when creating or updating data.

A P6 EPPM application operation requires a database connection, so it asks the connection pool for a database connection. If the connection pool contains a connection that is not currently leased, it returns that connection. If it doesn't have a connection available it will check to see if its current allocated count is below 50 (which is the default in the Maximum Connections setting). If the count is below 50, it will create a new database connection and open it, put it in the pool, and return it to the caller. The caller uses the connection, then releases it when they end the session.

If the pool could not allocate a connection because all 50 connections were leased, it will keep checking for the next 30 seconds (which is the default in the Lease Request Wait Timeout setting). If a connection becomes available within that 30 seconds, it will return that connection. If a connection does not become available, it will log the following error: "Error: Lease request timeout while waiting for a connection to become available. Database <dbname>" and the caller will have to try again at a later time.

To set your connection pool settings:

> **Note**: The defaults will provide optimal performance in most environments. Change them only if you are certain a change is needed. Contact My Oracle Support for more information.

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/Connection Pool[aaa]**.
   a. In the **Resize Rate** field, enter the timeout period when the system will close all of its unused connections. For example, if the resize rate is 4 minutes, then every 4 minutes the connection pool will attempt to close all of its unused connections.

   The default is 4m.

   Enter anything from 4m-12h.
   b. In the **Maintenance Frequency** field, enter how often maintenance will run to ensure leases have not exceeded the maximum duration.

   The default is 1m.

   Enter anything from 10s-1h.

c. In the **Lease Request Wait Timeout** field, enter the amount of time a request for a database connection will wait before timing out.

If a request for a database connection times out, the user can reload the page and attempt to connect to the database again.

The default is 30s.

Enter anything from 5s-2h.

d. In the **Maximum Connections** field, enter the maximum number of connections the server will have to the database.

The default for Regular and Transactional is 50 and the default for Long Running is 100.

Enter anything from 5-15000.

e. In the **Fetch Size** field, enter how many rows to pull from the database and send to the application server.

The default is 120.

f. In the **Trace SQL** field, choose true to trace all SQL sent to the database.

The default is false.

g. In the **Renewable Free Limit** field, enter the minimum number of connections that leases need to be renewed.

The default is 3.

You can enter anything from 3-5.

h. In the **Renewable Leases** field, choose **true** if you want connection leases 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 finish 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.

Choose **false** if you want each connection to be leased only for the MaxLeaseDuration period.

The default for Regular is false. The default for Long Running and Transactional is true.

i. In the **Maximum Lease Durations** field, enter the maximum time a database connection can be leased before it is revoked.

The default for Regular is 2m, with a range of 5s-4h.

The default for Long Running is 15m, with a range of 5s-6h.

> **Note**: During the summarization process, queries may take a long time to execute if the project has a high number of WBS nodes. If you receive timeout errors, set your Long Running maximum lease duration to at least 30 minutes.

The default for Transactional is 10m, with a range of 5s-6h.

Configuring Oracle Webcenter Content Core Capabilities Database Settings

Use the following:

▶ ***Configuring Oracle Webcenter Content Core Capabilities (WCCC) in the Database Instance Settings*** (on page 33)

> *Configuring Oracle Webcenter Content Core Capabilities (WCCC) in the Database Instance Settings*

To set your WCCC settings:

> **Note**: Ensure the settings you entered in when you configured the content repository match the settings you enter below.

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/Content Repository**.
4) In the **Type** field, choose **Oracle**.
5) In the **Maximum document size** field, enter the maximum size for documents that can be uploaded to P6. The default is 10240 KB. You can enter anything from 0-1048576 KB.
6) Expand **Database/Instance[n]/Content Repository/Oracle Webcenter Content Core Capabilities**.
7) In the **Host** field, enter the machine name or IP address of the content repository server.
8) In the **Port** field, enter the IntradocServerPort number of the content repository server. By default, this is 4444.
   a. Go to *WCCC_Home*`\ucm\cs\config\`.
   b. Edit the **config.cfg** file.
   c. Find the IntradocServerPort line, which contains the port number.
9) In the **Oracle Home** field, enter the location of the framework or Folder_G folder.

   For example:

   /Production/Oracle Primavera
10) In the **Oracle Security Group** field, enter the name of the Security Group assigned to the document folder created in WebCenter for P6 EPPM documents, as specified when you configured the content repository.
11) In the **Oracle Security Account** field, enter the name of the Security Account for P6 EPPM documents, as specified when you configured the content repository.

   If you did not enable security accounts, leave this setting blank.
12) In the **Oracle Document Type** field, enter the document type for P6 EPPM documents, which can be either an existing document type or a new one, as specified when you configured the content repository. If you enabled Document Types, you must configure this setting.

   For example:

   Enter the Document Type as Document.
13) In the **Metadata Prefix** field, enter the prefix added to P6 EPPM metadata fields, as specified when you configured the content repository.

14) In the **Admin User** field, enter the user name with administrative privileges, as specified when you configured the content repository. This setting is required.

15) In the **Authentication Mode** field, enter authentication mode used to access the content repository server. P6 EPPM users cannot access content repository functions if you do not configure this setting.

16) If you choose "Multiple User", all P6 EPPM content repository-related user names must match the equivalent content repository user name. For example, a P6 EPPM user named "Joe" must have an equivalent user named "Joe" in the content repository.If you choose "Single User", the administrative user specified in the setting above must have access to all appropriate Security Groups to browse to documents outside of the P6 EPPM home folder.

17) Expand **Autovue**.

18) In the **VueLink URL** field, enter the URL of the server hosting AutoVue VueLink. The default is `http://localhost/idc/jsp/autovue/csiApplet.jsp`.

> **Note**: Do not put a / at the end of the URL.

19) In the **Enable** field, choose **true** to enable Autovue. Choose **false** to disable it. The default is set to false.

20) Restart the P6 Server.

Configuring Microsoft SharePoint in the Database Instance Settings

To set your SharePoint settings:

> **Note**: Ensure the settings you entered in Configuring Microsoft SharePoint to Work with P6 match the settings you enter below.

1) Open the Primavera P6 Administrator.

2) In the **Configurations** tab, expand your configuration.

3) Expand **Database/Instance[n]/Content Repository**.

4) In the **Type** field, choose **SharePoint**.

5) In the **Maximum document size** field, enter the maximum size for documents that can be uploaded to P6. The default is 10240 KB. You can enter anything from 0-1048576 KB.

6) Expand **Database/Instance[n]/Content Repository/SharePoint**.

7) In the **Login Name** field, enter a SharePoint user name with administrative privileges.

> **Note**: You do not need to include your domain. You just need your user name.

8) In the **Password** field, enter the password for the SharePoint login name.

9) In the **Authentication Mode** field, select the mode used to connect to the SharePoint content repository database. P6 EPPM users cannot access content repository functions if you do not configure this setting.

If you choose "Multiple User", 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 you choose "Single User", the administrative user specified in the setting above must have access to all appropriate SharePoint libraries to browse to documents outside of the P6 EPPM home folder.

10) In the **Host Name** field, enter the machine name or IP address of the SharePoint server.

11) In the **Domain** field, enter the domain where the SharePoint server resides.

12) In the **Document Library URL** field, enter the URL of the P6 EPPM document library on SharePoint that you created when you configured SharePoint. The URL includes the machine name (or IP address) of the content repository server and the path to the content repository library.

Example format:

http://*<hostname>:<port>/<domain>/<doclib>*

> **Note**:
> - Do not put a / at the end of the URL.
> - Ensure there are no spaces in the URL.

13) In the **Web Service URL** field, enter the URL of the Web Service used to connect P6 EPPM to SharePoint, as specified when you configured SharePoint. The URL includes the machine name (or IP address) of the content repository server, port number of the server, and web service name.

Example format:

http://*<hostname>:<port>/WS_FPRPC*

> **Note**: Do not put a / at the end of the URL.

14) In the **External Document Library URL** field, enter the URL of an external document library. If you need to connect to a non-P6 EPPM document library, you must configure this setting.

Example format:

http://*<hostname>:<port>/<extdoclib>*

15) Expand **Autovue**.

16) In the **VueLink URL** field, enter the URL of the server hosting AutoVue VueLink. The default is `http://localhost/idc/jsp/autovue/csiApplet.jsp`.

> **Note**: Do not put a / at the end of the URL.

17) In the **Enable** field, choose **true** to enable Autovue. Choose **false** to disable it.The default is set to false.

18) Restart the P6 server.

Configuring CMIS-Compliant Content Repository in the Database Instance Settings

To configure your CMIS-compliant content repository:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/Content Repository**.
4) In the **Type** field, choose **CMIS**.
5) In the **Maximum document size** field, enter the maximum size for documents that can be uploaded to P6. The default is 10240 KB. You can enter anything from 0-1048576 KB.
6) Expand **Database/Instance[n]/Content Repository/CMIS**.
7) In the **Login Name** field, enter the user name for your content repository.
8) In the **Password** field, enter the password for the user name you entered above.
9) In the **Authentication Mode** field, enter authentication mode used to access the content repository server. P6 EPPM users cannot access content repository functions if you do not configure this setting.

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

   If you choose "Single User", the administrative user specified in the setting above must have access to all appropriate Security Groups to browse to documents outside of the P6 EPPM home folder.
10) In the **Repository Name** field, enter the name for your content repository.
11) In the **Document Home** field, enter the location of your documentation home where you want to store P6 documents.
12) In the **Web Service URL** field, enter the URL for your web services home.
13) Expand **Autovue**.
14) In the **VueLink URL** field, enter the URL of the server hosting AutoVue VueLink. The default is `http://localhost/idc/jsp/autovue/csiApplet.jsp`.

   > **Note**: Do not put a / at the end of the URL.

15) In the **Enable** field, choose **true** to enable Autovue. Choose **false** to disable it.The default is set to false.
16) Restart the P6 server.

Configuring the Oracle Database Content Repository

To configure the Oracle database as your content repository:

1) Open the Primavera P6 Administrator.

2) In the **Configurations** tab, expand your configuration.

3) Expand **Database/Instance[n]/Content Repository**.

4) In the **Type** field, choose **Oracle Database**.

   This option will save documents and associated information in the P6 database schema. This option is only applicable if you are using an Oracle database on-premises.

5) In the **Maximum document size** field, enter the maximum size for documents that can be uploaded to P6. The default is 10240 KB. You can enter anything from 0-1048576 KB.

6) Restart the P6 server.

Configuring Session Settings in the Database Instance Settings

The session settings allow you to issue database statements to customize the database environment when the connections are created. You need to set these settings only if you have a customization you need to apply to a database environment.

To set your session settings:

1) Open the Primavera P6 Administrator.

2) In the **Configurations** tab, expand your configuration.

3) Expand **Database/Instance[n]/Session Settings**.

4) In the **Setting [n]** field, enter the commands used to establish cursor sharing, rule-based mode, SQL trace, and more when database connections are created. Invalid settings in these fields are ignored. You can create five session settings.

   Oracle Example:

   alter session set _ = _

   Microsoft SQL Server Example:

   SET TRANSACTION ISOLATION LEVEL READ UNCOMMITTED

Configuring Cost Based Optimization Settings in the Database Instance Settings

The cost based optimization settings will enable you to manipulate base SQL queries based on optimization statistics.

> **Caution:** Do not alter these settings unless you are familiar with cost based optimization. Contact My Oracle Support for more information.

To set your cost based optimization settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/Cost Based Optimization settings**.
   a. In the **Enable** field, choose **true** to enable Cost Based Optimization. Choose **false** to disable it.
   b. In the **Dump Matching SQL** field, choose **true** to dump the SQL where a match is found in the QUERYLIB table for a given SQL statement.

   Choose **false** to dump the SQL where a match is not found in the QUERYLIB table for a given SQL statement.

> **Note**: To see these entries, you must set your logging level to INFO in *Configuring Log Settings* (on page 44).

Configuring Eventing in the Database Instance Settings

Depending on your administrative settings, you can use P6, P6 EPPM Web Services, or P6 Integration API to update or create objects and trigger events 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 in the *Using Events With P6* document to work with your Java Messaging Service (JMS), the application server, and P6 EPPM.

> **Note**: Add the JMS vendor jar files to the application classpath. Refer to the My Oracle Support's Knowledge Articles for additional information and examples.

To set your eventing settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/Eventing**.

   a. In the **Enable** field, choose **true** to enable sending events for P6, P6 EPPM Web Services, and P6 Integration API. Choose **false** to disable sending events.

   The default is false.

   b. In the **Interval** field, enter 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 that the Event Notification System reports events to the message queue.

   The default is 5m.

   Enter anything from 1s-10m.

   c. In the **Max Queue Size** field, enter the amount of memory allocated to the queue for events. Once exceeded, events will publish immediately.

   The default is 1000.

   Enter anything from 10-5000.

   d. In the **Show Costs** field, choose **true** to enable the display of cost fields in event notifications. Choose **false** to disable the display.

   The default is false.

   e. In the **JMS Connection Factory** field, enter the JNDI name of the JMS Connection Factory.

   f. In the **JMS Destination Name** field, enter the JNDI name of the queue or topic where events publish.

   g. In the **JMS Destination Security Enabled** field, choose **true** to use the username and password specified when sending messages to JMS queue. Choose **false** if you do not want to enable security.

   The default is true.

   h. In the **JMS Destination Username** field, enter the username to use when sending events to the specified JMS destination.

   i. In the **JMS Destination Password** field, enter the password to use when sending events to the JMS Destination specified.

j. In the **Configuration** field, enter the options for Business Object changes and Special Operation processes that trigger event notifications.

1. Right-click to select the node.

2. Choose **Configure** to select the options. For detailed information about these options, see the *Using Events with P6* document.

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

4) To finish configuring the eventing services, go to ***Configuring Directory Services Settings*** (on page 46) and complete the steps in that section.

Configuring AIA in the Database Instance Settings

Use the AIA settings to configure Oracle Application Integration.

To set your AIA settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/AIA**.

a. In the **Enabled** field, choose **true** to enable P6 EPPM to integrate with AIA components or **false** to disable integration. If set to true, you must set up a Datasource in WebLogic for your connection (see the WebLogic documentation for more information).
The default is false.

b. In the **Datasource JNDI Name** field, enter the datasource from WebLogic to connect to a direct JDBC URL.
The default is AIA_ProjP6EPPM_DS.

c. In the **Username** field, enter the database user name of the Advanced Queues (AQ) owner.

d. In the **Context Factory** field, enter the Context Factory class for the application server.
The default is weblogic.jndi.WLInitialContextFactory.

e. In the **Queue Name** field, enter the name of the AQ queue receiving AIA messages.
The default is AIA_ProjP6EPPMJMSQueue.

f. In the **System Id** field, enter the system identification code that AIA will use to identify P6 EPPM.
The default is P6EPPM_01.

g. In the **Target System Id** field, enter the external system code that AIA will use to identify a supported Oracle Enterprise Resource Planning (ERP) application.
Examples:
JDE-001 for JDEdwards
EBS-001 for E-Business Suite

Configuring Fusion Projects Settings in the Database Instance Settings

Use the fusion projects settings to configure P6 to use Fusion PPM Bridge

To set your fusion project settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/Fusion Projects**.
    a. In the **URL** field, enter the WDSL URL for connecting to the Fusion PPM Bridge instance and web services definition (WDSL).

       Example format: *http://serverIP:port number/context URL/web service definition*

       Example:
       http://fusionserverexample:6124/soa-infra/services/default/PjgTopProjectIntegrationComposite/ProjectIntegrationService?wsdl
    b. In the **UserName** field, enter the Fusion PPM Bridge Integration Gateway User ID specified in the *Oracle Fusion Applications Administrator's Guide*.

       > **Note:** The Fusion PPM Bridge Integration Gateway User ID is the only user name that can activate the integration.

    c. In the **Password** field, enter the password for the user to connect to Fusion PPM Bridge.
    d. In the **Integration Id** field, enter your Fusion Integration ID.
    e. In the **Schema Version** field, enter version (for example, v1) for the Fusion Schema.

Configuring BI Publisher in the Primavera P6 Administrator

To set your BI Publisher settings for BI Publisher to work with P6:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/BI Publisher**.
4) In the **Server URL** field, enter the URL used to connect to the BI Publisher web service to P6. For
   example, `http://serverIP:port/xmlpserver/services/PublicReportService?WSDL`
5) In the **Version** field, enter the version of BI Publisher (11.1.1.7.x) that you want to integrate with P6.
6) In the **Folder Paths** field, enter the relative path to the BI Publisher P6 reports folder where P6 will search for reports.
   Example format (the forward slash is required):
   /P6REPORTS

> **Notes**:
>
> - You can find the relative path (for example,   /P6Reports) in the following folder:
> - For
>   11g, `%weblogic_home%\user_projects\domains\bifoundation_domain\config\bipublisher\repository\Reports`

7) In the **Admin Username** field, enter a BI Publisher web services user name with administrative privileges (for example, PxRptUser).
8) In the **Password** field, enter the password for the administrative user name.
9) In the **From Address for Email** field, enter the email address that you want users to see if they choose to receive reports by email.
10) In the **Personal Folders** field, select the option (true) to enable personal folders per user. If you do not want to use personal folders, leave the option clear. Users have their own personal folders where they can store their objects. Only the user who created and saved the content in the folder can access the folder.
11) In the **Scrub Username** field, select the option (true) to enable the setting or leave it clear (false) to ensure it's disabled.

    This setting controls whether special characters (non-alphanumeric) are removed from the user name when connecting to BI Publisher. The default is 'false,' meaning special characters will not be removed.

    If you are using the P6 EPPM Extended Schema for BI Publisher reporting, leave the setting as false.

    If you are using the P6 ODS Schema for BI Publisher reporting, change the setting to true. Setting the value to true will allow the user's security context (user name) to format properly before it goes to BI Publisher. This allows reporting queries to perform against the ODS tables.
12) In the **Cache Timeout** field, enter how long cached report definitions should appear.

The default is 1d.

Configuring P6 to Connect to Oracle BPM

To connect P6 and BPM 11g:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/BPM Settings**.
4) In the **Connector file location** field, enter the full path (including the file name) where you copied the connector files.

   For example:

   c:/oracle/bpm1111x/eppmjars/prm-bpm-connector-11.1.1.x-v1.0.jar or /home/oracle/bpm1111x/prm-bpm-connector-11.1.1.x-v1.0.jar
5) In the **BPM library path** field, enter the path of the directory where you copied all the 11g jars.

   > **Note**: If the above settings are incorrect or the BPM jar files are incomplete, you will be prompted with an error message when you try to configure the BPM. Verify that your settings and jar files are correct.

6) Right-click **BPM Configuration**, then select **Configure** to set options from the dialog box. If you receive an error message, check your values from the previous steps in this section.
7) To configure P6 to use BPM 11g, add the following settings:

   > **Caution**: Do not put a forward slash / at the end of the URL. For example, it should read only `http://host:port`, and not `http://host:port/`.

   a. In the **bpm.user** field, enter the BPM 11g user with administrative access to BPM.
   b. In the **bpm.password** field, enter the password for the user.
   c. In the **bpm.t3.url** field, enter the T3 URL for your Oracle SOA configuration. For example: `t3://`*<host_name>*`:`*<port>*`/soa-infra`
   d. In the **bpm.security.realm** field, enter the name of the security realm used by BPM. This is `jazn.com` by default.
   e. In the **bpm.soap.url** field, enter the URL for the SOAP services. Usually this URL takes the form of `http://`*<host_name>*`:`*<port>*.
   f. In the **bpm.workspace.url** field, enter an address in the form of `http://`*<host_name>*`:`*<port>* that indicates where the BPM Workspace application is hosted.

      > **Note**: The host can be an IP address or a host name such as a machine name.

   g. In the **bpm.partition** field, enter the name of the SOA partition containing the BPM composite applications you would like to use in P6. The default partition name is `default`.
8) Click **OK** and save changes. When the configuration is complete, you will see a **BPM properties have been configured** message.
9) Restart the P6 application server.

Configuring Thread Pool Settings

The Thread Pool performs background job work. These settings control how many thread pools are available and how long any job can use them. Oracle recommends you keep the defaults because they will provide optimal service for most environments. Change the defaults only if you are configuring a large amount of services (scheduler, leveler, apply actuals, etc.).

To set your thread pool settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Thread Pool**.

   a. In the **Number of Threads** field, enter the number of server threads.

      The default is 50.

   b. In the **Maximum Task Duration** field, enter the maximum amount of time a task can use a thread from the P6 thread pool. Only the P6 activity view uses the P6 thread pool.

      The default is 3m.

      Since database transactions can run inside the P6 thread pool, Oracle recommends setting the duration to be longer than the the Regular Connection Pool's **Maximum Lease Duration** setting.

      > **Notes**:
      >
      > - A thread from the P6 thread pool can only be interrupted when it is in a wait condition (such as waiting for a database request to complete).
      > - See *Configuring Connection Pool for Database Instance Settings* (on page 30) for related settings.

   c. In the **Maximum Long Running Task Duration** field, enter the maximum amount of time a long running task can run before being interrupted and canceled. This setting is used for Job Services (scheduler, summarizer, and leveler), which use the P6 Long Running Thread Pool.

      The default is 20m.

      Oracle recommends you set the **Maximum Long Running Task Duration** for the thread pool to a value longer than the Long Running Connection Pool's **Maximum Lease Duration**.

   d. In the **Maintenance Frequency** field, enter the frequency at which threads are checked for excess time durations.

      The default is 45s.

Configuring Log Settings

You can use the log settings to set how the system logs errors and warnings.

To set your log settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Log/Console Logger**.
    a. In the **Severity Level** field, enter severity level for the Console Logger.

    > **Note**: The ranges are inclusive. For example, choose "debug" to log all messages; choose "warning" to log both warning and error level messages.

    b. In the **Enabled** field, choose **true** to enable the console logger or **false** to disable the console logger.
4) Expand **Log/File Logger**.
    a. In the **Archive Size** field, enter the minimum size (in Kb) a log file must be before it is archived.
    The default is 1024.
    Enter anything from 1024-2073600000.
    b. In the **Severity Level** field, enter the severity level for the File Logger.

    > **Note**: The ranges are inclusive. For example, choose "debug" to log all messages; choose "warning" to log both warning and error level messages.

    c. In the **Number of Archive Files** field, enter the maximum number of log files to use.
    Enter anything from 2-2073600000.

    > **Note**: The default files are named WebAccessLog0.html through WebAccessLog5.html.

    d. In the **HTML** field, choose **true** to log as HTML or **false** to log as plain text.
    e. In the **Enabled** field, choose **true** to enable the File Logger or **false** to disable it.

    > **Note**: Log files are created in a folder named WebAccessLogs, located in:
    > - WebLogic on Windows:
    >   *webaccesshome*\WebAccessLogs
    > - WebSphere on Windows:
    >   *webaccesshome*\WebAccessLogs
    > - WebSphere on Oracle Enterprise Linux:
    >   /*mount_point*/WebSphere/AppServer/WebAccessLogs

5) Expand **Log/Email Logger**.

> **Note**: The email logger only sends information about Error messages. Messages are sent asynchronously.

   a. In the **SMTP Host** field, enter SMTP server that will send the e-mail message.

   b. In the **From Email Address** field, enter the e-mail address that you want to send log messages.

   c. In the **To Email Address** field, enter the e-mail address where you would like log messages sent.

   d. In the **Email Subject** field, enter the subject line for error e-mails. The default is P6 Web Access error.

   e. In the **Enabled** field, choose **true** to enable the email logger or **false** to disable it.

6) Expand **Log**.

7) In the **Asynchronous** field, choose **true** to log messages after the previous one has been logged for better performance or **false** to disable this feature.

Configuring Directory Services Settings

Directory Services define how a user connects to external message queues.

> **Note**: If you are using eventing services, ensure you have completed the steps in *Configuring Eventing in the Database Instance Settings* (on page 38) before completing this section.

To set your directory services settings:

1) Open the Primavera P6 Administrator.

2) In the **Configurations** tab, expand your configuration.

3) Expand **Directory Services**.

   a. In the **Provider URL** field, enter the URL of the JNDI provider used for eventing.
      Example:
      t3://host_name:8203

   b. In the **Initial Context Factory** field, enter the class name of the initial context factory for the JNDI connection for eventing.
      Example:
      weblogic.jndi.WLInitialContextFactory

   c. In the **Security Principal** field, enter the WebLogic administrative user connected to the JNDI provider for eventing.

   d. In the **Security Credentials** field, enter the password for the WebLogic administrative user connected to the JNDI provider for eventing.

   e. In the **Security Level** field, select one of the following: **NONE** (if you don't want to use security) or **SIMPLE** (if you want use an unencrypted user name and password for security). Your selection determines the security level used to authenticate to the directory service for eventing.

      Oracle recommends using **Simple** for eventing.

f.   In the **Lookup Name** field, enter the JNDI queue name used when testing the directory connection for eventing.

4)   Right-click on **Directory Services** and select **Test Connection**.

   If the test fails, ensure you have entered all the credential above correctly.

Configuring Client Properties Settings

Client Properties describe what java plug-ins client browsers use and how they communicate.

To set your client properties settings:

1)   Open the Primavera P6 Administrator.

2)   In the **Configurations** tab, expand your configuration.

3)   Expand **Client Properties**.

   a.   In the **Internet Explorer Java Plugin URL** field, enter the URL for Internet Explorer users to download the Java Plug-in (JRE).

      This setting defaults to the plug-in version you installed during setup.

   b.   In the **Standard Browsers Java Plugin URL** field, enter the URL for Firefox, Chrome, or Safari users to download the Java Plug-in (JRE).

      This setting defaults to the plug-in version you installed during setup.

   c.   In the **Internet Explorer Java Plugin Version** field, enter the JRE version used by applets in Internet Explorer.

      This setting defaults to the plug-in version you installed during setup.

   d.   In the **Standard browsers Java Plugin Version** field, enter the JRE version used by applets in Firefox, Chrome, or Safari.

      This setting defaults to the plug-in version you installed during setup.

   e.   In the **JRE version for Java Web Start (JNLP)** field, enter the JNLP JRE version.

   f.   In the **Use JNLP when launching applets** field, choose **true** to use JNLP when launching applets. Choose **false** if you do not want to use JNLP when launching applets.

   g.   In the **Maximum memory allocated to Java Applets** field, enter the maximum amount of memory, in megabytes, that Java Applets can use. If the Maximum Activities per Activity View setting is greater than 5000, the memory allocation must be set to 128 or greater. (See *Configuring Application Settings in the Primavera P6 Administrator* (on page 49) for more information.)

      The default is 256.

      Enter anything from 64-1024.

   h.   In the **Compress Applet Communication** field, choose **true** to compress communication between applets and the server. Choose **false** if you don't want to compress communication.

   i.   In the **Compress HTML Content** field, choose **true** to compress HTML-related content generated by P6, including .html, .js, and css files, and Ajax content. Choose **false** if you don't want to compress HTML-related content.

   > **Note**: Choosing to compress will improve downloads on slower connections, but requires more CPU effort on the server and client.

j. In the **HTTP Server and Port Override** field, enter the HTTP front-end server and port that P6 clients should use.

Example   format:

http://*servername*:80

> **Note**:
> - Set this setting only if you have problems using the front-end web proxy server.
> - Do not include the context root.

k. In the **Ajax request wait timeout** field, enter how long the system should wait to timeout BPM workflows and action required tabs.

The default is 30s.

Enter anything from 1s to 24h.

Configuring Web Proxy Settings

When internal services in P6 EPPM need to access external web sites, they may need to go through your organization's firewall. You can configure that capability in the Web Proxy settings. P6   uses web proxy settings when it displays Contract Manager portlets that integrate with a Fusion server and when it connects to a Geo Code Provider server.

To set your web proxy settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Web Proxy**.
    a. In the **Web Proxy Server** field, enter the proxy server host name or IP address to use.
    b. In the **Web Proxy Port** field, enter the proxy port to use. The default is 80.
    c. In the **Web Proxy Ignore List** field, enter a comma separated list of hosts that should not go through the web proxy.

About Application Settings in the Primavera P6 Administrator

Once you have installed P6, you will need to set your Primavera P6 Administrator settings to create multiple databases and get items such as your help and tutorials working with P6. These settings also focus on items within P6 such as custom portlets.

Manage Access to Multiple Database Instances

P6 enables you to access data from different P6 EPPM databases. When you configure P6 to support multiple database instances, the Login page displays a Database list that enables users to choose the database instance where they want to connect.

Through the Primavera P6 Administrator, you can configure the server for P6 to manage user access to specific databases by requiring a database parameter in the URL. The database parameter, which is the name of a database instance, connects to the P6 server URL and points to that specific database instance. When users access the URL you specify, the Database list does not display in the Login page and they have login access only to the database instance defined by the database parameter. If users attempt to access the login page URL without specifying the required database parameter, a message displays to indicate that the URL is invalid and directs them to the administrator of P6.

For example, the following URL would log a user into the database instance named Sample:

`http://`*serverIP*`:`*listenport*`/login?db=Sample`

As the administrator, you can specify a keyword that bypasses the database parameter requirement, so that you can access all databases through the Login page database list.

Follow instructions for the database dropdown key in *Configuring Application Settings in the Primavera P6 Administrator* (on page 49) to require a database parameter for the URL and to set a keyword to bypass the database parameter requirement.

Configuring Application Settings in the Primavera P6 Administrator

To set your application settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Application**.
   a. In the **Ignore Daylight Savings Time** field, choose **false** to recognize daylight savings time or **true** to ignore it.

      > **Notes**: This setting will also impact P6 Team Member. If you notice dates and tasks are off by an hour in your P6 Team Member interfaces, the time difference could be caused by this setting.

   b. In the **Maximum Transactions for Excel Import of Resources** field, enter the maximum number of transactions (activities or resources) that can be imported at once from an .xls or .csv file.
      The default is 2000.
      Enter anything from 100-2000.

c. In the **Maximum Excel Import File Size** field, enter the maximum size (in KB) of the .xls or .csv file uploaded during import.

   The default is 1048.

   Enter anything from 64-4096.

d. In the **Allow Auto-Summarize Option** field, choose **true** to allow automatic summarization to be available in Resource Staffing user preferences or **false** to disable the auto-summarize option.

e. In the **Database Dropdown Key** field, enter the keyword to use for enabling database selection control in the login page. Pass this as a URL parameter db=keyword.
   See *Manage Access to Multiple Database Instances* (on page 49) for more information.

   Set this to an empty string if you do not want to require the keyword.

   You can also use the value you specify as the keyword to bypass the database requirement when logging into the server for P6. For example, `https://`*serverIP*`:`*listenport*`/login?db=bypass`

f. In the **Logout URL** field, enter a specific URL that appears when the user exits with the Logout/Close icon in the banner of P6. You can use any valid URL.

   If you are using WebSSO, Oracle recommends you set the Logout URL to your SSO server's logout page to end the current SSO session.

   If you do not specify a URL, P6 directs the user to the launch page of P6.

   > **Note**: If you selected the "Don't show this again" option when you used the SSO login screen, that screen will not reappear after you logout then try to log back in. To get it to reappear, you need to clear the cookies for P6.

g. In the **Filter Portfolio Stale Period** field, enter a time period of inactivity that indicates a filtered portfolio should be refreshed when a user views the projects of a filtered portfolio in either a dashboard or portfolio view.

   The default is 1d.

   Enter anything from 0s-24d20h31m23s647.

h. In the **Maximum Projects in Portfolio** field, enter the maximum number of projects returned when creating a portfolio with a filter.

   The default is 1000.

   Enter anything from 1-100000.

i. In the **Maximum Loaded Resource Planning Projects** field, enter the maximum number of projects that can open in the Resource Planning spreadsheet.

   The default is 100.

   Enter anything from 1-1000.

j. In the **Maximum Portlets per Dashboard** field, enter the maximum number of portlets that can display in a dashboard on the Dashboards Home page.

   The default is 12.

   Enter anything from 1-50.

k. In the **Maximum Projects per Portfolio View** field, enter the maximum number of projects that can display in a portfolio view on the Portfolio Analysis tab and in Portfolio View portlets on dashboards.

The default is 5000.

Enter anything from 1-20000.

l. In the **Maximum Activities per Activity View** field, enter the maximum number of activities that can display in the Activities tab of the Projects section. If greater than 5000, the Maximum memory allocated to Java Applets setting must be 128 or greater (see *Configuring Client Properties Settings* (on page 47)).

The default is 5000.

Enter anything from 1-100000.

> **Note**: Oracle recommends that the maximum value be set to 5000 (or lower) if users need to display Earned Value or Baseline-related information to avoid database timeouts.

m. In the **Maximum Assignments per Assignment View** field, enter the maximum number of assignments that can appear in an assignment view.

The default is 2000.

Enter anything from 1-15000.

n. In the **Maximum Projects per EPS View** field, enter the maximum number of projects that can appear in an EPS view.

The default is 2000.

Enter anything from 1-100000.

o. In the **Maximum Resource Chart Grouping Limit** field, enter the maximum number of charts that are allowed while grouping the project in Resource Analysis views.

p. In the **Maximum Users for shared view and filter** field, enter the maximum number of users that can be added to a shared view or filter, for example in the EPS, Activities, and Assignments views and EPS, Activities, Assignments, and User Interface View filters.

The default is 100.

Enter anything from 1 to 150

q. In the **Maximum MRU List Items** field, enter the maximum number of items that can display in a Most Recently Used (MRU) list.

The default is 5.

Enter anything from 1-10.

r. In the **Custom Portlet URL Encryption Key** field, enter Encryption key for custom portlet user password.

In the Dashboards and Project Workspace page of P6, users can create custom portlets. Depending on the target, P6 can pass the password of the currently logged on user to the target application. By default, the password is not encrypted. Use this setting to encrypt the password.

> **Notes**:
> - Assigning a key encrypts the password that is part of the URL for a custom portlet.
> - The value can be any alphanumeric character or string of characters.
> - This encryption uses the Sun/Blowfish algorithm.
> - See the *P6 Help* for more information on custom portlets.

s. In the **Use HTTP POST for Custom Portlets** field, choose **true** to use HTTP POST requests instead of GET requests when loading custom portlets. Choose **false** to continue using GET requests.

t. In the **Transaction Monitor Execution Interval** field, enter how often the transaction monitor job will run. This will ensure there are no orphan transactions.

The default is 10m.

Enter anything from 1s-24d20h31m23s647.

u. In the **Enable Cross Site Scripting Filter** field, choose **true** to allow P6 EPPM to check for unsafe http requests from the browser and unsafe responses from P6, including requested documents. P6 EPPM considers requests and responses that contain JavaScript that P6 did not generate unsafe.

The browser will display an error message for all unsafe page requests. Internet Explorer 7 will show an error message if users attempt to download an unsafe document. Internet Explorer 8 and Firefox will prompt users to download the document file instead of viewing the document directly in the P6 browser.

You do not need to restart the server after changing the value of this setting.

v. In the **Enable Cross Site Request Forgery Checking (CSRF)** field, choose **true** to allow CSRF for your environment. Choose **false** if you do not want to use CSRF.

w. In the **Enable Session Hijack Checking** field, choose **true** to allow hijack checking. Choose false if you don't want to use hijack checking.

x. In the **Contract Management Encryption Key** field, enter the Encryption key for communication between P6 EPPM and Contract Management version 13. The default key is based on the string, "Oracle Primavera." Enter a string and it will convert to a Universally Unique IDentifier (UUID). The UUID will encrypt 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.

y. In the **P6 Help Server URL** field, enter the URL used to launch P6 Help.

The default URL points to the Oracle Technology Network (OTN). OTN houses Oracle's most up-to-date documentation. If documentation needs to change to match P6 functionality, those changes will appear in the help documentation on OTN.

Note: If you chose to install

If you prefer to use the local version of the P6 Help, you can use the local host URL. You can use the local help only if you installed and deployed the p6help.war file in WebLogic or WebSphere.

Example format:

`http://`*<server_name>*`:`*<listen_port>*`/`*<context_root>*

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

z. In the **TM Help Server URL** field, enter the URL used to launch P6 Team Member Help.

The default URL points to the Oracle Technology Network (OTN). OTN houses Oracle's most up-to-date documentation. If documentation needs to change to match P6 functionality, those changes will appear in the help documentation on OTN.

If you prefer to use the local version of the P6 Team Member Help, you can use the local host URL. You can use the local help only if you installed and deployed the p6tmhelp.war file in WebLogic or WebSphere

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

Configuring Notification Settings in Application Settings

To set your notification settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Application/Notifications**.
   a. In the **Enable Issue Notifications** field, choose **true** to enable automated notifications when Issues are added or modified. Choose **false** to disable this setting.
   b. In the **Override Notification Email from User** field, choose **true** to always use the system's From e-mail address.

      Choose **false** to use the e-mail address of the user who sends notifications, if their e-mail address is configured.
   c. In the **Notification from Email User** field, enter the e-mail address that will send Notifications when either NotificationsFromEmailOverride is true or the user's e-mail address is not configured.

Configuring User Productivity Kit Settings in Application Settings

To set your User Productivity Kit (UPK) settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Application/User Productivity Kit**.

   a. In the **Enable User Productivity Kit** field, choose **true** to allow tutorials to be available within P6 EPPM. Choose **false** if you do not want to use tutorials.

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

   b. In the **User Productivity Kit URL** field, enter the URL used to launch UPK content.

      Notes:

      - The URL might be case-sensitive, depending on your application server configuration.
      - If you create your own UPK file, you should keep the file name the same as the one provided.   WebLogic requires that the name stay the same when you deploy your custom UPK file otherwise it will not work. If you change the file name, you will have to create a new domain in WebLogic to match the name of the new UPK file.

About the Primavera P6 Administrator Services Settings

Once you have installed P6, you will need to set your Primavera P6 Administrator services settings to set items such as scheduler, leveler, and apply actuals. These services settings manage your long running services including when to run them and how many threads to use.

Oracle recommends having at least two configurations: one for application servers hosting P6 and another for the background service applications that run services, but do not process web pages. You can create more configurations as needed.

For the P6 application server, you need to limit background services and how often they run. This will allow users' requests to process more quickly.

For the background services configuration, you can have more threads configured and run them at shorter intervals. For information on setting up a separate server for job services, see *Configuring a Separate Server for Job Services* (on page 94).

If you are running background services and P6 on the same server, Oracle recommends keeping the settings' defaults for your configuration.

Configuration for ASAP and Scheduled Services

The availability of ASAP and Scheduled Services depends on which Primavera P6 Administrator settings you populate and whether you are using P6 or P6 Professional. The summary below will help you to determine when you need to configure the Primavera P6 Administrator for job services.

ASAP Jobs

For P6, you must populate the appropriate Primavera P6 Administrator settings for all ASAP jobs that you want to run.

For P6 Professional, you must populate the Summarizer and Apply Actuals Primavera P6 Administrator settings for those features to run. The Scheduler, Leveler, Store Period Performance, and Recalculate Assignment Costs features will run locally in P6 Professional.

Scheduled Services Jobs

For P6, you must populate the appropriate Primavera P6 Administrator settings for all scheduled services jobs that you want to run. All scheduled services jobs are run from and are displayed in P6.

P6 Professional cannot run any scheduled services jobs or display the status of P6 scheduled services jobs.

> **Note:** Scheduled Services cannot run for Project Templates; however, Scheduler, Leveler, and Recalculate Assignment Costs features can be run as ASAP jobs for templates in P6.

Configuring Services Settings

To set your services settings:

> **Note**: If you are running services and P6 on the same server, you should keep the defaults for the rates settings. If you want to apply the service immediately, you should set the rates low. Remember that if the server is actively applying the service, all users will experience delays in the application.

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services**.
   a. In the **Enable All Services** field, choose **true** to enable 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. Oracle recommends setting this value to true if you are using the Summarize or Apply Actuals features in P6 Professional.

      Choose **false** if you want the application to treat the concurrent threads of services as equal to zero. When you set to false, the values for the threads will stay the same.
   b. In the **Job Service Poll Rate** field, enter the rate at which the server polls the database for new jobs to run.

      The default is 10s.

      Enter anything from 1s-24d20h31m23s647.
   c. In the **ASAP Cleanup Rate** field, enter the rate that the database removes completed WebASAP jobs from the database.

      The default is 1d.

      Enter anything from 1h-24d.

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.

d. In the **Enable Job Cleanup on Startup** field, choose **true** to restart recurring jobs that are stuck in the running state.

Enable Job Cleanup on Startup will start when the application initially launches and will check for any recurring jobs that are running. It will set the status of all running jobs to pending for all databases that have **Database/Instance/Auto Start Services** enabled. It also follows the **Services/Enable All Services** setting and will not run if **Enable All Services** is set to false.

Enable Job Cleanup on Startup can run on a full build or the separate job services application. If you are on a clustered environment, run this service in only one instance.

e. In the **Job Service Shared Folder Location** field, enter the location to store temporary files while they are in the job queue.

Tips

See *Configuring a Separate Server for Job Services* (on page 94) for more information on how to set these settings.

Configuring Publication Settings in Services Settings

To set your publication settings:

> **Note**: The default settings should be the optimal settings for most environments. Change them only if your environment requires different settings.

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Publication/Settings**.
4) Expand **General**.
   a. In the **Page Size** field, enter the maximum number of rows of general data a job can process. This applies to each business object that falls under the general category; general data is not time-distributed (spread), not hierarchical, and not in a blob. When using this setting, each business object processes separately.

   The default is 32.

   Enter anything from 1-8192.
   b. In the **Max Job Count** field, enter the number of processes used for this service on your server.

   The default is 1.

   Enter anything from 1-20.
5) Expand **TimeDistributed**.
   a. In the **Page Size** field, enter the maximum number of rows of time-distributed (spread) data that a job can process. This applies to each business object that falls under the time-distributed category. When using this setting, each business object processes separately.

   The default is 16.

   Enter anything from 1-8192.
   b. In the **Max Job Count** field, enter the number of processes used for this service on your server.

   The default is 1.

   Enter anything from 1-20.
6) Expand **Blob**.
   a. In the **Page Size** field, enter the maximum number of rows of blob data that a job can process. This applies to each business object that falls under the blob category. When using this setting, each business object processes separately.

   The default is 25.

   Enter anything from 1-8192.
   b. In the **Max Job Count** field, enter the number of processes used for this service on your server.

   The default is 1.

   Enter anything from 1-20.
7) Expand **Log**.

a. In the **Security Level** field, select the level of information contained in the log file for all publication services. The ranges are inclusive. For example, choose "debug" to log all messages; choose "info" to log details about what runs, exceptions, and warnings; choose "warning" to log both warning and error level messages.

    The default is info.

    Select info, debug, warning, or error.

b. In the **Global Service Log File Cap (Success)** field, enter the number of logs to retain for successful global publication services. This will retain a log for each global service. If set to 5, the last 5 successful service runs will be retained for each global service.

    The default is 5.

    Enter anything from 1-25.

c. In the **Global Service Log File Cap (Fail)** field, enter the number of logs to retain for failed global publication services. This will retain a log for each global service. If set to 5, the last 5 failed service runs will be retained for each global service.

    The default is 5.

    Enter anything from 1-25.

d. In the **Project Service Log File Cap (Success)** field, enter the number of logs to retain for successful Publish Project jobs. This will retain a log for each project service. If set to 5, the last 5 successful service runs will be retained.

    The default is 5.

    Enter anything from 1-25.

e. In the **Project Service Log File Cap (Fail)** field, enter the number of logs to retain for failed Publish Project jobs. This will retain a log for each project service. If set to 5, the last 5 failed service runs will be retained, per project.

    The default is 5.

    Enter anything from 1-25.

Configuring Publication Services in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you have scheduling work that needs to be done immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high. Remember that if the server is actively applying the service, all users will experience delays in the application.

To set your publication settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Publication/Services**.
4) Expand **Project Arbiter**. Use the Project Arbiter to automate submitting Publish Project services for eligible projects to the service queue.

   a. In the **Interval** field, enter the amount of time the service will wait before running the next available job.

   The default is 10s.

   Enter anything from 1s-24d20h31m23s647.

   b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that this service will not run on this server.

   The default is 1.

   Enter 0 or 1.

   c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all jobs finish. Choose **false** if you want each job processed according to the Interval.

5) Expand **Publish Project**.

   a. In the **Interval** field, enter the amount of time the service will wait before running the next available job.

   The default is 10s.

   Enter anything from 1s-24d20h31m23s647.

   b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that this service will not be run on this server.

   The default is 2.

   Enter anything from 0-20.

   c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all jobs finish. Choose **false** if you want each job processed according to the Interval.

6) Expand **Publish Enterprise Data**.

   > **Note**: Publish Enterprise Data, Enterprise Summaries, Resource Management, and Security will recalculate data and store it in physical fields in the Extended Schema tables, and will perform other data denormalization tasks. For example, duration fields are calculated fields in the existing P6 schema tables, but will be recalculated and stored as physical fields in the extended schema tables when a project is published.

   a. In the **Interval** field, enter the amount of time the service will wait before running the next available job.

The default is 10s.

Enter anything from 1s-24d20h31m23s647.

b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that this service will not run on this server.

The default is 1.

Enter anything from 0-1.

c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all jobs finish. Choose **false** if you want each job processed according to the Interval.

7) Expand **Publish Enterprise Summaries**.

a. In the **Interval** field, enter the amount of time the service will wait before running the next available job.

The default is 10s.

Enter anything from 1s-24d20h31m23s647.

b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that this service will not be run on this server.

The default is 1.

Enter anything from 0-1.

c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all jobs finish. Choose **false** if you want each job processed according to the Interval.

8) Expand **Publish Resource Management**.

a. In the **Interval** field, enter the amount of time the service will wait before running the next available job.

The default is 10s.

Enter anything from 1s-24d20h31m23s647.

b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that this service will not be run on this server.

The default is 1.

Enter anything from 0-1.

c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all jobs finish. Choose **false** if you want each job processed according to the Interval.

9) Expand **Publish Security**.

a. In the **Interval** field, enter the amount of time the service will wait before running the next available job.

The default is 10s.

Enter anything from 1s-24d20h31m23s647.

b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that this service will not run on this server.

The default is 1.

Enter anything from 0-1.

c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all jobs finish. Choose **false** if you want each job processed according to the Interval.

Configuring Module Access Service in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you want to apply the service immediately, you should set the rates low (e.g., 30s). Remember that if the server is actively applying the service, all users will experience delays in the application.

To set your module access service settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Module Access Service**.
   a. In the **Update Rate** field, enter the rate when a Business Rule Engine synchronizes with the database for license counts.

      The default is 30s.

      Enter anything from 100-1m.
   b. In the **Expiration Check Rate** field, enter the rate when the database checks licenses to see if they should expire.

      The default is 2m.

      Enter anything from 500-15m.

Configuring Timestamp Service in Services Settings

When the timestamp service runs, it searches the database for what items have changed and need to be refreshed in the cache.

To set your timestamp service settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Timestamp Service**.
4) In the **Refresh Rate** field, enter the rate when the database is queried to determine if a table change notification is necessary.

      The default is 1m.

      Enter anything from 15s-1h.

      Note: If you are running services and P6 on the same server, you should keep the defaults. If you enter a longer rate, the server will run more efficiently, but the data may be out of date. If you enter a shorter time, the data will be up to date, but the server may not run as efficiently.

Configuring Registry Service in Services Settings

The registry service finds changes in the Primavera P6 Administrator configuration settings and deploys those changes in the server. If you are running services and P6 on the same server, you should keep the defaults. If you enter a longer rate, the server will run more efficiently, but the data may be out of date. If you enter a shorter time, the data will be up to date, but the server may not run as efficiently.

To set your registry service settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Registry Service**.
    a. In the **Refresh Rate** field, enter the rate when the Business Rule Engine status updates in the database.

       The default is 1m30s.

       Enter anything from 15s-1h.
    b. In the **Stale Period** field, enter the duration of inactivity that indicates an inoperable Business Rule Engine.

       The default is 4m.

       Enter anything from 1m-10m.
    c. In the **Port** field, enter the TCP/IP port that will receive requests to revive dead Business Rule Engines.

       The default is 9192.

       Enter anything from 1-65535.

Configuring Next Key Service in Services Settings

The next key service finds cached keys that need updating.

To set your next key service settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Next Key Service**.
    a. In the **Refresh Rate** field, enter the rate to refresh the next key cache.

       The default is 1m.

       Enter anything from 15s-1h.

    > **Note**: If you are running services and P6 on the same server, you should keep the defaults. If you enter a longer rate, the server will run more efficiently, but the data may be out of date. If you enter a shorter time, the data will be up to date, but the server may not run as efficiently.

    b. In the **Maximum Cached Keys** field, enter the maximum next keys to cache per table.

       The default is 10.

       Enter anything from 1-100.

Configuring Alert Notification Service in Services Settings

The alert notification service controls how often the P6 database checks for alerts.

To set your alert notification service settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Alert Notification Service**.
4) In the **Refresh Rate** field, enter the rate to refresh alerts.

   The default is 30s.

   Enter anything from 15s-15m.

> **Note**: If you are running services and P6 on the same server, you should keep the defaults. If you enter a longer rate, the server will run more efficiently, but the data may be out of date. If you enter a shorter time, the data will be up to date, but the server may not run as efficiently.

Configuring Performance in Services Settings

To set your performance settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Performance**.
   a. In the **Use Enterprise Summary** field, choose **true** to use enterprise level summary data for resources and roles (EPS records). Choose **false** to use Project records.

      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 the histogram uses only one record (EPS record). If false, the histogram uses a larger number of records (Project records) to draw the histogram chart, so performance is slower. Note that histogram data is more accurate when the setting is false.
   b. In the **Maximum Summary Node Count** field, enter 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, data does not display.

      The default is 1000.

      Enter anything from 1-50000.

Configuring Scheduler in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you have scheduling work that needs to be done immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively scheduling work, all users will experience delays in the application.

To set your scheduler settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Scheduler**.

    a. In the **Interval** field, enter the amount of time the Web Scheduler will wait before scheduling the next available job.

       The default is 10s.

       Enter anything from 1s-24d20h31m23s647.

    b. In the **Concurrent Threads** field, enter the number of processes (active schedulers) used for scheduling on this server. A value of 0 indicates that scheduling will not perform on this server.

       The default is 2.

       Enter anything from 0-20.

    c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all jobs are scheduled. Choose **false** if you want each job processed according to the Scheduling Interval.

Configuring Leveler in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you have leveling work that needs to be done immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively doing leveling work, all users will experience delays in the application.

To set your leveler settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Leveler**.

    a. In the **Interval** field, enter the amount of time the Web Leveler will wait before leveling the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds).

       The default is 10s.

       Enter anything from 1s-24d20h31m23s647.

    b. In the **Concurrent Threads** field, enter the number of processes (active levelers) used for leveling on this server. A value of 0 indicates this server will not perform leveling.

       The default is 2.

       Enter anything from 0-20.

    c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all jobs are leveled. Choose **false** if you want each job processed according to the Leveling Interval.

Configuring Summarizer in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you have summarizing work that needs to be done immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively doing summarizing work, all users will experience delays in the application.

To set your summarizer settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Summarizer**.
4) In the **Maximum Duration to Summarize** field, enter the maximum activity duration that the summarizer will handle. Any projects that contain activities with durations longer than this setting will fail summarization and an error will be displayed for that project.

Configuring CopyProject in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you want the server to check CopyProject immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively checking for CopyProject, all users will experience delays in the application.

To configure the CopyProject settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/CopyProject**.
   a. In the **Interval** field, enter the amount of time to wait before running the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds).
      The default is 10s.
      Enter anything from 1s-24d20h31m23s647.
   b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that that this job will not run on this server.
      The default is 2.
      Enter anything from 0-20.
   c. In the **Active Mode** field, choose true if you want jobs processed continuously until all jobs finish. Choose false if you want each job processed according to the Interval.

Configuring Unifier in Services Settings

To set your Unifier integration settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Unifier**.
4) Expand **SendToScheduleSheet**.

> The SendToScheduleSheet service sends P6 data to Unifier's schedule sheet when the Send to Schedule Sheet action is used in P6.

   a. In the **Interval** field, enter the amount of time to wait before running the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds).

   The default is 10s.

   Enter anything from 1s-24d20h31m23s647.

   b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that that this job will not run on this server.

   The default is 2.

   Enter anything from 0-20.

   c. In the **Active Mode** field, choose true if you want jobs processed continuously until all jobs finish. Choose false if you want each job processed according to the Interval.

5) Expand **SummarizeByCBS**.

> The **SummarizeByCBS** service creates either CBS Summary data or Resource and Expenses Summary and Spread data depending on a project's Schedule Type when the Send to Summary Sheet action is used in P6.

   a. In the **Interval** field, enter the amount of time to wait before running the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds).

   The default is 10s.

   Enter anything from 1s-24d20h31m23s647.

   b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that that this job will not run on this server.

   The default is 2.

   Enter anything from 0-20.

   c. In the **Active Mode** field, choose true if you want jobs processed continuously until all jobs finish. Choose false if you want each job processed according to the Interval.

6) Expand **ProjectUpdateCheck**.

> If a project has been summarized and there hasn't been any changes made to the project since it was summarized, the ProjectUpdateCheck service will prevent the SummarizeByCBS service from running.

   a. In the **Interval** field, enter the amount of time to wait before running the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds).

   The default is 10s.

   Enter anything from 1s-24d20h31m23s647.

   b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that that this job will not run on this server.

The default is 2.

Enter anything from 0-20.

   c. In the **Active Mode** field, choose true if you want jobs processed continuously until all jobs finish. Choose false if you want each job processed according to the Interval.

Configuring GatewaySynchronization

The GatewaySynchronization service sends information from P6 to Primavera Unifier or Oracle Primavera Prime via Primavera Gateway.

To configure GatewaySynchronization:

1) Open the Primavera P6 Administrator.

2) In the **Configurations** tab, expand your configuration.

3) Expand **Services/GatewaySynchronization**.

   a. In the **Interval** field, enter the amount of time to wait before running the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds).

The default is 10s.

Enter anything from 1s-24d20h31m23s647.

   b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that that this job will not run on this server.

The default is 2.

Enter anything from 0-20.

   c. In the **Active Mode** field, choose true if you want jobs processed continuously until all jobs finish. Choose false if you want each job processed according to the Interval.

Configuring Apply Actuals in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you have apply actuals work that needs to be done immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively applying actuals, all users will experience delays in the application.

To set your apply actuals settings:

1) Open the Primavera P6 Administrator.

2) In the **Configurations** tab, expand your configuration.

3) Expand **Services/Apply Actuals**.

   a. In the **Interval** field, enter the amount of time to wait before running the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds).

The default is 10s.

Enter anything from 1s-24d20h31m23s647.

   b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that that this job will not run on this server.

The default is 2.

Enter anything from 0-20.

   c. In the **Active Mode** field, choose true if you want jobs processed continuously until all jobs finish. Choose false if you want each job processed according to the Interval.

Configuring Overallocation Check in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you want the server to check for overallocations immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively checking for overallocations, all users will experience delays in the application.

> **Note**: Enable the Project Arbiter service because projects will be published before running the overallocation service.

To set your overallocation check settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Overallocation Check**.

    a. In the **Interval** field, enter the amount of time to wait before running the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds).

       The default is 10s.

       Enter anything from 1s-24d20h31m23s647.

    b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that that this job will not run on this server.

       The default is 2.

       Enter anything from 0-20.

    c. In the **Active Mode** field, choose true if you want jobs processed continuously until all jobs finish. Choose false if you want each job processed according to the Interval.

Configuring Status Update Check in Services Settings

When you set a user as a reviewer for status updates in P6, you can have them receive notifications about pending status updates from team members using the P6 Team Member interfaces.

> **Note**: To set a user as a reviewer, see the *P6 Help* for information on P6 Team Member interfaces.

To set your status update check settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Status Update Check**.
   a. In the **Enabled** field, choose **true** if want the reviewer to receive notifications when they have pending status updates to review. Choose **false** if you don't want the reviewer to receive notifications.

   > **Note**: Admin and Project superusers can review status updates, but they will not receive a notification. Only the reviewer will receive notifications.

   b. In the **Service Run Time** field, select the time of day the service will poll the database for pending updates and send the notification.
      The default is 12AM.

Configuring Store Period Performance in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you have store period performance work that needs to be done immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively running store period performance work, all users will experience delays in the application.

To set your store period performance settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Store Period Performance**.
   a. In the **Interval** field, enter the amount of time the PeriodPerformance service will wait before running the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds).
      The default is 10s.
      Enter anything from 1s-24d20h31m23s647.
   b. In the **Concurrent Threads** field, enter the number of processes used for the PeriodPerformance service on this server. A value of 0 indicates that the service is not available on this server.
      The default is 2.
      Enter anything from 0-20.
   c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all jobs finish. Choose **false** if you want each job processed according to the Interval.

Configuring Recalculate Assignment Cost in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you have recalculate assignment cost work that needs to be done immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively running recalculate assignment cost work, all users will experience delays in the application.

To set your recalculate assignment cost settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Recalculate Assignment Cost**.

   a. In the **Interval** field, enter the amount of time the RecalculateAssignmentCost service will wait before scheduling the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds). When P6 initiates the RecalculateAssignmentCosts service, it will attempt to run immediately but switch to running as a job service if it takes too long to start.

      The default is 10s.

      Enter anything from 1s-24d20h31m23s647.

   b. In the **Concurrent Threads** field, enter the number of processes used for the RecalculateAssignmentCost service on this server. A value of 0 indicates that the service is not available on this server.

      The default is 2.

      Enter anything from 0-20.

   c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all jobs finish. Choose **false** if you want each job processed according to the Interval.

Configuring Sync Actual This Period in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you want to sync actuals immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively synchronizing actuals, all users will experience delays in the application.

To set your Sync Actual This Period settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Sync Actual This Period**.

   a. In the **Enabled** field, choose whether to synchronize actuals and ActualThisPeriod values. If you choose true, the setting recalculates actual units and costs for ThisPeriod. Choose if you do not want to synchronze actuals and ActualThisPeriod values.

   b. In the **Execution Interval** field, enter the 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.

      The default is 5m.

      Enter anything from 1s-24d20h31m23s647.

c. In the **ActivityThreshold** field, determine 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.

   The default is 8000.

   Enter anything from 1-2147483647.

d. In the **Concurrent Threads** field, enter the number of processes used for the SyncActualThisPeriod service on this server. A value of 0 indicates that the service is not available on this server.

   The default is 2.

   Enter anything from 0-20.

Configuring Sync Remaining to Planned in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you want to sync immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively synchronizing, all users will experience delays in the application.

To set your Sync Remaining To Planned settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Sync Remaining to Planned**.

a. In the **Enabled** field, choose **false** to disable the SyncRemainingtoPlanned service. Choose **true** to enable the SyncRemainingtoPlanned service.

b. In the **Execution Interval** field, enter the 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.

   The default is 5m.

   Enter anything from 1s-24d20h31m23s647.

c. In the **ActivityThreshold** field, determine 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.

   The default is 8000.

   Enter anything from 1-30000.

d. In the **Concurrent Threads** field, enter the number of processes used for the SyncRemainingtoPlanned service on this server. A value of 0 indicates that the service is not available on this server.

The default is 2.

Enter anything from 0-20.

Configuring Sync Actuals with Duration % Complete in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you want to sync actuals immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively synchronizing actuals, all users will experience delays in the application.

To set your Sync Actuals With Duration % Complete settings:

1) Open the Primavera P6 Administrator.

2) In the **Configurations** tab, expand your configuration.

3) Expand **Services/Sync Actuals with Duration % Complete**.

   a. In the **Enabled** field, choose **false** to disable the SyncActualswithDuration%Complete service. Choose **true** to enable the SyncActualswithDuration%Complete service.

   b. In the **Execution Interval** field, enter the 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.

      The default is 5m.

      Enter anything from 1s-24d20h31m23s647.

   c. In the **ActivityThreshold** field, determine 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.

      The default is 8000.

      Enter anything from 1-2147483647.

   d. In the **Concurrent Threads** field, enter the number of processes used for the SyncActualswithDuration%Complete service on this server. A value of 0 indicates that the service is not available on this server.

      The default is 2.

      Enter anything from 0-20.

Configuring Send to Fusion in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you want to send To Fusion immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively sending to Fusion, all users will experience delays in the application.

To set your send to Fusion settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Send to Fusion**.
   a. In the **Interval** field, enter the amount of time the service will wait before scheduling the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds).

   The default is 10s. Oracle recommends you keep this setting as is.

   Enter anything from 1s-24d20h31m23s647.
   b. In the **Concurrent Threads** field, enter the number of processes used for this service on this server. A value of 0 indicates that the service is not available on this server.

   The default is 2. Oracle recommends you keep this setting as is.

   Enter anything from 0-20.
   c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all jobs finish. Choose **false** if you want each job processed according to the Interval.

   Oracle recommends you choose true.

Configuring Import Service in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you have store period performance work that needs to be done immediately, you should set the Interval low (e.g., 10s) and the Concurrent Threads high (e.g., 20). Remember that if the server is actively running store period performance work, all users will experience delays in the application.

To set your store period performance settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Import Service**.
   a. In the **Interval** field, enter the amount of time the service will wait before running the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds).

   The default is 10s.

   Enter anything from 1s-24d20h31m23s647.
   b. In the **Concurrent Threads** field, enter the number of processes used for the service on this server. A value of 0 indicates that the service is not available on this server.

   The default is 2.

   Enter anything from 0-20.
   c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all jobs finish. Choose **false** if you want each job processed according to the Interval.

Configuring Project Hierarchy Cache in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you want to apply the cache immediately, you should set the Frequency low. Remember that if the server is actively applying the cache, all users will experience delays in the application.

To set your project hierarchy cache settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Project Hierarchy Cache**.
   a. In the **Cache Policy** field, select the cache policy to use. The cache policy determines how much data is in the cache and which data to remove to reclaim memory.

      You can select one of the following:
      - **FIFO** First In First Out-projects are cleared from the cache in the same order they were added to memory.
      - **LRU** Least Recently Used projects are cleared from the cache before more recently used ones.
      - **JVMM** Java Virtual Machine Managed uses soft references to cache elements; memory used by soft references is reclaimed by the JVM as required.
      - **PRR** Projects are selected at random to be cleared from cache.
      - **PRFIFO** Periodic Refresh First In First Out is the same as FIFO, except policy is enforced based on MaintenanceFrequency.
      - **PRLRU** Periodic Refresh Least Recently Used is the same as LRU, except policy is enforced based on MaintenanceFrequency.
      - **PRCC** Periodic Refresh Clear Cache ignores CacheLimit to flush the entire cache, based on MaintenanceFrequency.
   b. In the **Cache Limit** field, enter the maximum number of projects stored in memory.

      The default is 5000.

      Enter anything from 1000-30000.
   c. In the **Maintenance Frequency** field, enter the frequency for applying the specified cache policy. If you apply the cache policy, the system can reclaim memory from the cache.

      The default is 5h.

      Enter anything from 1m-24d.
   d. In the **Enable WBS Hierarchy Preload** field, select true or false.

      Oracle recommends keeping this setting **true** for most situations since security checks rely on the WBS Hierarchy cache preload.

      Make this setting **false** only if you are loading project details (for example, an API request) and the preloading cache with WBS Hierarchy details is taking a lot of time.

Configuring Collaboration Synchronization Service in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you want to apply the service immediately, you should set the Interval low. Remember that if the server is actively applying the service, all users will experience delays in the application.

To set your collaboration synchronization service settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Collaboration Synchronization Service**.
4) In the **Synchronization Interval** field, enter the interval when the collaboration synchronization service runs. The synchronization service deletes documents and workflows for deleted projects.

   The default is 1h.

   Enter anything from 1m-24d20h31m23s647.

Configuring Asynchronous Jobs in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you want to apply the service immediately, you should set the Interval low. Remember that if the server is actively applying the service, all users will experience delays in the application.

To set your asynchronous jobs service settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Asynchronous Jobs**.
   a. In the **Purge Interval** field, enter how often to remove long running job records from the database.

      The default is 1h.

      Enter anything from 1m-24d20h31m23s647.
   b. In the **Grace Time** field, enter the minimum age of long running job records removed during purge.

      The default is 1d.

      Enter anything from 0-24d20h31m23s647.

Configuring Mail Service in Services Settings

If you are running services and P6 on the same server, you should keep the defaults. If you want to apply the service immediately, you should set the Interval low. Remember that if the server is actively applying the service, all users will experience delays in the application.

To set your mail service settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Mail Service**.

    a. In the **Email Server** field, enter the hostname or IP address of the e-mail notification server.

    b. In the **Security** field, select one of the following based on the security you are using:

        ▪ **SSL**
        ▪ **TLS**
        ▪ **None**

    c. In the **SMTP(S) Port** field, enter the TCP/IP port of the outgoing SMTP server.

       The default is 25.

       Enter anything from 1-65535.

    d. In the **Bounce Email Address** field, enter the email address where you want bounced emails to be sent.

> **Note**: Bounced emails will be sent to the person who sent them automatically. This bounce field allows you to send bounced emails to your administrators so they can investigate potential problems with emails.

    e. In the **Send Interval** field, enter how often to send queued mail messages.

       The default is 1m.

       Enter anything from 0-24d20h31m23s647.

    f. In the **Maximum Queue Length** field, enter the maximum size of the mail message queue.

       The default is 250.

       Enter anything from 0-2147483647.

    g. In the **Authorized User Name** field, enter the name of the account to use to send mail from this mail server.

    h. In the **Authorized User password** field, enter the password of the account used to send mail from this mail server.

Configuring Import/Export Options in Services Settings

To set your import/export options settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/Import/Export Options**.
   a. In the **Temporary File Location** field, enter the location to store the temporary file during the XML import/export process. If you do not specify a location, the temporary file is placed in the bootstrap home location, which is in the P6 home directory (for example, c:\p6home).
   b. In the **Maximum file size** field, enter the maximum file size (in KB) for XML import/export. JVM settings and available space in the Temporary File Location determine the file size. 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.

   The default is 102400.

   Enter anything from 1024-2147483647.

Configuring UpdateBaseline in Service Settings

As a project progresses, you may want to update baseline data without restoring the baseline or creating a new baseline. When a project is in progress, creating a new baseline may not yield accurate comparison results. When you update a baseline, only the data types you select will be updated.

To set your UpdateBaseline settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Services/UpdateBaseline**.
   a. In the **Interval** field, enter the amount of time UpdateBaaeline will wait before update the baseline during the next available job (in 1d1h1m1s format - specifying only numbers without letters implies milliseconds).

   The default is 10s.

   Enter anything from 1s-24d20h31m23s647.
   b. In the **Concurrent Threads** field, enter the number of processes used for update the baseline on this server. A value of 0 indicates this server will not update the baseline.

   The default is 2.

   Enter anything from 0-20.
   c. In the **Active Mode** field, choose **true** if you want jobs processed continuously until all baselines are updated. Choose **false** if you want each baseline updated according to the interval.

Configuring P6ProCloudConnect Settings

To configure settings for P6 Pro Cloud Connect:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **P6ProCloudConnect**.
   a. In the **FetchSize** field, enter the maximum number of rows gathered in a database block. The default is 254. You can enter anything from 0-255.
   b. In the **TaskMaxTime** field, enter the maximum time allowed for a P6 Pro task to complete. A job consists of one or more P6 Pro tasks. The default is 5m.
   c. In the **TransactionMaxInactiveInterval** field, enter the timeout interval for an inactive session that has a pending database transaction. The default is 15m.
   d. In the **SessionMaxInactiveInterval** field, enter the timeout interval for an inactive session. The default is 2h.

Configuring Tracer Settings

fWhen you configure the SQL tracer, the user can see what queries P6 EPPM generates. Before you configure these settings, you need to get the tracer JAR from My Oracle Support.

To set your tracer settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Tracer**.
   a. In the **Enabled** field, choose **true** to send debugging messages to the Tracer application. Choose **false** if you do not want debugging messages sent.
   b. In the **Server Name** field, enter the destination IP address or hostname for sending tracer information.

      The default is localhost.
   c. In the **Port** field, enter the port to use for the Tracer socket connection.

      The default is 9210.

      Enter anything from 1-65535.
   d. In the **Use Background Send Thread** field, choose **true** to use the background thread to send TCP messages to tracer. Choose **false** if you don't want to use the background thread to send TCP messages.

Configuring GeoCodeProvider Settings

Configuring your Geo Code Provider settings will allow you to use the locations feature in P6. With the locations feature, you can assign locations to projects, activities, and resources so you can later report in Analytics based on geographical location.

To set your GeoCodeProvider settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **GeoCodeProvider**.
   a. In the **GeoCodeProvider** field, choose your provider:
      - Oracle 11g GeoCoder
      - Third Party Geocoder
      - None
   b. In the **Geo Code Provider URL** field, enter the URL for your geocode provider.

   > **Note**: The P6 server may have trouble starting if it cannot connect to the Geo Code URL. On the machine where you installed P6, test the URL in a browser to ensure you can connect before you enter the URL in this setting.

   For Oracle 11g GeoCoder, the default is http://elocation.oracle.com/geocoder/gcserver.
   For a third party geocoder, use the URL associated with your geocoder.

Configuring Integration API Server Settings

To configure P6 Integration API and P6 to work together, you will need to set the P6 Integration API settings in the Primavera P6 Administrator.

> **Note**: For more information on the Primavera P6 Administrator see **About the Primavera P6 Administrator** (on page 21).

To set your Integration API server settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Integration API Server/RMI**.
   a. In the **Enable** field, choose whether to enable the RMI server. You need to enable the RMI server only if you are using P6 Integration API.
   b. In the **Registry Port** field, enter the port for the RMI Registry. This value is usually set to at least 1024.

   The default is 9099.

   You can enter anything from 1-65535.
   c. P6 Integration API supports three modes. Depending on the mode you are using, enable one of the following:
      - In the **Enable Compression** field, choose whether to enable compression service mode.
      - In the **Enable SSL** field, choose whether to enable SSL service mode.
      - In the **Enable Standard Service** field, choose whether to enable Standard service mode.
   d. Depending on which mode you enable, set the corresponding port for that mode:
      - In the **Compression Service Port** field, enter 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.

        The default is 0.

        You can enter anything from 1-65535.
      - In the **SSL Service Port** field, enter 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.

        The default is 0.

        You can enter anything from 1-65535.
      - In the **Standard Service Port** field, enter 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.

        The default is 0.

        You can enter anything from 1-65535.
4) In the **Session Timeout** field, enter the amount of time when the connection for an idle will end.

The default is 120.

Enter anything from 1-24d.

About Configuring P6 EPPM Web Services in the Primavera P6 Administrator

One P6 EPPM Web Services server instance can control more than one database and you can specify an authentication mode for a database through the Authentication Configuration wizard.

You can use the Primavera P6 Administrator to set the authentication mode, token profiles and message protection settings. If you use SAML for P6 EPPM Web Services, you must use Single Sign-on or LDAP authentication for P6 EPPM. You must configure additional settings for LDAP authentication with secure communication (SSL) between the P6 EPPM Web Services server and the LDAP server.

To configure P6 EPPM Web Services and P6 to work together, you will need to set the P6 EPPM Web Services settings in the Primavera P6 Administrator.

Note:

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

- For more information on the Primavera P6 Administrator see *About the Primavera P6 Administrator* (on page 21).

- See the *P6 Web Services Programmer's Guide* for more information.

Configuring Authentication Mode for P6 EPPM Web Services

To set your authentication mode:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Web Services/Security/Authentication**.
4) In the **Mode** field, choose the method clients use for authentication. The default is Username Token Profile. You can choose one of the following:

   ▸ **Username Token Profile** - Oracle recommends using this authentication mode. It defines how a web service client application can supply a user name and an optional password in the message request that the web service server can use to authenticate the requester's identity.

   ▸ **SAML Token Profile** - Security Assertion Markup Language (SAML) defines an XML-based mechanism for exchanging messages that contain security information in the form of assertions.

   ▸ **Cookies** - This option requires you to call the Authentication service Login operation to establish a session and obtain a cookie before you can use any other P6 web service.

   > **Note**: See the *P6 Web Services Programmer's Guide* for more information.

Configuring Username Token Profile Settings for P6 EPPM Web Services

To set your Username Token Profile settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Web Services/Security/Authentication/Username Token Profile/Nonce**.

   a. In the **Require Nonce** field, choose **true** to enable nonce or **false** to disable it.

   Nonce is a token that contains a random value and is used to prevent attacks.

   b. In the **Nonce Cache Timeout** field, enter the value, in the format 1d1h1m1s, for the Nonce cache timeout. The value specified indicates how long the nonce remains cached before it is deleted.

   The default is 600 seconds (10m).

   Enter anything from 5m-24d.

4) Expand **Web Services/Security/Authentication/Username Token Profile/Created**.

   a. In the **Require Created** field, choose **true** to enable the Username token timestamp or **false** to disable it.

   Requiring a Created element allows the server to determine whether the difference between two timestamps falls within an allowable window of time and can then reject any messages that exceed the window.

   b. In the **Timeout** field, enter the value, in the format 1d1h1m1s, for the Created timestamp timeout. You can specify a minimum of 300 seconds (5m).

   The default is 600 seconds (10m).

   Enter anything from 5m-24d.

Configuring SAML Token Profile Settings for P6 EPPM Web Services

To set your SAML Token Profile settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Web Services/Security/Authentication/SAML Token Profile.**
   a. In the **SAML Version** field, choose the SAML version of the token.
   b. In the **Require Signed SAML Token** field, choose **true** to require signed SAML tokens or **false** to require unsigned SAML tokens.
4) Expand **Web Services/Security/Authentication/SAML Token Profile/SAML Tokens**.
   a. In the **Issuer** field, enter the valid issuer for the SAML token. Use a space to separate multiple valid issuers.

      Default Example:

      http://your.saml.issuer.com
   b. In the **IssueInstant Timeout** field, enter the value, in the format 1d1h1m1s, 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.

      The default is 300 seconds (5m).

      Enter anything from 5m-24d.
   c. In the **AuthenticationInstant Timeout** field, enter the value, in the format 1d1h1m1s, for the AuthenticationIssueInstant timeout. The value specified indicates the maximum time allowed between the time the token is issued, the time the user is authenticated, and the time the token is received by the web service.

      The default is 300 seconds (5m).

      Enter anything from 5m-24d.
5) Expand **Web Services/Security/Authentication/SAML Token Profile/Signed SAML Tokens**.
   a. In the **KeyStore Type** field, choose the KeyStore type.

      The default is JKS.
   b. In the **File Location** field, enter the absolute path to the key store file. This file must exist on the local filesystem.

      Default Example:

      c:\keystore\keystore.jks.
   c. In the **KeyStore Password** field, enter KeyStore password.
   d. In the **Certificate Alias** field, enter alias for the client certificate containing the public key.

      The default is alias.

Configuring Message Protection Settings for P6 EPPM Web Services

To set your message protection settings:

1) Open the Primavera P6 Administrator.

2) In the **Configurations** tab, expand your configuration.

3) Expand **Web Services/Security/Message Protection.**

   a. In the **Require Timestamp** field, choose **true** if incoming SOAP messages must contain the WS-Security Timestamp. Choose false if it does not need the WS-Security Timestamp.

   b. In the **Require Digital Signatures for Incoming Messages** field, choose **true** to require that incoming SOAP messages are signed and conform to Web Service Security 1.1 standards. Choose false if 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.

   c. In the **Require Encryption for Incoming Messages** field, choose 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 EPPM Web Services request message must be encrypted. Choose false if incoming SOAP messages must not be encrypted.

   > **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.
   > - 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.

   d. In the **KeyStore Type** field, choose the KeyStore type.

   The default is JKS.

   e. In the **File Location** field, enter the absolute path to the key store file. This file must exist on the local filesystem.

   Default Example:

   c:\keystore\keystore.jks.

   f. In the **KeyStore Password** field, enter KeyStore password.

   g. In the **Private Key Alias** field, enter alias for the private key in KeyStore.

   The default is alias.

   h. In the **Private Key Password** field, enter password for the private key.

   i. In the **Encrypt Response** field, choose whether to encrypt outgoing messages. You can use this setting only when you enable encryption 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.

Configuring Message Protection Settings for Fusion Integration

To set your message protection settings for Fusion integration:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Web Services/Security/Message Protection/Fusion Integration/Outgoing Messages.**

   a. In the **Require Encryption for Incoming Messages** field, choose 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 EPPM Web Services request message must be encrypted. Choose false if incoming SOAP messages must not be encrypted.

   b. In the **KeyStore Type** field, choose the KeyStore type.

   The default is JKS.

   c. In the **File Location** field, enter the absolute path to the key store file. This file must exist on the local filesystem.

   Default Example:

   c:\keystore\keystore.jks.

   d. In the **KeyStore Password** field, enter KeyStore password.

   e. In the **Certificate Alias** field, enter alias for the private key in KeyStore.

   The default is alias.

Configuring P6 Team Member Settings

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Team Member**.
4) Expand **User Productivity Kit** (UPK):
   a. Set the User Productivity Kit URL to `http://`*localhost*`:listen`*port*/*ContextRoot*

      where *localhost* is your server's host name, *listenport* is your P6 port number, and *ContextRoot* is the root for your tutorials (for example, P6Tutorials).
5) Expand **Team Member**:
   a. Expand **Connection Pool** if you want to alter the following default values:
      - **Initial connection pool size:** *10*
      - **Maximum active database connections:** *150*
      - **Maximum idle database connections:** *-1*
      - **Minimum idle database connections:** *10*
   b. Expand **Logging** if you want to alter the following default:
      - **Enable:** *enabled*
      - **Severity Level:** *Error*
      - **Log File Name:** *p6tmweb.log*

Authentication in P6 EPPM

This chapter describes the authentication modes for P6 EPPM and outlines the steps required to implement an authentication scheme. It also details steps on how to import user information from an LDAP server.

> **Note**: If you are using LDAP, you need to verify your field mappings and alter them to match the fields for your LDAP environment.
> See *Provisioning LDAP User Information for the First Time* (on page 91) for more information.

Authentication Modes in P6 EPPM

To manage how users can access your applications, use authentication and authorization mechanisms. Authentication is the process of validating user identity and authorization is how you control what resources and data your users can access.

P6 uses multiple settings to support authentication. These settings also control the authentication used for all P6 EPPM applications except P6 EPPM Web Services. You set authentication settings in the Primavera P6 Administrator's Authentication tab.

P6 EPPM supports these authentication modes:

▶ **Native** is the default mode for P6 EPPM. In Native mode, the P6 EPPM database acts as the authority and the application handles the authentication of the user who is logging into that application.
▶ **Single Sign-On (SSO)** controls access to Web applications. In SSO mode, the applications are protected resources. When a user tries to login to one, a Web agent intercepts the login and prompts the user for login credentials. The Web agent passes the user's credentials to a policy server, which authenticates them against a user data store. With SSO, once the users login, they are logged into all Web applications during their browser session (as long as all Web applications authenticate against the same policy server).
▶ **Lightweight Directory Access Protocol (LDAP)** authenticates users through a directory and is available for all applications. You can use LDAP referrals with Oracle Internet Directory and Microsoft Windows Active Directory. LDAP referrals allow authentication to extend to another domain. You can also configure multiple LDAP servers, which supports failover and enables you to search for users in multiple LDAP stores. An LDAP directory server database confirms the user's identity when they attempt to login to the application.

> **Note**: For Oracle Internet Directory, referrals only work when you configure the directories to search anonymously.

Regardless of the authentication scheme you choose, the P6 EPPM database controls user authorization.

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 Primavera P6 Administrator. Although you specify authentication modes for client/server applications and Web applications separately, you must use a consistent authentication scheme within P6 EPPM. For example, client/server and Web applications must *both* be configured for either LDAP authentication or native authentication.

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.

Login Procedures and Authentication in P6 EPPM

The authentication modes have different login procedures:

In Native mode

P6 EPPM presents a login dialog that prompts for a user name and password. Depending on whether you enabled the password policy option in Application Settings in P6, the user may have to create a strong password.

In LDAP mode

▶ All P6 EPPM applications and the P6 Professional SDK require a login password.
▶ Since the LDAP directory stores and authenticates passwords, users cannot change their passwords in P6 EPPM.

In Single Sign-On mode

▶ For P6, the Single Sign-On server requests and validates login credentials. Once a user is authenticated, the launch page for P6 appears so the user can select a database and language.
  Users cannot change their passwords in P6 EPPM because passwords are stored and authenticated against a directory server user store.

Authentication Configuration Process in P6 EPPM

By default, all P6 EPPM applications use Native authentication. After you install your P6 EPPM applications, you can choose a different authentication scheme.

> **Note:** If you are upgrading from a previous version of P6 EPPM, see the *Automatically Upgrading and Configuring P6 EPPM* guide before modifying the authentication settings.

Your database instance controls your Authentication mode, which means you can enable a different authentication mode for each of your configurations.

▶ If using Single Sign-On authentication, you can set P6 to SSO but set P6 Professional and P6 Integration API to LDAP. When using SSO mode, P6 Integration API uses LDAP mode.
▶ If using LDAP authentication, you can specify LDAP servers, configure more than one LDAP server for each database instance, map LDAP attributes to P6 EPPM database fields, and provision users.

Follow the guidelines below to specify an authentication scheme and perform additional configuration tasks for authentication:

▶ Configure administrative settings using the Primavera P6 Administrator. See ***About the Authentication Tab in the Primavera P6 Administrator*** (on page 89) for details on these settings.
▶ When using LDAP mode, provision user information from the LDAP server using P6. See ***Provisioning LDAP User Information for the First Time*** (on page 91).
▶ Configure BI Publisher to use with P6 when using LDAP or SSO mode. See the *Connecting BI Publisher to P6* guide for more information.

Tips

▶ If multiple instances within a configuration point to the same database, P6 EPPM will use the Authentication Mode for the first instance in the list.

▸ To enable you to configure more than one LDAP server for each database instance, you can set multiple LDAP Connection Settings for authentication. Right-click the **LDAP Connection Settings** folder to duplicate, delete, copy, paste, or test a configuration. When P6 authenticates a user, it will search each LDAP server in order for a user name that matches the login name and will use the first matching user to verify the password.

▸ 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 will display; the user must select a database that matches the authentication mode set for the P6 server.

About the Authentication Tab in the Primavera P6 Administrator

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

> **Notes:**
>
> - See the procedures in the *Automatically Upgrading and Configuring P6 EPPM* if you are upgrading from a previous version of P6 EPPM software 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.
> - If you are using LDAP, you need to verify your field mappings and alter them to match the fields for your LDAP environment. See Provisioning LDAP User Information for the First Time for more information.

Configuring Web Single Sign-On Settings in the Primavera P6 Administrator

Single Sign-On (SSO) controls access to Web applications. In SSO mode, the applications are protected resources. When a user tries to login to one, a Web agent intercepts the login and prompts the user for login credentials. The Web agent passes the user's credentials to a policy server, which authenticates them against a user data store. With SSO, once the users login, they are logged into all Web applications during their browser session (as long as all Web applications authenticate against the same policy server).

To set your web single sign-on settings:

1) Open the Primavera P6 Administrator.
2) In the **Authentication** tab, expand your configuration.
3) Expand **Authentication**.
4) In the **Login Mode** field, select **WebSSO**.
5) Expand **Authentication/Web Single Sign-On**.
   a. In the **User Name Header Key** field, enter the name of the HTTP Header you specified in the policy server.

   The value you specify must match the property you created under the policy domain/realm, where the Web server for P6 resides.

For Oracle Single Sign-On, the value should be **Proxy-Remote-User**. The Proxy-Remote-User should match the LDAP server attribute that maps to the P6 EPPM database USER_NAME field. See *Provisioning LDAP User Information for the First Time* (on page 91).

For Oracle Access Manager, the value should be OAM_REMOTE_USER.

b. In the **Context Path Override** field, enter the path used to pass web requests from the Single Sign-On Web server to the P6 server. The default listed is the value for P6 (/p6).

c. In the **Allow Alternate Login Attribute** field, choose **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 e-mail address when authenticating 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.
> See *Provisioning LDAP User Information for the First Time* (on page 91).

d. In the **Header Key** field, enter the HTTP Header Key which contains the global user ID. The default is Osso-User-Guid.

e. In the **LDAP Search Attribute** field, enter the LDAP attribute searched by the Header Key to authenticate users. The default is orclguid.

> **Note**: You must configure the LDAP settings for the appropriate database instance to establish a connection to the LDAP server.

Configuring HTTPS Settings in the Primavera P6 Administrator

Native is the default mode for P6 EPPM. In Native mode, the P6 EPPM database acts as the authority and the application handles the authentication of the user who is logging into that application.

To set your HTTPS settings:

1) Open the Primavera P6 Administrator.
2) In the **Authentication** tab, expand your configuration.
3) Expand **Authentication**.
4) In the **Login Mode** field, choose **Native**.
5) Expand **Authentication/HTTPS**.

   a. In the **Enabled** field, choose **true** if users don't use an HTTPS URL for the login page. If you choose true, P6 redirects the users to an HTTPS login page to complete the login process. You must enable SSL communication for the application server or web server.

   Choose **false** if you do not want users redirected to an HTTPS URL for login.

   > **Caution**: If kept as false, the application server will receive the passwords as clear text when a user logs into the application.

   > **Note**: If you have problems accessing the P6 application and you enabled this setting, you will need to verify that you enabled the SSL listen port on your application server and that it matches the Authentication/HTTPS/Port setting below. You should also check the WebAccessLog to ensure there is not an "SSL disabled" error message.

   b. In the **Port** field, enter the port number used for SSL. You must enter the port number only if you enable the HTTPS option.

   The default is 443.

   Enter anything from 0-2147483647.

Configuring Database Instance Settings in the Primavera P6 Administrator

To set your database instance settings:

1) Open the Primavera P6 Administrator.
2) In the **Authentication** tab, expand your configuration.
3) Expand your **Database Instance**.
4) In the **Authentication Mode** field, choose your authentication mode.

   > **Note**: If you choose LDAP, you will need to set your LDAP Connection Settings. You will do this while you are *Configuring Database Instance Settings in the Primavera P6 Administrator* (on page 91).

Provisioning LDAP User Information for the First Time

To provision LDAP user information for P6 EPPM for the first time:

> **Caution:** Ensure that all users are logged out of P6 EPPM to ensure the Primavera P6 Administrator saves your new settings.
>
> **Note:** Verify your default global profile; the global profile will be assigned to all provisioned users.

1) Log into the Primavera P6 Administrator. See *About the Primavera P6 Administrator* (on page 21).
2) From the **Authentication** tab:
   a. Expand the **Authentication** folder and ensure that **Login Mode** is set to **NATIVE**.
   b. Expand the **Database instance** folder and ensure that **Authentication Mode** is set to **Native**.
   c. Click **Save Changes**.
3) Restart the application server instance.

> **Note:** If you do not restart the application server instance, the Primavera P6 Administrator will restore settings to the previous configuration.

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* (on page 125) to add a new user (in Native mode) that matches an LDAP server user with rights to read the LDAP directory.

> **Note**: Ensure that you have a P6 user and LDAP user that match.

   a. Assign a global profile that contains privileges to add new users and search the LDAP directory. See *Configuring User Access* (on page 129) for details.
   b. Assign the appropriate project profiles and module access. See *Configuring User Access* (on page 129) for details.
6) Log back into the Primavera P6 Administrator.
7) From the **Authentication** tab:
   a. Expand your configuration.
   b. Change **Login Mode** to **LDAP**.
   c. Expand **Database instance** and set **Authentication Mode** to **LDAP**.
   d. Expand **LDAP Connection Settings[n]**.
      1. In the **Host** field, enter the host name of your LDAP server.
      2. In the **Port** field, enter the port number of your LDAP server.
      3. In the **Username** field, enter the LDAP user name that has privileges to log into the LDAP server and perform LDAP searches.
      4. In the **Password** field, enter the password for the user name you entered above.
      5. In the **Enable SSL** field, choose **true** if you are using SSL or **false** if you are not using SSL.

6. In the **Chase Referrals** field, choose **true** to enable chase referrals or **false** to disable them.

7. In the **Base Directory Node** field, enter the base dn string that represents where LDAP tree should search during login or provisioning.

   Example:

   dc=ad, dc=Marketing, dc=CompanyABC, dc=com

8. In the **Preferred Pool Size** field, enter the preferred pool size. The default is 10.

9. In the **Maximum Pool Size** field, enter the maximum pool size. The default is 20.

10. In the **Connection Timeout (in seconds)** field, enter how long (in seconds) the system should try to connect to the LDAP before timing out. The default is 300.

11. Expand **Field Map**.

   Note: Except where noted, these settings represent what you will enter for an Oracle Internet Directory (OID) LDAP server and a Microsoft Active Directory.

12. In the **USER_NAME** field, enter the LDAP field name that holds the user's login ID.
   Example:

   uid

   or

   samaccountname (for Microsoft Active Directory)

13. In the **EMAIL_ADDR** field, enter the LDAP field name that holds the user's email address.
   Example:

   mail

14. In the **ACTUAL_NAME** field, enter the LDAP field name that holds the user's full name.
   Example:

   cn

   or

   displayname (for Microsoft Active Directory)

15. In the **OFFICE_PHONE** field, enter the LDAP field name that holds the user's phone number.
   Example:

   telephoneNumber

e. Right-click the **LDAP Connection Settings** folder and select **Test Connection**.

f. Click **Save Changes**.

8) Restart the application server instance.

   Note: If you do not restart the application server instance, the Primavera P6 Administrator will restore settings to the previous configuration.

9) Log into P6 as the new user you created when you were in Native mode.

10) On the **Users** page, click the 🖶 **Add** icon.

    a. Add users as described in ***Adding Users in LDAP or SSO Authentication Mode*** (on page 127).

    b. If needed, change the configuration settings for the new users. See ***Configuring User Access*** (on page 129).

Tips

▶ 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.

▶ You can copy a current user's settings to all the new users you create when you bring them in from LDAP.

Configuring LDAP Settings in the Primavera P6 Administrator

Lightweight Directory Access Protocol (LDAP) authenticates users through a directory and is available for all applications. You can use LDAP referrals with Oracle Internet Directory and Microsoft Windows Active Directory. LDAP referrals allow authentication to extend to another domain. You can also configure multiple LDAP servers, which supports failover and enables you to search for users in multiple LDAP stores. An LDAP directory server database confirms the user's identity when they attempt to login to the application.

To set your LDAP settings:

1) Open the Primavera P6 Administrator.
2) In the **Authentication** tab, expand your configuration.
3) Expand **Authentication**.
4) In the **Login Mode** field, choose **LDAP**.
5) Expand **Authentication/LDAP**.

    a. In the **SSL Certificate Store** field, enter the full path to the keystore that holds the SSL certificate for the LDAP server.

    b. In the **SSL Store Password** field, enter the password for the keystore that holds the SSL certificate.

Configuring a Separate Server for Job Services

For medium to large deployments, Oracle recommends setting up a dedicated application server node for job services. You should disable Job services on the server accepting user traffic.

> **Notes:**
>
> - For details on what constitutes a medium or large deployment, see the *P6 Enterprise Project Portfolio Management Performance and Sizing Guide* white paper.
> - These instructions assume that you have already configured the server accepting user traffic.

Follow the guidelines below to configure the dedicated job services server:

1) Copy the **p6services.jar** from the *p6home* directory where you installed P6 to a node that will use job services.
2) Ensure a supported JRE is in the system path. (See the *Tested Configuration* for supported JREs.)
3) Open a new command line or terminal window.
4) Navigate to the folder where p6services.jar was copied (for example, c:\jobservices).
5) Run the services application by typing "`java -Xms<MEMORY SIZE> -Xmx<MEMORY SIZE> -jar p6services.jar`" in the window. (See the *P6 Enterprise Project Portfolio Management Performance and Sizing Guide* white paper for the correct value for the <MEMORY SIZE> setting for your environment. The settings in the example are the recommended values.)

   The line should look similar to the following:

   `"java -Xms4096m -Xmx4096m -jar p6services.jar"`

   If you are using Sun JDK, it should look similar to the following:

   `"java -server -Xms4096m -Xmx4096m -jar p6services.jar"`

6) If a BREBootStrap.xml file is in the USER_HOME, you can specify the location to the BREBootstrap.xml file by adding the following line:

   > **Note:**
   >
   > - USER_HOME refers to your home directory. For example, in Windows it could be C:\Users\<USER_NAME> or C:\Documents and Settings\<USER_NAME>; in Unix, it could be /home/<USER_NAME>.
   > - If this is the first time you are launching p6services.jar, and a BREBootStrap.xml file does not exist in the USER_HOME, the database configuration wizard will launch. Skip to the next step.

   `-Dprimavera.bootstrap.home=<BOOTSTRAP_LOCATION>`

   The whole line should look similar to the following:

   `java -Xms4096m -Xmx4096m`
   `-Dprimavera.bootstrap.home=<BOOTSTRAP_LOCATION> -jar p6services.jar`

where *<BOOTSTRAP_LOCATION>* is the location where the BREBootStrap.xml is located (for example, C:/USER_HOME).

7) If this is the first time you are launching p6services.jar, and a BREBootStrap.xml file does not exist in the <USER_HOME> directory (or <BOOTSTRAP_HOME> directory if the primavera.bootstrap.home is specified), the database configuration wizard will launch.

Follow the steps in ***Changing Database Connection Settings for P6** (on page 17)*.

Create a new configuration when **The Installer has detected...** dialog box appears and give this new configuration a distinct name. For example, if you chose "P6 Users" for the configuration name for the server accepting user traffic, name the new configuration "P6 Job Services."

> **Note**: Create a new configuration for Job Services to ensure optimal database performance. Job Services could slow down performance if it is part of the same configuration.

8) In the Primavera P6 Administrator:

a. Locate the **Services/Enable All Services** setting for the configuration created for the job services server (for example, P6 Job Services). Set the setting to **true** to enable all services.

b. Locate the **Services/Enable All Services** setting for the configuration created for user traffic (for example, P6 Users). Set the setting to **false** to disable all services.

Users and Security in P6 EPPM

P6 EPPM enables multiple users to work simultaneously in the same projects across an organization. To ensure that data is protected from unauthorized changes, you can create global and project security profiles that control access. You can then set up users and assign organizational breakdown structure (OBS) elements to users, project profiles, and enterprise project structure (EPS) nodes. You can additionally configure resource security and define access to P6 functionality.

Read this chapter to understand the process for setting up users and implementing security in P6 EPPM.

Security Concepts in P6 EPPM

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

To ensure security at various levels of data, P6 provides two sets of security profiles:

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

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

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

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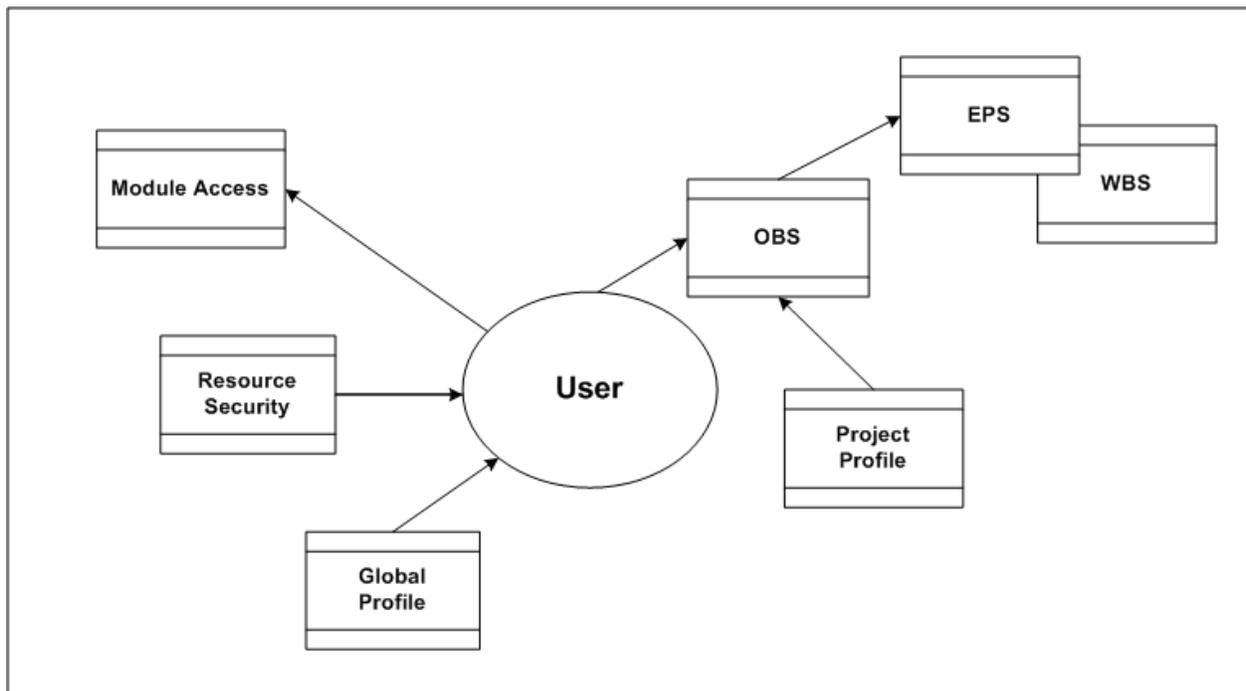
Security Samples

Review the following portions of a sample EPS for Capital Improvement projects in Oak County and its corresponding portion of the OBS.

## Organizational Breakdown Structure (OBS)
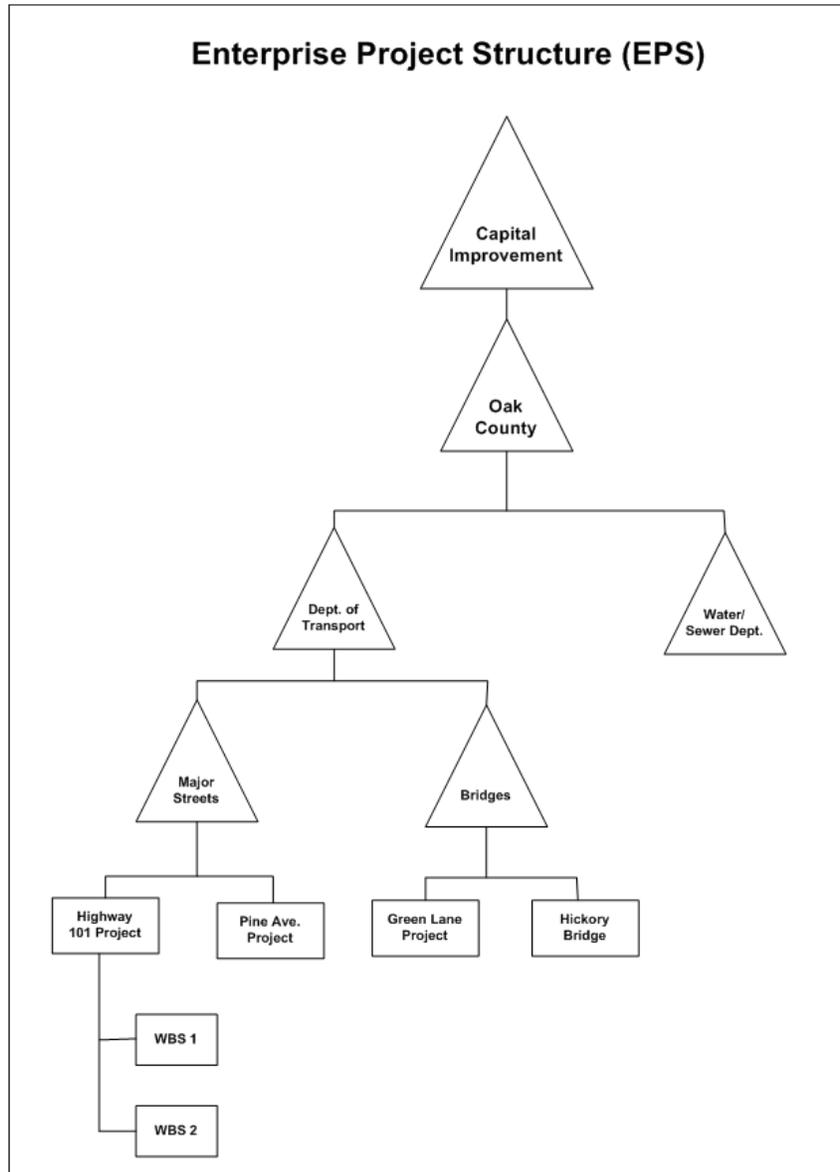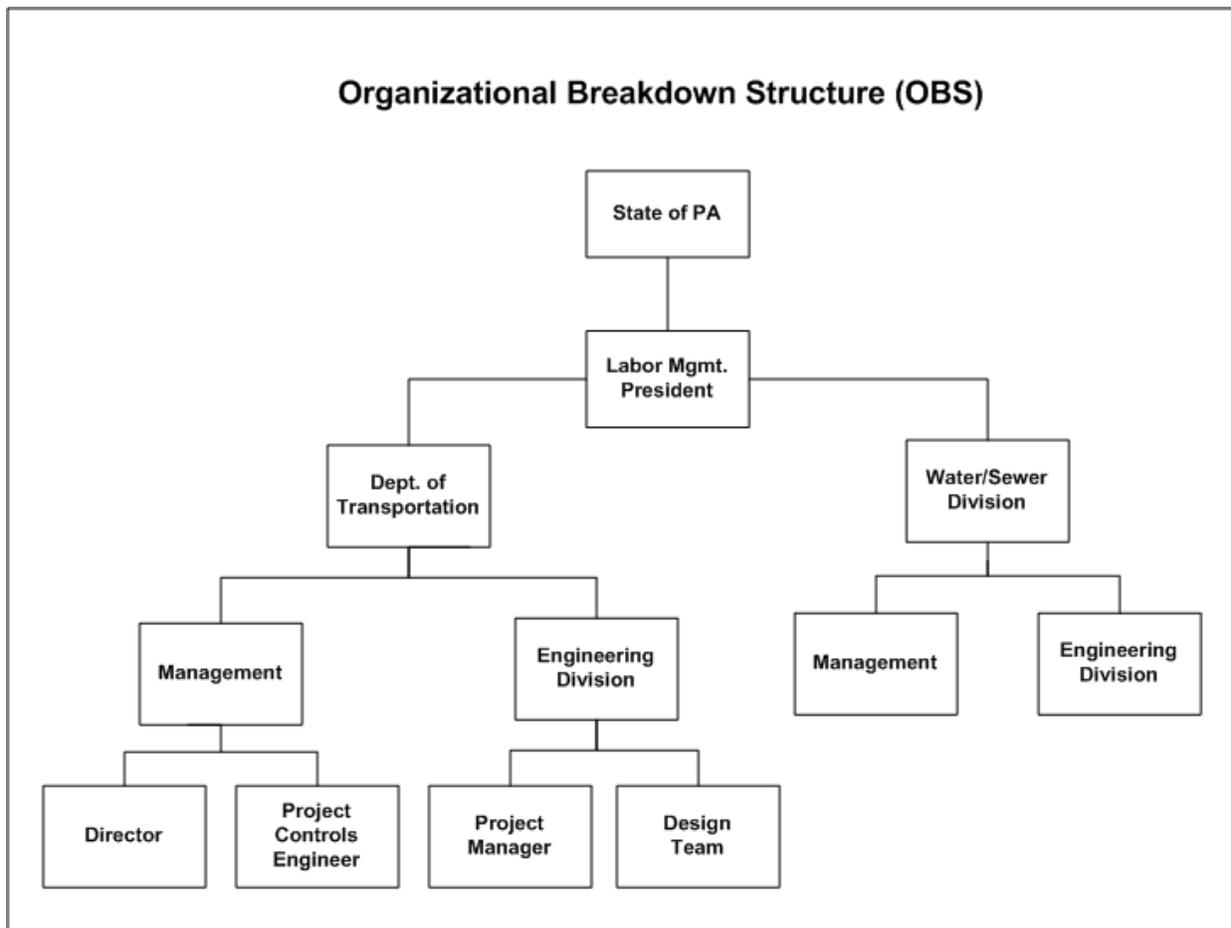
With these structures defined, you can map users to their corresponding roles in the OBS, which in turn can be assigned to each level in the EPS. The EPS level to which you assign the OBS determines the nodes/projects the associated user can access. For example, if you assign an OBS element to the root node of the EPS, the users associated with that OBS element can access the projects in the entire EPS. If you assign an OBS element to one branch of the EPS, the associated users can access only projects within that branch.

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

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

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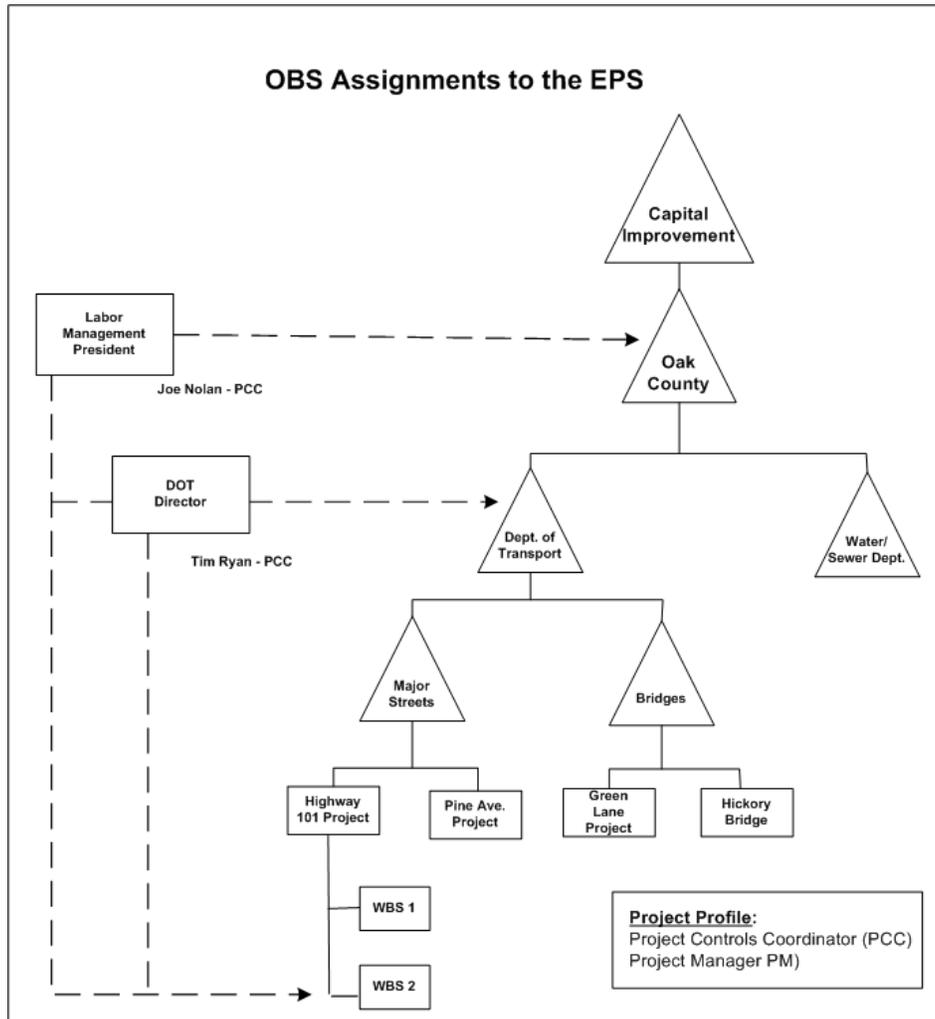

You can further control the access to projects by assigning OBS elements at the project and/or WBS level. In the previous example, if Marie Ross is the Project Manager in the Engineering Division responsible for the Highway 101 project, you can assign her to that OBS element with a Project Manager profile.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

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

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

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

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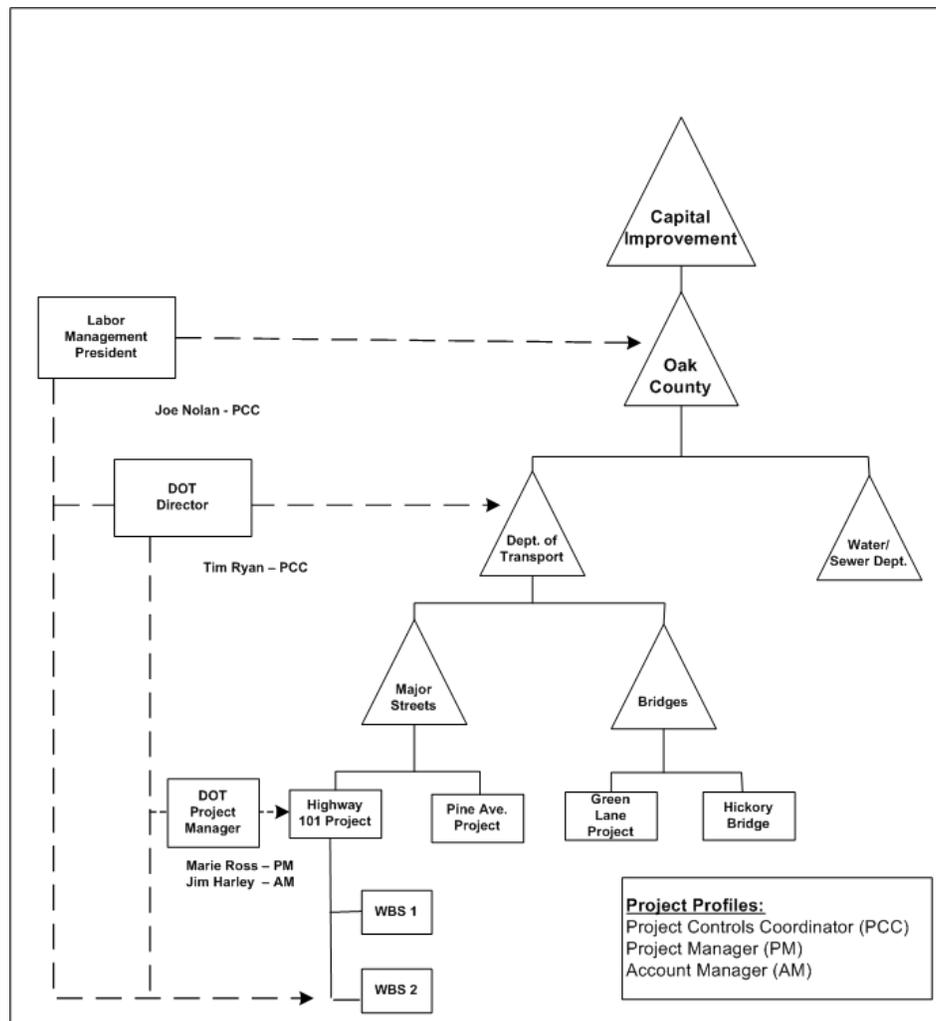
To designate that Jim Harkey has Project Manager rights to the Pine Avenue project and Marie Ross has Account Manager rights to the Pine Avenue project, you would need to add another element to the OBS.

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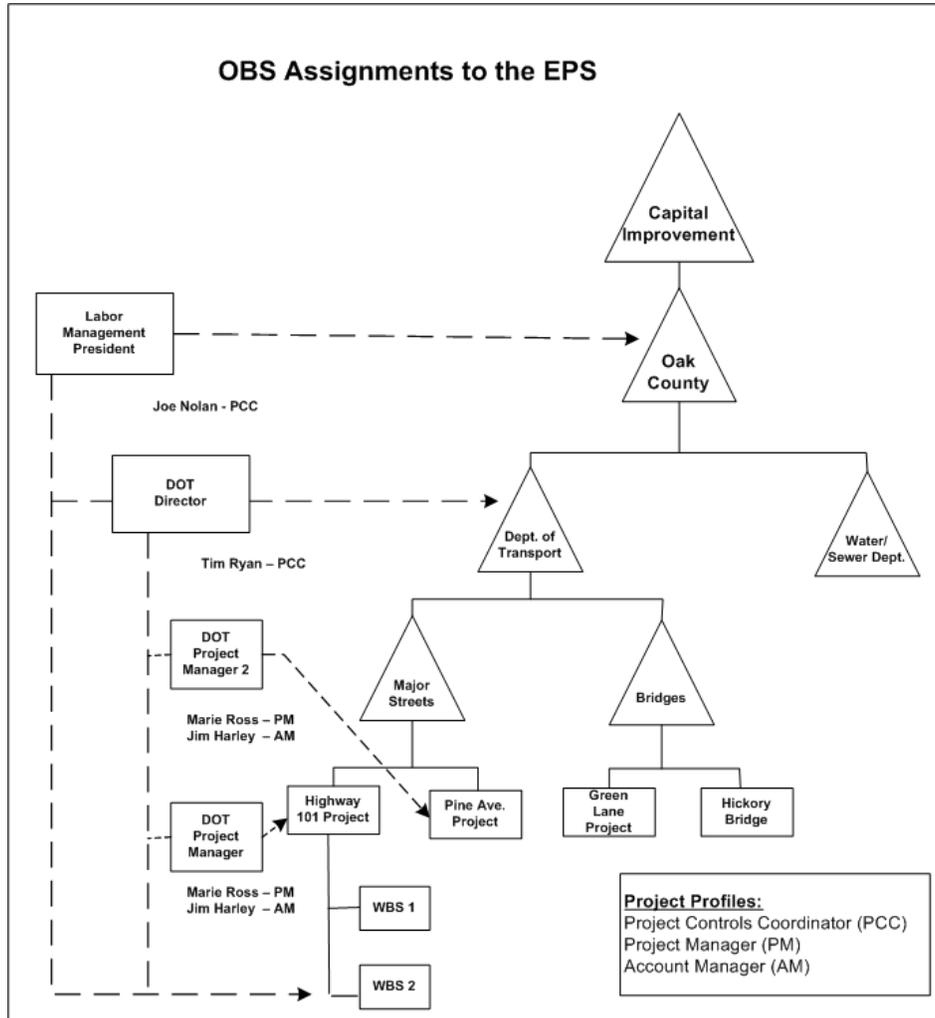
With these assignments, Jim Harkey and Marie Ross now have Project Manager rights to their primary projects and Account Manager rights to their secondary projects.

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

Useful P6 EPPM Terms

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

User Any person who needs access to P6 EPPM modules, including P6 Professional, P6 Team Member interface, and P6.

Resource The people, materials, and/or equipment that perform the work on activities. In P6, you can build a resource hierarchy that includes the required resources across all projects in the organization. Resources are assigned to activities in P6 and can be set up to use the P6 Team Member interface to report actual work hours for those resources.

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

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

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

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

A user does not have to be included in the OBS if he/she needs to access P6 but is not part of the responsible management structure. Similarly, a user might not be a part of the resource hierarchy. For example, if the user is a resource assigned to activities and needs to update them in the P6 Team Member interface, he/she must be included in the resource hierarchy; however, a user who is an executive requiring access to Dashboards in P6 is not a part of the resource pool.

For more information on resources, OBS, EPS, and WBS, see the *P6 Help*.

Security Configuration Process in P6 EPPM

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

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

▶ Create global and project security profiles in P6 EPPM.

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

▶ Add users in P6 EPPM.

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

▶ Define user interface views that restrict and provide access to P6 functionality according to the requirements of your company's functional roles. See *Defining User Interface Views* (on page 138).

▶ Set up the OBS for your company.

Identify your company's management structure and include the roles or names of those who will be responsible for the projects and work to be completed. See the *P6 Help* for more information.

▶ After setting up the OBS, assign the appropriate users and project profiles to each element of the OBS. See *Assigning OBS Elements and Project Profiles in P6 EPPM* (on page 148).

▶ Set up the EPS for your company.

Identify your company's project structure, which is global across the organization. See the *P6 Help* for more information.

▶ After setting up the EPS, assign the responsible manager (OBS) to each EPS node. See *Assigning OBS Elements to the EPS* (on page 154).

▶ Define the resources necessary to complete the projects across the organization. See the *P6 Help* for more information.

▶ Link resources to users if they will be using the P6 Team Member interface.

▶ Define user access to resource data. See *Defining User Access to Resources in P6 EPPM* (on page 154).

▶ Add projects to the EPS and define the WBS for each project (if needed).

Project managers usually perform this step. They can further control security within their own projects by assigning specific OBS elements to WBS levels. Refer to the *P6 Help* for more information.

▸ Set preferences for data in P6 EPPM. See *Application Settings and Global Enterprise Data in P6 EPPM* (on page 157).

Defining Global Security Profiles in P6 EPPM

A global security profile determines a user's access to application-wide information and settings, such as resources, global codes, and the OBS. P6 requires that you assign a global security profile to each user.

You can define an unlimited number of global security profiles in P6. In addition, P6 provides two predefined global security profiles: Admin Superuser and No Global Privileges.

▸ The **Admin Superuser** profile allows complete access to all global information and all projects. It also shows the full Administer menu, even when the currently assigned user interface view settings do not. For the pages and menus of the other sections, even for users with the Admin Superuser profile, the current user interface view settings still apply. The Admin Superuser profile is assigned to the application (administrative) user created during the P6 EPPM database installation.

🛡 For security reasons, Oracle strongly recommends that you replace the default Admin Superuser (admin) immediately after a manual database installation or an upgrade from P6 version 7.0 and earlier. Also, limit the Admin Superuser assignment to only those individuals who require access to all data. At least one user must be assigned to the Admin Superuser profile. If only one user is assigned to this profile, P6 will not allow that user to be deleted.

▸ The **No Global Privileges** profile restricts access to global data. Assign this profile to anyone who is strictly a P6 Team Member interfaces user and does not require access to P6 Professional or P6. If a user with rights to P6 Professional or P6 is assigned this profile, the user can log in to these applications but will not have access to project data and will have read-only access to global data. If a user is assigned this profile and is also assigned to an OBS element, the user will have access to project data as defined for the OBS element, but access to other global data is restricted.

The Admin Superuser can designate that users have the ability to add/delete, edit, assign, or view secure codes. Secure codes enable privileged users to hide Project, Activity, Resource, and Issue codes from users that do not have security privileges to view them. Also, users with privileges to Edit Security Profiles can restrict other users to edit, assign, and view privileges. For example, management could track project approval processes through secure codes that others cannot edit or, in some cases, view.

Tip

▸ When defining each global security profile, some privileges are structured hierarchically. In other words, if a user is granted add or delete privileges, that user automatically has edit, assign, and view privileges. If a user is granted edit privileges, that user is automatically granted assign and view privileges. If a user is granted assign privileges, that user is automatically assigned view privileges.

▸ See *The Default Admin Superuser* (on page 124) for guidelines on replacing the default Admin Superuser (admin) immediately after a manual database installation or an upgrade from P6 version 7.0 and earlier.

Creating Global Security Profiles

Create a global security profile to determine user access to application-wide information.

To create a global security profile:

1) Click the **Administer** ▾ menu and select **User Access**.
2) In the **User Access** pane, click **Global Security Profiles**.
3) On the **Global Security Profiles** page:
   a. Click ⊕ **Add**.
   b. In the **Profile Name** field, double-click and type a unique name.
   c. In the **Description** field, double-click and type a description.
   d. In the **Default** field, select the option if you want this profile to be the new default.
   e. Click each detail window and select options to assign privileges to the profile.

   > **Note**: Select the **Privilege** option in the detail window's header to assign all privileges in the window. Clear the **Privilege** option to disable all privileges in the window.

4) On the **Global Security Profiles** page, click 💾 **Save** (Ctrl+S) .

Tips

▸ Provide clear profile names and descriptions to help you manage profiles.

▸ 🛡 Create a default global profile with few or no privileges.

▸ To save time, consider copying, pasting, and modifying an existing profile: select the closest matching profile and click **Copy**. All privilege options are also copied. Click in the list and click **Paste**. The new profile will appear with a unique name based on the original. For example, if you copied *PM Set*, the copy is named *PM Set-1*.

Global Privilege Definitions

The lists on the following pages define each global privilege.

Administration Privileges

Add/Edit/Delete OBS option

Determines whether the profile will enable users to create, modify, and remove hierarchical data for the global Organizational Breakdown Structure.

Add/Edit/Delete Security Profiles option

Determines whether the profile will enable users to create, modify, and remove global and project security profiles, which grant access to application-wide and project-specific information.

Add/Edit/Delete Users option

Determines whether the profile will enable users to create, modify, and remove P6 EPPM user data. To search the LDAP directory when provisioning, users must also have the Provision Users from LDAP global privilege.

Add/Edit/Delete User Interface Views option

Determines whether the profile will enable users to create, modify, and remove user interface views configurations, which control the functionality users can access in P6.

Edit Application Settings option

Determines whether the profile will enable users to modify application settings, which set global preferences for P6 EPPM.

Provision Users from LDAP option

Determines whether the profile will enable users to search the LDAP directory when provisioning. For users who do not have this privilege assigned to their profile, the option to load an LDIF file to provision users will still be enabled. To search the LDAP directory, users also must also have the 'Add/Edit/Delete Users' global privilege.

Codes Privileges

Add Global Activity Codes option

Determines whether the profile will enable users to create global activity codes and code values data. This privilege also selects the 'Edit Global Activity Codes' global privilege.

Edit Global Activity Codes option

Determines whether the profile will enable users to modify global activity codes data. This privilege also enables users to create, modify, and remove global activity code values.

Delete Global Activity Codes option

Determines whether the profile will enable users to remove global activity codes and code values data. This privilege also selects the 'Add Global Activity Codes' and 'Edit Global Activity Codes' global privileges.

Add Global Issue Codes option

Determines whether the profile will enable users to create global issue codes and code values data. This privilege also selects the 'Edit Global Issue Codes' global privilege.

Edit Global Issue Codes option

Determines whether the profile will enable users to modify global issue codes data. This privilege also enables users to create, modify, and remove global issue code values.

Delete Global Issue Codes option

Determines whether the profile will enable users to remove global issue codes and code values data. This privilege also selects the 'Add Global Issue Codes' and 'Edit Global Issue Codes' global privileges.

Add Project Codes option

Determines whether the profile will enable users to create project codes and code values data. This privilege also selects the 'Edit Project Codes' global privilege.

Edit Project Codes option

Determines whether the profile will enable users to modify project codes data. This privilege also enables users to create, modify, and remove project code values.

Delete Project Codes option

Determines whether the profile will enable users to remove project codes and code values data. This privilege also selects the 'Add Project Codes' and 'Edit Project Codes' global privileges.

Add Resource Codes option

Determines whether the profile will enable users to create resource codes and code values data. This privilege also selects the 'Edit Resource Codes' global privilege.

Edit Resource Codes option

Determines whether the profile will enable users to modify resource codes data. This privilege also enables users to create, modify, and remove resource code values.

Delete Resource Codes option

Determines whether the profile will enable users to remove resource codes and code values data. This privilege also selects the 'Add Resource Codes' and 'Edit Resource Codes' global privileges.

Add/Delete Secure Codes option

Determines whether the profile will enable users to create and remove all secure project codes, global and EPS-level activity codes, and resource codes and code values data, as well as all secure issue codes and code values data. This privilege also selects the 'Edit Secure Codes,' 'Assign Secure Codes,' and 'View Secure Codes' global privileges.

Edit Secure Codes option

Determines whether the profile will enable users to modify all secure project codes, global and EPS-level activity codes, and resource codes and code values data, as well as all secure issue codes and code values data. This privilege also selects the 'Assign Secure Codes' and 'View Secure Codes' global privileges.

Assign Secure Codes option

Determines whether the profile will enable users to assign all secure project codes, global and EPS-level activity codes, and resource codes and code values data, as well as all secure issue codes and code values data. This privilege also selects the 'View Secure Codes' global privilege.

View Secure Codes option

Determines whether the profile will enable users to display all secure project codes, global and EPS-level activity codes, and resource codes and code values data, as well as all secure issue codes and code values data.

Global Data Privileges

Add/Edit/Delete Categories and Overhead Codes option

Determines whether the profile will enable users to create, modify, and remove categories and overhead codes data, which can be applied to all projects. Overhead codes are only available to P6 Team Member Web users.

Add/Edit/Delete Cost Accounts option

Determines whether the profile will enable users to create, modify, and remove cost accounts data.

Add/Edit/Delete Currencies option

Determines whether the profile will enable users to create, modify, and remove currencies data.

Add/Edit/Delete Locations option

Determines whether the profile will enable users to create, modify, and remove locations data.

Add/Edit/Delete Financial Period Dates option

Determines whether the profile will enable users to create, modify, and remove financial periods data. To edit period data, users must also have the 'Edit Period Performance' project privilege assigned to their profile.

Add/Edit/Delete Funding Sources option

Determines whether the profile will enable users to create, modify, and remove funding source data.

Add/Edit/Delete Global Calendars option

Determines whether the profile will enable users to create, modify, and remove global calendars data.

Add/Edit/Delete Global Portfolios option

Determines whether the profile will enable users to create, modify, and remove global portfolio configurations in Manage Portfolios Views.

Add/Edit/Delete Global Scenarios option

Determines whether the profile will enable users to create, modify, and remove scenarios configurations in the Manage Scenarios link.

Add/Edit/Delete Risk Categories, Matrices, and Thresholds option

Determines whether the profile will enable users to create, modify, and remove risk categories, risk scoring matrices, and risk thresholds data.

Add/Edit/Delete Timesheet Period Dates option

Determines whether the profile will enable users to create, modify, and remove individual or batched timesheet periods.

Add/Edit/Delete User Defined fields option

Determines whether the profile will enable users to create, modify, and remove User Defined fields. Even without this privilege, users can still display User Defined fields information.

Resources Privileges

Add Resources option

Determines whether the profile will enable users to create resource data. This privilege also selects the 'Edit Resources' global privilege.

Edit Resources option

Determines whether the profile will enable users to modify resource data. This privilege also enables users to assign, modify, and remove role assignments. To display resources' price/unit in reports, users must have this privilege and the 'View Resource and Role Costs/Financials' global privilege assigned to their profile. To display resource skill level (a resource's role proficiency) in the application and in reports, users must have this privilege and the 'View Resource Role Proficiency' global privilege assigned to their profile.

Delete Resources option

Determines whether the profile will enable users to remove resource data. This privilege also selects the 'Add Resources' and 'Edit Resources' global privileges.

Add/Edit/Delete Resource Calendars option

Determines whether the profile will enable users to create, modify, and remove resource calendars data. This privilege also enables users to edit Shifts in P6 Professional.

Add/Edit/Delete Resource Curves option

Determines whether the profile will enable users to create, modify, and remove resource distribution curves definitions.

Add/Edit/Delete Roles option

Determines whether the profile will enable users to create, modify, and remove roles data.

Add/Edit/Delete Global Resource and Role Teams option

Determines whether the profile will enable users to create, modify, and remove global Resource Teams and Role Teams. A Resource/Role Team is a collection of resources/roles.

Add/Edit/Delete Rate Types and Units of Measure option

Determines whether the profile will enable users to create, modify, and remove resource rate types and units of measure data.

View Resource and Role Costs/Financials option

Determines whether the profile will enable users to display all values for labor, material, and nonlabor resource costs, price/unit values for roles, and costs for resource and resource assignments User Defined fields. For users who do not have this privilege assigned to their profile, all areas that display monetary values for labor, material, and nonlabor resources and roles will display dashes and cannot be edited. For resources, such areas include resource price/unit, values in resource spreadsheets and histograms in Resource Analysis and Team Usage, and Cost data types for Resource User Defined fields. For roles, the area is the price/unit value in roles data. To display resources' price/unit, users must have this privilege and the 'Edit Resources' global privilege assigned to their profile.

View Resource Role Proficiency option

Determines whether the profile will enable users to display, group/sort, filter, search, and report on resource and role proficiency. To display resource skill level (a resource's role proficiency), users must have this privilege and the Edit Resources global privilege assigned to their profile.

Approve Resource Timesheets option

Determines whether the profile will enable users to approve or reject submitted timesheets as a Resource Manager.

Templates Privileges

Add/Edit/Delete Activity Step Templates option

Determines whether the profile will enable users to create, modify, and remove Activity Step Templates, which are used to add a set of common steps to multiple activities.

Add/Edit/Delete Issue Forms option

Determines whether the profile will enable users to create, modify, and remove issue forms.

Add/Edit/Delete Microsoft Project and Primavera Templates option

Determines whether the profile will enable users to create, modify, and remove templates that are used to import/export data from/to Microsoft Project or Primavera XML formats.

Add/Edit/Delete Project Templates option

Determines whether the profile will enable users to create, modify, and remove templates that can be used when creating new projects. To create project templates, users must also have the 'Add Projects' project privilege assigned to their profile. To modify templates, you must have the same project privileges that are required to modify projects. To delete project templates, users must also have the 'Delete Projects' project privilege assigned to their profile.

Tools Privileges for Global Privileges

Administer Global External Applications option

Determines whether the profile will enable users to create, modify, and remove entries in the list of global external applications in P6 Professional.

Administer Global Scheduled Services option

Determines whether users have the privilege to modify settings on the Global Scheduled Services dialog box. You can modify the following publishing services if you have this privilege: Publish Enterprise Data, Publish Enterprise Summaries, Publish Resource Management, Publish Security. With this privilege, you can enable the service, choose how often the service will run, and at what time the service will run.

Administer Project Scheduled Services option

Determines whether the profile will enable users to set up the Apply Actuals, Summarize, Schedule, and Level scheduled services to run at specific time intervals.

Edit Global Change Definitions option

Determines whether the profile will enable users to create, modify, and remove Global Change specifications available to all users in P6 Professional.

Import Project Management XER, MPP, MPX, and P3 option

Determines whether the profile will enable users to import projects, resources, and roles from XER, MPP, MPX, and P3 formats using P6 Professional. To create new projects when importing, users must also have the 'Create Project' project privilege assigned to their profile. Users must be an Admin or Project Superuser to update a project from XER or P3 formats.

Import XLS option

Determines whether the profile will enable users to import projects, resources, and roles from XLS files into P6 Professional and P6. P6 Professional users must also be a Project Superuser to update a project from XLS format. P6 users do not need to be a Project Superuser, but do require the Add/Edit Activities Except Relationships privilege.

Import XML option

Determines whether the profile will enable users to import projects from P6, P6 Professional, and Microsoft Project using XML format. To create new projects when importing, users must also have the 'Create Project' project privilege assigned to their profile.

View All Global/Project Data via SDK option

Determines whether the profile will enable users to view All Global and Project Data via SDK. For Admin Superusers, access to the P6 Professional SDK will be read/write. For all other users, access will be read only.

Views and Reports Privileges for Global Privileges

Add/Edit/Delete Global Activity and Assignment Layouts, Views and Filters option

Determines whether the profile will enable users to create, modify, and remove global activity and resource assignment layouts, views, and filters.

Add/Edit/Delete Global Dashboards option

Determines whether the profile will enable users to create, modify, and remove global dashboards.

Add/Edit/Delete Global Project, WBS and Portfolio Layouts, Views and Filters option

Determines whether the profile will enable users to create, modify, and remove global project, WBS, and portfolio layouts, views, and filters. This privilege is required to save view changes made to the Portfolio Analysis page.

Add/Edit/Delete Global Reports option

Determines whether the profile will enable users to create, modify, and remove global reports, including editing report groups and global report batches and saving global reports created or modified in P6 Professional.

Edit Global Tracking Layouts option

Determines whether the profile will enable users to create, modify, and remove global tracking layouts in P6 Professional.

Edit Projects from Scorecards option

Determines whether the profile will enable users to create, modify, and remove projects from scorecards in the Portfolio View portlet and the Portfolio Analysis page. This privilege is required to save data changes made to the Portfolio Analysis page. The following project privileges are also required for scorecards: 'Edit Project Details Except Costs/Financials' to edit project data, 'View Project Costs/Financials' to view project cost data, 'Edit WBS Costs/Financials' to edit project cost data, 'Create Project' to add a project, and 'Delete Project' to delete a project.

Add/Edit/Delete Global Visualizer Layouts option

Determines whether the profile will enable users to create, modify, and remove global layouts in Visualizer.

Add/Edit/Delete Global Visualizer Filters option

Determines whether the profile will enable users to create, modify, and remove global filters in Visualizer.

Defining Project Security Profiles in P6 EPPM

A project profile is a role-based profile that limits privileges to specific project data, such as baselines, the WBS, and expenses. P6 does not require that each user be assigned a project profile; however, users cannot access projects unless they are assigned a project profile or the global profile, Admin Superuser.

You can create an unlimited number of project profiles in P6. In addition, P6 provides a predefined project profile called Project Superuser. The Project Superuser profile allows complete access to elements within a project. 🛡️ For security reasons, limit the Project Superuser assignment to only those individuals who require access to all project data.

Project profiles are applied to users via OBS assignments. P6 requires that all EPS and WBS elements, and projects, are assigned a responsible OBS. The combination of the project profile/user assignment to an OBS assignment, and the OBS assignment to the EPS/WBS, determines which projects and data the user can access. The default profile is automatically assigned when an OBS is assigned to a user.

Tip

▸ When defining each project profile, some privileges are structured hierarchically. In other words, if a user is granted add or delete privileges, that user automatically has edit, assign, and view privileges. If a user is granted edit privileges, that user is automatically granted assign and view privileges. If a user is granted assign privileges, that user is automatically assigned view privileges.

▸ See **Assigning OBS Elements and Project Profiles in P6 EPPM** (on page 148) for more information on assigning users to OBS elements.

Creating Project Security Profiles

Create a project security profile to determine a user's level of access to each project within the enterprise project structure. A user can only access projects they have been assigned.

To create a project security profile:

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **Project Security Profiles**.
3) On the **Project Security Profiles** page:
    a. Click ⊕ **Add**.
    b. In the **Profile Name** field, double-click and type a unique name.
    c. In the **Description** field, double-click and type a description.
    d. In the **Default** field, select the option if you want this profile to be the new default.
    e. Click each detail window and select options to assign privileges to the profile.

    > **Note**: Select the **Privilege** option in the detail window's header to assign all privileges in the window. Clear the **Privilege** option to disable all privileges in the window.

4) Click 💾 **Save** (Ctrl+S).

Tips

▶ Provide clear profile names and descriptions to help you manage profiles.
▶ 🛡 Create a default project profile with few or no privileges.
▶ To save time, consider copying, pasting, and modifying an existing profile: select the closest matching profile and click **Copy**. All privilege options are also copied. Click in the list and click **Paste**. The new profile will appear with a unique name based on the original. For example, if you copied *PM Set*, the copy is named *PM Set-1*.

Project Privilege Definitions

The lists on the following pages define each project privilege.

Activities Privileges

Add/Edit Activities Except Relationships option

Determines whether the profile will enable users to create and modify all activity information in projects, except activity relationships. Users assigned a profile with this privilege can also designate another user as an activity owner and be assigned as a status reviewer for reviewing status updates from P6 Team Member interface users. Users assigned Team Member work distribution filters must have this privilege assigned. To modify activity IDs, users must also have the 'Edit Activity ID' project privilege assigned to their profile. To use the Recalculate Assignment Costs feature, users must also have the 'View Project Costs/Financials' project privilege assigned to their profile.

Delete Activities option

Determines whether the profile will enable users to remove activities from projects.

Add/Edit/Delete Activity Relationships option

Determines whether the profile will enable users to create, modify, and remove activity relationships assigned to projects.

Edit Activity ID option

Determines whether the profile will enable users to modify activity IDs. To modify activity IDs, users must also have the 'Add/Edit Activities Except Relationships' project privilege assigned to their profile.

Add/Edit/Delete Expenses option

Determines whether the profile will enable users to create, modify, and remove expenses assigned to projects.

Codes Privileges

Add Project Activity Codes option

Determines whether the profile will enable users to create project activity codes and code values data. This privilege also selects the 'Edit Project Activity Codes' project privilege.

Edit Project Activity Codes option

Determines whether the profile will enable users to modify project activity codes data. This privilege also enables users to create, modify, and remove project activity code values.

Delete Project Activity Codes option

Determines whether the profile will enable users to remove project activity codes and code values data. This privilege also selects the 'Add Project Activity Codes' and 'Edit Project Activity Codes' project privileges.

Add EPS Activity Codes option

Determines whether the profile will enable users to create EPS-level activity codes and code values. This privilege also selects the 'Edit EPS Activity Codes' project privilege.

Edit EPS Activity Codes option

Determines whether the profile will enable users to modify the name of EPS-level activity codes. This privilege also enables users to create, modify, and remove EPS-level activity code values.

Delete EPS Activity Codes option

Determines whether the profile will enable users to remove EPS-level activity codes and code values data. This privilege also selects the 'Add EPS Activity Codes' and 'Edit EPS Activity Codes' project privileges.

EPS and Projects Privileges

Add/Edit/Delete EPS Except Costs/Financials option

Determines whether the profile will enable users to create, modify, and remove EPS hierarchy nodes, edit EPS notebook, and edit all EPS-related data except financial information.

Edit EPS Costs/Financials option

Determines whether the profile will enable users to modify EPS budget logs, funding sources, and spending plans.

Add Projects option

Determines whether the profile will enable users to create, copy, and paste projects within the EPS node. To create project templates, users must also have the 'Add/Edit/Delete Project Templates' global privilege assigned to their profile.

Delete Projects option

Determines whether the profile will enable users to delete, cut, and paste projects within the EPS node. To delete project templates, users must also have the 'Add/Edit/Delete Project Templates' global privilege assigned to their profile.

Edit Project Details Except Costs/Financials option

Determines whether the profile will enable users to set Project Preferences and to edit project-level data. This privilege also enables users to assign or remove a risk scoring matrix to a project in the Risk Scoring Matrices page in Enterprise Data.

Certain Project Preferences, such as linking to a Contract Management project and editing Publication Priority, require additional privileges. To assign a project baseline, users must also have the 'Assign Project Baselines' project privilege assigned to their profile. To edit cost UDFs, users must also have the 'Edit WBS Costs/Financials' project privilege assigned to their profile.

Add/Edit/Delete WBS Except Costs/Financials option

Determines whether the profile will enable users to create, modify, and remove WBS hierarchy nodes, notebook entries, earned value settings, milestones, work products and documents, and dates.

Edit WBS Costs/Financials option

Determines whether the profile will enable users to modify Project or WBS budget logs, funding sources, spending plan, and financial data at the project level. This privilege also enables users to edit cost data at the activity level, including resource assignments. To edit costs and financials at the WBS level, including cost UDFs, users must also have the 'Add/Edit/Delete WBS Except Costs/Financials' project privilege assigned to their profile. The 'Edit WBS Costs/Financials' privilege also selects the 'View Project Costs/Financials' project privilege.

View Project Costs/Financials option

Determines whether the profile will enable users to display all monetary values for projects. For users who do not have this privilege assigned to their profile, all areas that display monetary values will display dashes and cannot be edited. To use the Recalculate Assignment Costs feature, users must also have the 'Add/Edit Activities Except Relationships' project privilege assigned to their profile. To display the resource price/unit, users must have the 'View Resource and Role Costs/Financials' global privilege assigned to their profile.

Delete Project Data with Timesheet Actuals option

Determines whether the profile will enable users to delete activities and resource assignments for projects that have timesheet actuals. This includes cutting an activity with timesheet actuals and pasting the activity to another project. To delete project data at all different levels (activity, WBS, project, and EPS), users must also have the appropriate privileges assigned to their profile. For example, to delete activities with timesheet actuals, users must also have the 'Delete Activities' project privilege assigned to their profile. To delete activities and WBS nodes with timesheet actuals, users must additionally have the 'Add/Edit/Delete WBS Except Costs/Financials' project privilege assigned to their profile.

Tips

▶ To modify templates, you must have the same project privileges that are required to modify projects.

▶ The administrator should not assign any of the following privileges to users who should not have access to view cost information while copying and pasting project/EPS or assigning WBS and Fill Down on the WBS column in the Activities view: View Project Costs/Financials, Edit WBS Costs/Financials, and Edit EPS Costs/Financials.

Project Data Privileges

Add/Edit/Delete Issues and Issue Thresholds option

Determines whether the profile will enable users to create, modify, and remove thresholds and issues assigned to projects. The privilege also enables users to assign issue codes to project issues.

Add/Edit/Delete Project Baselines option

Determines whether the profile will enable users to create, modify, and remove baselines for projects.

Add/Edit/Delete Project Calendars option

Determines whether the profile will enable users to create, modify, and remove calendars assigned to projects.

Add/Edit/Delete Risks option

Determines whether the profile will enable users to create, modify, and remove risks assigned to projects.

Add/Edit/Delete Template Documents option

Determines whether the profile will enable users to create, modify, remove project template documents. If the content repository is installed and configured, this privilege also enables users to check out and start reviews for project template documents. A profile must be assigned the 'Add/Edit/Delete Work Products and Documents' project privilege before you can select this privilege.

Add/Edit/Delete Work Products and Documents option

Determines whether the profile will enable users to create, modify, and remove project documents that do not have a security policy applied. Document security policies are available only in P6 and only for documents stored in the content repository. When the content repository is installed and configured, this privilege also enables users to create document folders in P6.

Add/Edit Workgroups option

Determines whether the profile will enable users to create and modify workgroups.

Delete Workgroups option

Determines whether the profile will enable users to remove workgroups.

Edit Workspace and Workgroup Preferences option

Determines whether the profile will enable users to customize the project workspace and workgroup preferences.

Assign Project Baselines option

Determines whether the profile will enable users to assign project baselines to projects. To assign project baselines, users must also have the 'Edit Project Details Except Costs/Financials' project privilege assigned to their profile.

Related Applications Privileges

Import/View Contract Management Data option

Determines whether the profile will enable users to import and display data from Contract Management in P6 Professional.

Administer Project External Applications option

Determines whether the profile will enable users to modify entries in the External Applications feature in P6 Professional.

Exchange Project Data with Primavera Unifier option

Determines whether the profile will enable users to exchange project data with a linked Primavera Unifier project.

Exchange Project Data with Primavera Prime option

Determines whether the profile will enable users to exchange project data with a linked Oracle Primavera Prime project.

Exchange Project Data with ERP option

Determines whether the profile will enable users to exchange project data with a linked ERP project.

Resource Assignments Privileges

Add/Edit Activity Resource Requests option

Determines whether the profile will enable users to create and modify resource requests for activities.

Add/Edit/Delete Resource Assignments for Resource Planning option

Determines whether the profile will enable users to assign, modify, and remove resource assignments on a project or WBS level in Resources. This privilege also enables users to define search criteria and conduct a search for resource assignments. For users who do not have this privilege assigned to their profile, the resource assignment information on the Planning page is read-only for that particular project or WBS. Since project-level security privileges go down to the WBS level, it is possible to be able to assign a resource to one WBS in a project and not another.

Add/Edit/Delete Role Assignments for Resource Planning option

Determines whether the profile will enable users to assign, modify, and remove role assignments on a project or WBS level in Resources. This privilege also enables users to define search criteria for role assignments. For users who do not have this privilege assigned to their profile, role assignment information on the Planning page is read-only for that particular project or WBS. Since project-level security privileges go down to the WBS level, it is possible to be able to assign a role to one WBS in a project and not another.

Edit Committed Flag for Resource Planning option

Determines whether the profile will enable users to identify committed resource and role assignments on a project or WBS level on the Planning page. The 'Add/Edit/Delete Resource Assignments for Resource Planning' project privilege is also required for this functionality.

Edit Future Periods option

Determines whether the profile will enable users to enter, modify, and delete future period assignment values in the Planned Units and Remaining (Early) Units fields of the Resource Usage Spreadsheet using P6 Professional. The 'Add/Edit Activities Except Relationships' project privilege is also required for this functionality.

Edit Period Performance option

Determines whether the profile will enable users to modify period performance values for labor and nonlabor units as well as labor, nonlabor, material, and expense costs using P6 Professional. The 'Add/Edit Activities Except Relationships' and 'View Project Costs/Financials' project privileges are also required for this functionality.

Timesheets Privileges

Approve Timesheets as Project Manager option

Determines whether the profile will enable users to approve or reject submitted timesheets as a Project Manager in Timesheet Approval.

Tools Privileges for Projects

Allow Integration with ERP System option

Determines whether the profile will enable users to send project data to an integrated Oracle system using the Send to ERP or Send to Fusion feature on the Activities page in the Projects section. This is a project level privilege and is not specific to each level of the WBS.

Apply Actuals option

Determines whether the profile will enable users to apply actuals to activities in projects.

Check In/Check Out Projects and Open Projects Exclusively option

Determines whether the profile will enable users to check projects out to work remotely and then check them back in using P6 Professional, and whether users can open projects exclusively. Opening a project exclusively places a lock on the project allowing only the user who opened the project to make changes to the project. Other users can view project data, but cannot make updates until the exclusive lock is released.

Edit Contract Management Project Link option

Determines whether the profile will enable users to create, edit, and delete a link to Contract Management projects.

Level Resources option

Determines whether the profile will enable users to level resources in projects. This privilege also selects the 'Schedule Project' project privilege.

Schedule Projects option

Determines whether the profile will enable users to schedule projects.

Monitor Project Thresholds option

Determines whether the profile will enable users to run the threshold monitor for projects in P6 Professional.

Store Period Performance option

Determines whether the profile will enable users to track actual this period values for actual units and costs in projects. The 'Add/Edit Activities Except Relationships' project privilege is also required for this functionality.

Summarize Projects option

Determines whether the profile will enable users to summarize data for all projects in the EPS.

Edit Publication Priority option

Determines whether the profile will enable users to edit the Publication Priority for the project. This privilege should be granted only to administrators to optimize the flow of projects through the service queue.

Run Baseline Update option

Determines whether the profile will enable users to update baselines assigned to projects with new project information using the Update Baseline tool.

Run Global Change option

Determines whether the profile will enable users to run Global Change specifications to update activity detail information in P6 Professional.

Allow Integration with Primavera Unifier option

Determines whether the profile will enable users to link projects to Primavera Unifier projects and schedule sheets.

Views and Reports Privileges for Projects

Add/Edit Project Level Layouts option

Determines whether the profile will enable users to create, modify, and remove project level layouts in the Activities, Assignments, or WBS windows in P6 Professional.

Edit Project Reports option

Determines whether the profile will enable users to modify reports, modify report batches, and export reports for projects in P6 Professional.

Publish Project Website option

Determines whether the profile will enable users to publish a Web site for projects in P6 Professional.

Add/Edit/Delete Project Visualizer Layouts option

Determines whether the profile will enable users to create, modify, and remove project layouts in Visualizer.

Configuring Users in P6 EPPM

Depending on your security profile, the Users table enables you to add and remove users and control user access to P6 EPPM modules. You must add a user in P6 for each person who needs access to any P6 EPPM module.

At a minimum, each user requires a login name, global profile, and module access. You can also provide additional information about the user, such as an e-mail address and phone number.

If your organization centralizes user information in an LDAP directory, you can add P6 EPPM users by provisioning from the LDAP store. After you provision users, you will need to assign each user module access.

If your company's OBS is established, and you know which OBS elements to associate with each user, you can make the assignments using the Project Access window of the Users table. See *Assigning OBS Elements and Project Profiles in P6 EPPM* .

About User Access

User access helps you create user accounts, assign access, manage the organizational breakdown structure (OBS) and configure profiles. The User Access page presents a list of tabs:

Users: Presents options to modify security attributes and project and module access for all users of P6 EPPM modules.

OBS: Presents options to configure the OBS hierarchy.

Global Security Profiles: Presents options to assign or omit global privileges to profiles.

Project Security Profiles: Presents options to assign or omit project privileges to profiles.

Working with User Access

On the **User Access** page, you can assign users access to the module and projects, create OBSs, and assign global and project privileges.
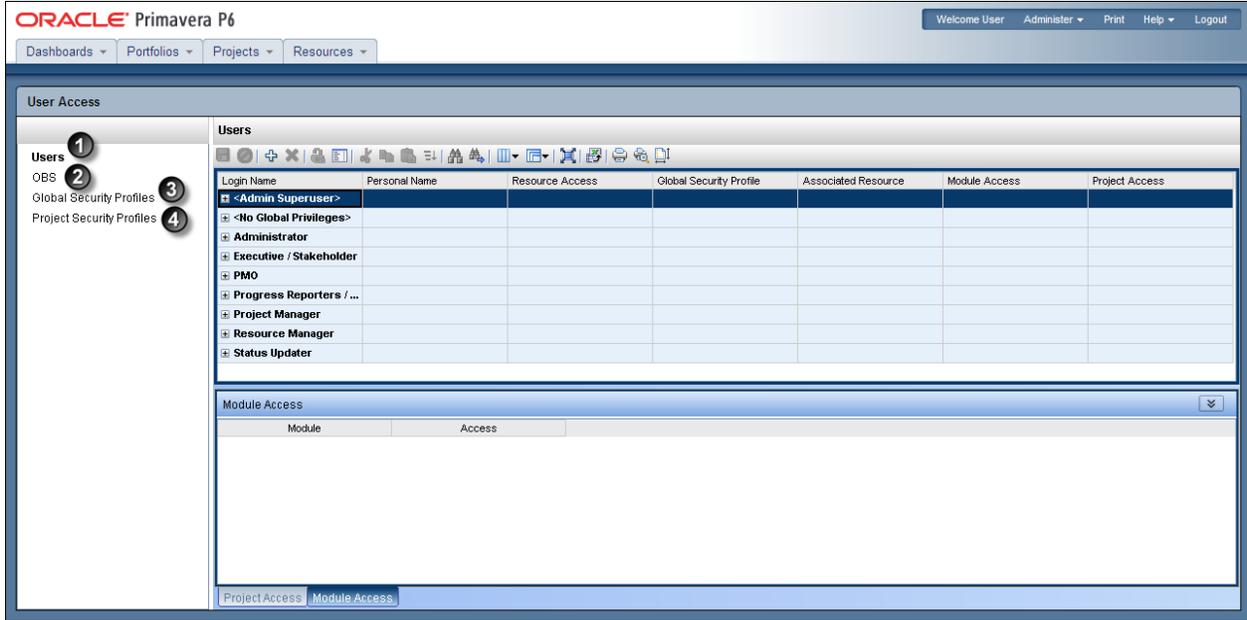
Table of the User Access Page

Item	Description
①	**Users**: Use the **Users** page to assign users access to the module and to projects.
②	**OBS**: Use the **OBS** page to assign managers to an OBS.
③	**Global Security Profiles**: Use the **Global Security Profiles** page to assign global privileges to users.
④	**Project Security Profiles**: Use the **Project Security Profiles** page to assign project privileges to users.

The Default Admin Superuser

For security reasons, Oracle strongly recommends that you replace the default Admin Superuser (admin) in P6 immediately after a manual database installation or an upgrade from P6 version 7.0 and earlier. Since P6 requires that at least one Admin Superuser exists at all times, execute the procedures below in the order specified.

1) Follow the steps in ***Creating User Accounts for P6 EPPM*** (on page 125) to create a new user.
2) Follow the steps in ***Assigning Global Security Profiles*** (on page 130)to assign "Admin Superuser" as the global profile for the new user.
3) Follow the steps in ***Assigning Module Access*** (on page 136) to assign at least one of the following module access rights: Portfolios, Projects, or Resource.
4) Create a new Admin Superuser then delete the original Admin Superuser, "Admin" by default.

> **Note:** Only Admin Superusers can create, edit, and delete other Admin Superusers. You must have at least one Admin Superuser to create other Admin Superusers.

Creating User Accounts for P6 EPPM

Follow these steps to create new user accounts for applications in P6 EPPM including P6, P6 Professional, and P6 Team Member interfaces. These steps represent the minimum you must do to create a user account. You can also configure user access to grant or deny a user's access to data.

> **Note**: When you copy a user the user's settings are copied. The new user will have the same Resource Access, Global Security Profile, Project Access, Module Access, Global Preferences, User Interface View, Dashboards, Activities Toolbars, Activities Views, EPS Toolbars, EPS Views, Resource Assignment Toolbars, and Resource Assignment Views as the copied user. The user's Associated Resource, E-mail address, Phone, and View Preferences are not copied. If the users view is grouped by global security profile or user interface view and you select a different grouping band before pasting a copied user, the new user will be assigned with the global security profile or user interface view corresponding to the grouping band you selected.

To create a new user account:

1) Launch **P6** as an administrator.
2) Click the **Administer** ▼ menu and select **User Access**.
3) In the **User Access** pane, click **Users**.
4) On the **Users** page, click the ✛ **Add** icon.
5) What appears next depends on your security configuration:

To add users in Native authentication mode see ***Adding Users in Native Authentication Mode*** (on page 127).

To add users in LDAP or SSO authentication mode see ***Adding Users in LDAP or SSO Authentication Mode*** (on page 127).

> **Note**: If you want further information about creating new users with provisioning in Oracle Identity Manager, refer to the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

Tips

- For a video tutorial about creating User Accounts, please visit the following knowledge article: How To Configure User Access In P6 [Video] [ID 1462852.1]
- Give each user a unique name with up to 30 alpha-numeric characters.
- 🛡 Oracle recommends using strong passwords. Strong passwords in P6 EPPM contain between 8 and 20 characters and at least one numeric and one alpha character. To further strengthen the password, use a mixture of upper and lower case letters.
- 🛡 For security reasons, Oracle strongly recommends that you replace the default Admin Superuser (admin) immediately after a manual database installation or an upgrade from P6 version 7.0 and earlier.

Adding Users in Native Authentication Mode

If P6 is configured for native authentication you add users with the **Add User** dialog box.

To add users in native authentication mode:

1) Fill in the **Login Name**, **Personal name**, **Password**, and **Confirm Password** fields.
2) Click **Add**.
3) If the ability to edit a personal resource calendar or access to P6 Team Member is required, you can select an **Associated Resource** in the **Users** table at this time, or you can create the link when you add resources.
4) In the **Users** table, add the **E-mail** and **Phone** columns (if they are not already present), and enter the appropriate data.
5) Click ▣ **Save**.

> **Notes**:
>
> - Your user name can be a maximum of 30 characters.
> - If you intend to use BI Publisher, avoid using commas when creating data other than Project names. The way that data other than Project names is passed to BI Publisher can cause a comma to be interpreted as a delimiter between data items.
> - The assigned **Global Security Profile** will determine the user's capabilities.
> - 🛡 When the **Password Policy** is enabled, the password must be between 8 and 20 characters and contain at least one number and one letter. The policy is enabled by default.
> - When the **Password Policy** is disabled, the password must be between 1 and 20 characters. The application does not allow blank passwords.

Adding Users in LDAP or SSO Authentication Mode

If P6 is configured for LDAP or SSO authentication mode you add users with the **Add Users From LDAP** dialog box.

To add users in LDAP or SSO authentication mode:

> **Notes**:
> - If you intend to use BI Publisher, avoid using commas when creating data other than Project names. The way that data other than Project names is passed to BI Publisher can cause a comma to be interpreted as a delimiter between data items. You may need to work with your Network Administrator to make sure that User names do not include commas.
> - 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.
> - The new users will be assigned the default global profile unless you selected to copy another users settings.

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.

A list of users appears, grouped by status. For example, LDAP repository users that do not exactly match P6 EPPM users are 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 Primavera P6 Administrator 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.

3) 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.
   a. If you are importing from LDAP:
      1. Click the **Copy preferences from (optional):** button.
      2. In the **Select a User** dialog box, select the user whose settings you want to apply to the imported users. Click **OK**.
   b. If you are importing from LDAP:
      1. Select the **Create resources from imported users** option to save time and effort in creating resources.

2. In the **Select Parent Resource** dialog box, select the resource where you want create the new resources. Click **Add**.

> **Note**: If you selected the **Create resources from imported users** option, the resources are created and the **Associated Resource** column is populated when you save the changes in the **User Access** page.

4) Click **Import**.
5) On the **Users** page, click 💾 **Save**.

Configuring User Access

For security purposes, configure user access controls to grant or deny user's access to data.

To configure user access, see:

- ▸ *Assigning Associated Resources* (on page 129)
- ▸ *Assigning Global Security Profiles* (on page 130)
- ▸ *Assigning Module Access* (on page 136)
- ▸ *Assigning OBS Elements to Users* (on page 136)
- ▸ *Assigning Resource Access* (on page 137)

Tips

Show or hide columns on the **Users** page to configure additional user access options.

Assigning Associated Resources

Assign an associated resource to the user profile to connect the user with a resource in the application. Each user can have only one resource assigned, and a resource cannot be assigned to more than one user at the same time. Not all users require an associated resource, but users must have a resource assigned to enable them to edit their personal resource calendars and use P6 Team Member Web or P6 mobile. Also, by associating a resource with a user, the user will be able to see all projects to which the resource is assigned using the Activities page in P6 if the user is assigned Contributor module access.

To assign an associated resource:

1) Click the **Administer** ▾ menu and select **User Access**.
2) In the **User Access** pane, click **Users**.
3) On the **Users** page:
   a. Select a user.
   b. In the **Associated Resource** field, double-click and click ⬚.
4) In the **Select Resource** dialog box, select a resource and click **Assign**.
5) On the **Users** page, click 💾 **Save**.

Tip:

If the resource you need to assign to the user does not yet exist, you can create one quickly by clicking 👤**Create Resource from Selected Users**.

Assigning Global Security Profiles

Every user is assigned a global security profile by default. You can change a global security profile for every user to control user access to application-wide information.

To change the user's global security profile:

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **Users**.
3) On the **Users** page:
   a. Select a user.
   b. In the **Global Security Profile** field, double-click and choose a profile from the list.

   > **Note**: The assigned **Global Security Profile** will determine the location of the user in the **Users** tab hierarchy if they are grouped by the global profile.

   c. Click 💾 **Save**.

Tips

▶ You must have the appropriate privileges to assign security attributes.
▶ An Admin Superuser is a global security profile that gives a user read/write privileges for application-wide information and features. The Admin Superuser always has access to all resources. If resource security is enabled, resource access settings are not applicable. To make global information read-only for a user, choose No Global Privileges. The No Global Privileges profile provides read-only access to all global data except costs and secure codes.

Module Access Definitions

Selecting a module access option gives the user access to the following:

Notes:

- If users need to access P6, they must have one of the following module access rights: Projects, Portfolios, Resources, Contributor, or Enterprise Reporting.

- All modules provide access rights to E-mail Statusing Service and P6 mobile. If users need access to P6 Team Member Web, they must have Team Member or Timesheet module access rights. Only users with Timesheet module access rights will be permitted to display and enter time in the Timesheets tab of P6 Team Member Web module.

- All module access rights except P6 Integration API, Analytics, P6 Professional, Team Member Interfaces, and P6 EPPM Web Services provide access to Dashboards in P6; however, the Dashboards menu items that are available depend on the user interface view and whether users are assigned the Timesheet Approval security privilege. Also, the portlets that are available on the Dashboards Home page are based on each user's module access rights and configuration of the Primavera P6 Administrator, and the data that is displayed in the Dashboards portlets are dependent on each user's security privileges.

Contributor option

Determines limited user access to P6, such as the Dashboards and Projects sections (Workspace and Activities pages). For user interface views, only the options on the Activity Editing tab apply to contributors. Access to P6 functionality is additionally determined by a user's OBS access and relationship to the project, that is, whether the user is assigned as a resource to activities or designated as an activity owner. You must clear all other module access options in order to select Contributor module access; conversely, you must clear Contributor module access in order to select any other module access option.

Enterprise Reports option

Determines user access to the Reports section in P6. By selecting this module access option, the P6 EPPM user will be able to run reports.

Note: Security for reports is enforced when the report is executed. See the *Connecting BI Publisher to P6* guide for more information on security.

Integration API option

Determines user access to log into the PMDB database through P6 Integration API via Java.

P6 Analytics option

Determines user access only to the Star database through Oracle Business Intelligence. By selecting this module access option, a Star user is created for the P6 EPPM user as long as the user name matches Oracle database user name requirements. For example, if the P6 EPPM user name begins with anything other than a letter, a Star user cannot be created. Once a Star user is created, the user will be able to access the Oracle Business Intelligence Dashboards application.

P6 Professional option

Determines user access to P6 Professional.

Portfolios option

Determines user access to the following functionality in P6: the Portfolios section, Project Performance portlets, the Portfolio View portlet in the Dashboards section, document management functionality (if the Content Repository is configured), and workflow functionality (if the integration with BPM is configured).

Projects option

Determines user access to the following functionality in P6: the Projects section, Project Performance portlets in the Dashboards section, document management functionality (if the Content Repository is configured), and workflow functionality (if the integration with BPM is configured).

Resources option

Determines user access to the following functionality in P6: the Resources section, Resources portlets in the Dashboards section, document management functionality (if the Content Repository is configured), and workflow functionality (if the integration with BPM is configured).

Team Member option

Determines user access to the P6 for Android and P6 for iOS mobile apps and P6 Team Member interfaces: P6 Team Member Web and E-mail Statusing Service. All modules provide access rights to E-mail Statusing Service, P6 for Android, and P6 for iOS on iPhone, but only the Team Member Interfaces module access option provides access rights to P6 Team Member Web and P6 for iOS on iPad.

Timesheet option

Determines user access to Timesheets in P6 Team Member.

Visualizer option

Determines user access to Visualizer.

Web Services option

Determines user access to P6 EPPM Web Services, which uses open standards, including XML, SOAP, and WSDL, to seamlessly integrate P6 EPPM functionality into other applications. Using P6 EPPM Web Services, organizations can share P6 EPPM data between applications independent of operating system or programming language.

Tips

▶ Some P6 EPPM products, such as the P6 Professional SDK, do not require module access.

▶ Users can view project data in P6 without Contributor module access as long as they have Portfolios, Projects, or Resources module access. When this is the case, users can view data for a project when they have OBS access to the project, they are assigned as a resource to an activity in the project, or they are the project owner. For more detailed information on Contributor module access, see *What Does the Contributor Module Access Enable a User to Access?* (on page 133).

What Does the Contributor Module Access Enable a User to Access?

Contributor module access provides access to some P6 functionality. The following sections describe P6 functionality that a Contributor user can access.

In general, all users with Contributor module access can:

▶ create private and multi-user dashboards
▶ import calendar nonwork time
▶ create private and multi-user activity views
▶ set their own preferences

Depending on OBS access to projects (as described in the following sections), users with Contributor module access can also:

▶ add/edit project issues
▶ add/edit resource assignments
▶ add activity steps
▶ edit activity dates
▶ edit activity status
▶ add/edit/delete activity relationships
▶ add/edit activity expenses
▶ add/edit activity notebook topics
▶ add/edit user-defined fields
▶ add private documents

> **Note:** If you assign a user interface view to a user who has only Contributor module access, all view settings, except Activity Editing options, are ignored; the functionality available to Contributor users is controlled by module access rights. For example, even if the assigned user interface view allows the display of all Administration tasks, Contributor module access will only display My Preferences and My Calendar (if applicable). See *Defining User Interface Views* (on page 138) for more information on assigning user interface views.

Dashboards

In the Dashboards section of P6, Contributor users can create private and multi-user dashboards and approve timesheets (with the required security privilege). Dashboard portlets display data for projects the user is associated with that meet the criteria of the specified Dashboard Filter. Together, a user's association with a project, OBS access, and security privileges, determine the level of view and edit access that is granted to project data. A Contributor can be associated with a project via OBS access, by assignment as an activity resource, by assignment as an activity owner in a Reflection project (P6 Professional only), and by assignment as an activity owner in a What-if project (will appear in P6 only).

> **Note:** The Reflection project and activity owner features can be used together to collect and review activity progress information from Contributor users who are not assigned as activity resources. For more details, refer to the *P6 Professional Help*.

Contributor users can access the following Dashboards portlets (full functionality is available except where noted):

▸ My Projects
▸ My Workgroups
▸ My Activities
▸ My Risks — Users can view, but not add, risks.
▸ My Issues — Users without OBS access to a project can view, but not add, issues. Users with OBS access to a project can add issues with the required security privilege.
▸ Communication Center
▸ My Documents — Users can add private documents only. This portlet is available only when the Content Repository is configured for use with P6, regardless of a user's module access.
▸ My Calendar
▸ Document Reviews — This portlet is available only when the Content Repository is configured for use with P6, regardless of a user's module access.
▸ Workflows — This portlet is available only when the Workflows Repository is configured for use with P6, regardless of a user's module access.
▸ Cost Worksheet
▸ Custom Portlet

All other portlets are not available to Contributor users.

Projects

In the Projects section of P6, Contributor users can access the Open Project dialog and the Workspace and Activities pages.

The **Open Projects dialog** can be organized by EPS, portfolio, or project code. Within each grouping category, the dialog displays all projects to which the user has OBS access, all projects in which the user is assigned as an activity resource, all Reflection projects in which the user is designated as an activity owner (P6 Professional only), all What-if projects in which the user is designated as an activity owner (P6 only), and all projects in which the user is designated as a project owner. Users can access the Open Projects dialog by choosing Open Projects from the Projects menu in the global navigation bar.

The **Activities page** in the Projects section displays all activities the user is associated with either as an assigned resource or as an activity owner. Users who are associated with activities, but who do not have OBS access rights, can view, print, and export data but cannot access features and functions that change project data. For example, they cannot edit activity data in the table, modify the Gantt chart, or modify activity details. Users associated with activities who have OBS access to the project and the required security privileges can access, add, and edit activities, edit fields in the Activity Table, modify Gantt chart bars, establish relationships, print, export, and import information.

> **Note:** Contributor users cannot delete activities or add/edit WBS elements.

In the **Workspace page**, Contributor users can access the following portlets (full functionality is available except where noted):

▸ Project Documents — Users can view, download, and check out, but not add, project documents. Advanced document management capabilities are only available when the Content Repository is configured for use with P6, regardless of a user's module access rights.
▸ Project Risks — Users can view, but not add or edit, project risks.
▸ Project Issues — Users without OBS access to the project can view, but not add or edit, project issues. Users with OBS access to the project can add and edit issues if they are assigned the required project privilege.
▸ Project Notebooks — Users can view, but not add or edit, project notebooks.
▸ Overallocated Resources
▸ Critical activities behind schedule — Users can view all activities behind schedule for the project. For users without OBS access to the project, all activity details accessed from this portlet are read-only. For users with OBS access to the project, users can edit activity details accessed from this portlet if they have the appropriate security privileges and are a resource on the activity or are the activity owner.
▸ Milestone status — Users can view all milestone activities for the project. For users without OBS access to the project, all activity details accessed from this portlet are read-only. For users with OBS access to the project, users can edit activity details accessed from this portlet if they have the appropriate security privileges and are a resource on the activity or are the activity owner.
▸ Communication Center

▶ Project Calendar — Users can view all activities for the project scheduled for the selected week. For users without OBS access to the project, all activity details accessed from this portlet are read-only. For users with OBS access to the project, users can edit activity details accessed from this portlet if they have the appropriate security privileges and are a resource on the activity or are the activity owner.

▶ Workgroups

▶ Custom Portlet

▶ Contract Management portlets — Users can view all Contract Management portlets if P6 is configured to access Contract Management and the P6 project is linked to a Contract Management project.

All other Workspace portlets are only available to Contributor users if they are granted access when you customize the project workspace.

Assigning Module Access

Assign user module access to allow or deny the user access to different parts of the application.

To assign user module access:

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **Users**.
3) On the **Users** page:
   a. Select a user.
   b. In the **Module Access** field, double-click and click ⊡.
4) In the **Module Access** detail window, select options to grant access to each module or feature set.
5) On the **Users** page, click 💾 **Save**.

Assigning OBS Elements to Users

Assign OBS elements to a user to control their access to the EPS and projects.

> **Caution**: Users assigned to an OBS that is assigned to the root EPS have access to all projects at all levels.

To assign OBS elements to a user:

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **Users**.
3) On the **Users** page, select a user.
4) In the **Project Access** detail window:
   a. Click 🖼️ **Add**.
5) In the **Select Responsible Manager** dialog box:
   a. Select a **Project Security Profile**.
   b. Select one or more OBS element from the list and click **Assign**.
   c. Select additional Project Security Profiles and additional OBS elements as necessary.
   d. Click **Close** when finished.
6) On the **Users** page, click 💾 **Save**.

Tips

▸ You can also assign users to OBS elements using the Users Detail Window of the OBS Page in *P6 Help*.

▸ Project access settings are not applicable to users with the special *Admin Superuser* global security profile. The *Admin Superuser* profile always has access to all projects.

▸ To remove an OBS assignment, select an element in the **Project Access** detail window and click ✖ **Delete**.

Assigning Resource Access

You can control which resources a user can access.

To control resource access:

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **Users**.
3) On the **Users** page:

    a. Select a user.

    b. In the **Resource Access** field, double-click ⬚.

4) In the **Specify Resource Access** dialog box, select one of the following and click **Assign**:

    ▸ **No Resources**: to deny the user access to resources. This is the default resource access setting for new users.

    ▸ **All Resources**: to grant the user access to all resources.

    ▸ **Select Resources**: to grant the user access to the selected resource node and its children.

    > **Note**: You can assign only one node to a user.

5) On the **Users** page, click 💾 **Save**.

Tips

▸ Resource access settings are not applicable to Admin Superusers. Superusers always have access to all resources.

▸ Resource access changes go into effect almost immediately for P6 users. P6 Professional users should exit the application and log in again for the changes to take effect.

▸ If a resource is deleted from the resource hierarchy, users that previously had been assigned to the deleted resource will automatically be assigned to the **No Resources Access** option.

Defining User Interface Views

In addition to module access and security privileges, you can further control access to P6 functionality with user interface views. A user interface view is a defined set of tabs, pages, and menu items that a user assigned to that view can access in the main sections of P6 (Dashboards, Portfolios, Projects, and Resources). It also helps to control the fields that a user can edit in the Activity page. You can create multiple user interface views that correspond to the job functions performed by each role in your organization, or you can create user interface views to meet each individual user's needs.

> **Note:** You can designate one user interface view as the default view for new users. The default view controls user access to functionality only for new users who are not already assigned a user interface view. When you paste a copied user, however, the new user will have the same user interface view as the copied user. If the user you copy has modified their user interface view, the pasted user will be assigned the default view. Existing users who do not have an assigned user interface view can continue to access all functionality. You can define the default view for new users on the **User Interface Views** page using the **User Interface View for new users** list. See the *P6 Help* for more information.

Creating User Interface Views

Create a user interface view to optimize user to module interaction. The user interface view permits visibility to features essential for a role while hiding functionality that is not applicable. You can choose to create a brand new user interface view or modify an existing view.

To create a user interface view:

1) Click the **Administer** ▼ menu and select **User Interface Views**.
2) On the **User Interface Views** page, click **Create User Interface View**.
3) In the **Copy from Existing User Interface View** dialog box:
   a. Choose **New User Interface View** to create a new user interface view, or select an existing user interface view to use as a starting point.
   b. Click **OK**.
4) On the **Create User Interface View** page, click the **Content** tab:
   a. Enter a unique name in the **User Interface View Name** field.
   b. Select which section the new user interface view should show when it is first opened from the **Start Page** list.
   c. Expand each section and select options for menu items and pages you want to include in the view.
      ▪ If you select the option next to **Menu Items** or **Pages**, all items will be included in the view. Conversely, if you clear the option, none of those items will be displayed in the view.
      ▪ Click the ⬇ **Move Down** or ⬆ **Move Up** to configure the sequence of items. The first item listed in each section is designated as the first page for that section. For example, if **Activities** is the first item listed for **Projects Pages**, when a user opens a project, the **Activities** page will be displayed automatically.

5) On the **Create User Interface View** page click the **Activity Editing** tab:

   a. Expand each section and select the option in the **Edit** field to allow the user to edit that section.

      ▪ If you select the option next to the name of the section, all items in that section will be editable. **Global Activity Codes**, **EPS Activity Codes**, **Project Activity Codes**, and **User Defined** do not have the select all option; you must select each code individually.

6) On the **Create User Interface View** page, click the **Users** tab:

   a. Select a user from the **Available Users** window to assign the user to that view.

      ▪ Click ▶ **Select** to move the user to the **Selected Users** column.

      ▪ Select the **Allow Editing** option to enable the user to edit the contents of their interface view.

   b. Select a user from the **Selected Users** window to remove the user from that view.

      ▪ Click ◀ **De-select** to remove the user.

7) Click **Save and Close**.

Tips

▶ Users can view their interface view settings on the **My Preferences** page **View** tab.

▶ Continue to configure views over time in line with changing roles, capabilities, features, and organizational needs.

▶ You can quickly add users to a user interface view by double-clicking their name in the **Available Users** column. Likewise, you can remove users from a view by double-clicking their name in the **Selected Users** window.

▶ You can also assign user interface views on the **Users** page.

Assigning User Interface Views

Assign user interface views to users to give users a view that is optimized for their role. User interface views permit visibility to features essential for a user's role and determine the default start page, while hiding functionality that is not applicable. You can assign user interface views only if you have the necessary privileges.

To assign a user interface view:

1) Click the **Administer** ▾ menu and select **User Access**.

2) In the **User Access** pane, click **Users**.

3) On the **Users** page:

   a. Select a user.

   b. In the **User Interface View** field, double-click and click ▣.

4) In the **Select User Interface View** dialog box, select a user interface view and click **Assign**.

5) On the **Users** page, click ▣ **Save**.

Deleting User Accounts

Delete a user account when an employee has left the organization or the user no longer requires access to P6.

> **Note**: If a user has P6 Team Member module access or is associated with a resource and has actual working hours on a project, deactivate the user account instead of deleting it to avoid loss of data.

To delete a user:

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **Users**.
3) On the **Users** page:
   a. Click on the user.
   b. Click ✖ **Delete**.
   c. Click 💾 **Save**.

Tips

If a resource is associated with a user, the resource remains in the database. Determine if the resource needs to be deleted from the Resources Administration page or if the resource should be marked as inactive. To indicate a resource is inactive, clear the Active column for the resource on the **Resources Administration** page.

Deactivating User Accounts

Deactivate a user account when an employee has left the organization or the user no longer requires access to P6. Deactivate the account instead of deleting the user if the user uses P6 Team Member or when you need to retain the history of actual working hours on the projects the user is assigned to. Deleting a user will cause historical data to change.

To deactivate a user account:

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **Users**.
3) On the **Users** page:
   a. Click on the user.
   b. Click the **Module Access** detail window.
4) In the **Module Access** detail window, clear the **Access** option for all modules.
5) Click 💾 **Save**.

Tips

If the user is assigned an associated resource, the resource and the resource assignments remain in the database.

Deleting Resources

Delete a resource when the resource no longer works at the organization. Deleting a resource deletes the resource, all child resources, and all assigned activities.

> **Note**: Do not delete the resource if you want to retain resource assignments. Instead, clear the **Active** option for the resource on the **Resources** tab on the **Resources Administration** page.

1) Click **Resources**.
2) On the **Resource** page, click the **Administration** tab.
3) On the **Administration** tab:
   a. Click on the resource.
   b. Click ✖ **Delete**.
   c. If the resource has assignments, you are prompted to reassign the assignments to another resource or delete the resource without reassigning the resource's assignments. Make your selection and click **OK**.

   > **Note**: Reassigning the assignments to another resource will replace the resource for all activity assignments, regardless of the activity status (Not Started, In Progress, Completed) or the status of the project (Planned, Active, Inactive, What if).

   d. Click 💾 **Save**.

Changing Passwords

Administrators can change a user's password and users can change their own passwords.

▸ Administrators: See Changing User Passwords.
▸ Users: See Changing Your Own Password.

Changing User Passwords

Administrators can change users' passwords.

To change a user password:

1) Click the **Administer** ▾ menu and select **User Access**.
2) In the **User Access** pane, click **Users**.
3) On the **Users** page:
   a. Select a user.
   b. Click 🔒 **Change Password**.
4) In the **Change Password** dialog box:
   a. In the **New Password** field, enter a new password.

   > **Notes**:
   >
   > - 🛡 When the **Password Policy** is enabled, the password must be between 8 and 20 characters and contain at least one number and one letter. The policy is enabled by default.
   > - When the **Password Policy** is disabled, the password must be between 1 and 20 characters. The application does not allow blank passwords.

   b. In the **Confirm New Password** field, enter the new password again for verification and click **OK**.
5) On the **Users** page, click 💾 **Save**.

Tips

You cannot change passwords if you are running P6 EPPM in LDAP or SSO authentication mode.

Changing Your Own Password

Users can change their own password at any time.

> **Note**: You cannot change passwords if you are running P6 EPPM in LDAP or SSO authentication mode.

To change your own password:

1) Click the **Administer** ▼ menu and select **My Preferences**.
2) On the **My Preferences** page, click the **Password** tab.
3) On the **Password** tab:
    a. In the **Current Password** field, enter the current password.
    b. In the **New Password** field, enter a new password.

    > **Notes**:
    >
    > - ⬤ When the **Password Policy** is enabled, the password must be between 8 and 20 characters and contain at least one number and one letter. The policy is enabled by default.
    > - When the **Password Policy** is disabled, the password must be between 1 and 20 characters. The application does not allow blank passwords.

    c. In the **Confirm New Password** field, enter the new password again for verification.
    d. Click **Save**.

Counting Users

As an aid in determining whether you have reached licensing limitations, use the Count feature to view the number of users assigned access to each P6 EPPM module:

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **Users**.
3) On the **Users** page, click ▦ **Count**.
4) In the **Count** dialog box, view the user count by module.
    a. If needed, click 📊 **Export to Excel** or 🖨 **Print** to create an output of the results.

Resetting User Sessions

Reset a locked-out user's session to grant the user rights to initiate a new session. Users may be locked out if they have attempted to log in while a session is already running, or if they have repeatedly entered incorrect login information.

> **Notes**:
>
> - You can use the Primavera P6 Administrator to specify the number of times a user can fail to login before P6 locks them out. The default setting is 5.
> - Accounts that are locked out, but not reset, will become available after a length of time defined in the Primavera P6 Administrator. The default setting is 1 hour.

To reset user sessions:

1) Click the **Administer** ▼ menu and select **User Sessions**.
2) On the **User Sessions** page:

> **Caution**: Oracle recommends that users only be reset if they are locked out. Clearing sessions for active users can have adverse effects in the application.

- ▶ To reset all user sessions, click **Reset All Users**.
- ▶ To reset only the selected user, click **Reset User**.

Tips
- ▶ A user account that is locked out is highlighted in red and denoted by an asterisk.
- ▶ You must be an Admin Superuser to access the **User Sessions** page.
- ▶ The **User Sessions** page displays users who are currently logged in, users who left the application but did not log out, and users whose failed login count exceeds the acceptable threshold.

About the OBS

The organizational breakdown structure (OBS) is a hierarchical way to represent the managers responsible for the projects in your enterprise. You can associate the responsible managers with their areas of the enterprise project structure (EPS) with either an EPS node or a project. When you associate a responsible manager with an EPS node, any projects you add to that branch of the EPS are assigned that manager element by default. An OBS supports large projects that involve several project managers with different areas of responsibility.

To access a project, a user must have access permissions for an OBS element within the project. You can then assign users to OBS elements. When you assign users to OBS elements, users get access privileges to projects and EPS nodes where they have OBS access. These access privileges are not passed down to child OBS elements. If some users need access to multiple OBS elements, you must assign those users to all of the OBS elements they need to access. The type of access granted to a user is determined by the project security profile assigned to the user.

Working with the OBS

Use the OBS page to assign projects to responsible managers in your enterprise.

Table of OBS Page

Item	Description
❶	**OBS page**: Use the **OBS** page to assign responsible managers to a project.
❷	**Responsibility tab**: Use this tab to view an OBS' Project ID/WBS Code and Project Name/WBS Name. You can associate the responsible managers with their areas of the EPS—either nodes or individual projects. When you associate a responsible manager with an EPS node, any projects you add to that branch of the EPS are assigned that manager by default.
❸	**Users tab**: Use this tab to give users specific access to an OBS. To access a project, a user must have access permissions for an OBS element within the project. This provides user access to WBS information for which the specified OBS element is responsible, as well as limits user access to WBS information that might lie beyond the user's scope.
❹	**Description tab**: Use this tab to add a description about the OBS. To add a description, you will double-click in the **Description** field on the OBS page and type in a description on the **Description** tab.

Creating an OBS

Create an organizational breakdown structure (OBS) to hierarchically represent the managers responsible for your projects. You must have the appropriate privileges to create an OBS.

To create a new OBS:

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **OBS**.
3) On the **OBS** page:
   a. Click ✛ **Add**.

   > **Note**: The OBS is automatically added as a child of another OBS.

   b. Move the OBS to the correct location in the list and hierarchical position by clicking the ⬆ **Move Up**, ⬇ **Move Down**, ⬅ **Move Left**, or ➡ **Move Right** arrows.
   c. In the **OBS Name** field, double-click and type a unique name.
   d. Click the **Users** detail window.
4) In the **Users** detail window, remove or assign users to the OBS.
   ▸ To remove a user from the OBS, select a user and click the ✖ **Delete** icon.
   ▸ To assign users to the OBS, click the ✛ **Add** icon.
5) In the **Select Users** dialog box:
   a. Select a **Project Security Profile**.
   b. Select one or more users and click **Assign**.
   c. When you are finished assigning users, click **Close**.
6) On the **OBS** page, click 💾 **Save**.

Tips

▸ When you set up enterprise project structure (EPS) nodes, a root OBS is automatically assigned to the root EPS.
▸ When you create a new project, the default responsible manager is automatically assigned so that an OBS element is available for each work breakdown structure (WBS) element added to the project.

Assigning OBS Elements and Project Profiles in P6 EPPM

To restrict or grant access to projects and their data, you must assign project profiles to users. A project profile is a role-based profile that limits privileges to specific project data, such as baselines, the WBS, and expenses. Project profiles are linked to users through one or more OBS assignments. You assign responsibilities to specific projects and work within projects by assigning OBS elements to various levels of the EPS and each project's WBS.

The combination of the user assignment to an OBS element, and the OBS assignment to the EPS/project/WBS, determines which projects and project data the user can view. For each OBS element a user is assigned to, the user's assigned project security profile (per OBS assignment) further determines the project data the user can view or edit.

> **Note:** OBS assignments can be made at both the project and WBS levels; therefore, a project and its WBS elements might have different OBS assignments. When this occurs, a user's OBS assignment/project security profile only applies to WBS elements that have the same OBS assignment as the project; for WBS elements with a different OBS assignment than the project, the data is read-only for users that are not assigned to the same OBS element as the WBS element. To grant a user rights (beyond read-only rights) to a WBS element that has a different OBS assignment than the project, you must assign the user to the same OBS element that the WBS element is assigned to, then select the appropriate project security profile for the new OBS assignment.

You can assign a user an OBS element and a corresponding project profile in the Users table when you are adding users, or you can make the assignment in the OBS tab during or after creating the OBS.

You need to assign a user to an OBS (or an OBS to a user) for a user to access a project. When that assignment is made, the default project profile is automatically related to and made available to the user. You can subsequently assign a different project security profile to that user. See *Defining Project Security Profiles in P6 EPPM* (on page 114) for more information on project profiles.

Assigning Users to an OBS

Except for a project owner or a Contributor user, a user must have permission to access an organizational breakdown structure (OBS) to access a project assigned to that OBS. If you have appropriate privileges, you can assign users to OBS elements using their login names.

> **Caution**: Users assigned to an OBS that is assigned to the root EPS have access to all nodes beneath the root.

To assign users to an OBS:

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **OBS**.
3) On the **OBS** page, select an OBS and click the **Users** detail window.
4) In the **Users** detail window, click **Assign User**.
5) In the **Select Users** dialog box:
   a. Select a **Project Security Profile** with which you want to assign users.
   b. Select one or more users and click **Assign**.
   c. Select additional Project Security Profiles and assign additional users as necessary.
   d. Click **Close** when finished.
6) On the **OBS** page, click **Save**.

Tip:

You can also select multiple OBS elements in the OBS page then assign one or more users to them simultaneously by selecting **Assign User** in the Users detail window.

Assigning OBS Elements to Users

Assign OBS elements to a user to control their access to the EPS and projects.

> **Caution**: Users assigned to an OBS that is assigned to the root EPS have access to all projects at all levels.

To assign OBS elements to a user:

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **Users**.
3) On the **Users** page, select a user.
4) In the **Project Access** detail window:
   a. Click 🖼 **Add**.
5) In the **Select Responsible Manager** dialog box:
   a. Select a **Project Security Profile**.
   b. Select one or more OBS element from the list and click **Assign**.
   c. Select additional Project Security Profiles and additional OBS elements as necessary.
   d. Click **Close** when finished.
6) On the **Users** page, click 💾 **Save**.

Tips

▸ You can also assign users to OBS elements using the Users Detail Window of the OBS Page in *P6 Help*.

▸ Project access settings are not applicable to users with the special *Admin Superuser* global security profile. The *Admin Superuser* profile always has access to all projects.

▸ To remove an OBS assignment, select an element in the **Project Access** detail window and click ✖ **Delete**.

About the Enterprise Project Structure (EPS)

The enterprise project structure (EPS) represents the hierarchical structure of all projects in the database. The EPS can be subdivided into as many levels or nodes as needed to represent work at your organization. Nodes at the highest, or root, level might represent divisions within your company, project phases, site locations, or other major groupings that meet the needs of your organization; projects always represent the lowest level of the hierarchy. Every project must be included in an EPS node.

The number of EPS levels and their structure depend on the scope of your projects and how you want to summarize and aggregate data. For example, you might want to define increasingly lower levels of EPS nodes, similar to an outline, to represent broad areas of work that expand into more detailed projects. Specify as many projects as needed to fulfill the requirements of your operations executives and program managers.

Multiple levels enable you to manage projects separately while retaining the ability to aggregate and summarize data to higher levels. For example, you can summarize and aggregate information for each node in the EPS. Conversely, you can use top-down budgeting from higher-level EPS nodes down through their lower-level projects for cost control.

User access and privileges to nodes within the EPS hierarchy are implemented through a global organizational breakdown structure (OBS) that represents the management responsible for the projects in the EPS. Each manager in the OBS is associated with an area of the EPS, either by node or by project, and the WBS of the particular level of the hierarchy.

Once you have added users and associated them with OBS elements and project profiles, you can define the EPS and assign a responsible manager (OBS element) to each level. You must specify a responsible manager for each node of the EPS.

Working with the EPS

Your P6 projects are arranged in a hierarchy called the enterprise project structure, or EPS. The EPS can be subdivided into as many levels or nodes as needed to parallel work at your organization. Nodes at the highest, or root, level might represent divisions within your company, project phases, site locations, or other major groupings that meet the needs of your organization. Projects always represent the lowest level of the hierarchy. Every project must be included in an EPS node.

Ideally, one person or group controls the EPS across the organization. The project control coordinator creates the hierarchical structure that identifies the company-wide projects. The coordinator works with the project manager in each area of the organization to define basic project information for each group and to develop standards before any projects are added.

After you set up an EPS, you can define additional data about each EPS division, such as anticipated dates, budgets, and spending plans. Use the detail windows on the EPS page to specify this information. Or, you can begin adding projects under the applicable levels in the structure if you have access rights to these functions. Access rights are set by your application administrator.

Throughout the application, when selecting projects to work with, you can open all projects that belong to an EPS node or sort them by EPS. When you create a project, you must specify a single parent EPS node. User access and privileges to nodes within the EPS hierarchy are implemented through a global OBS that represents the management responsible for each project. Each manager in the OBS is associated with an area of the EPS, either by node or by project, and the WBS of the particular level of the hierarchy.
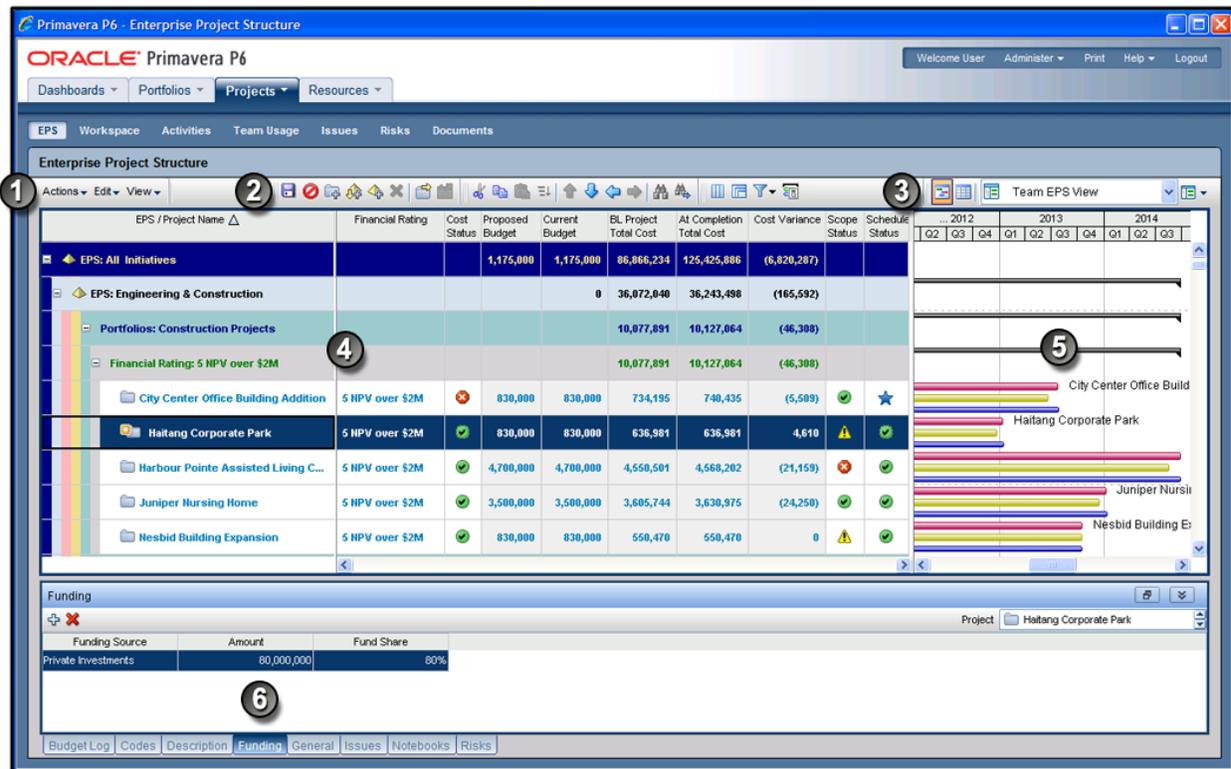
Table of Key EPS Page Elements

Item	Description
❶	**Actions, Edit, and View menus**: Use these menus to work with and customize the **EPS** page.
❷	**EPS toolbars**: Customize the toolbars to include icons that you use most often.
❸	**EPS View toolbar**: Determines how you see data on the **EPS** page.
❹	**EPS/Project table**: Displays each project within the EPS. In this example, the data is grouped by **EPS**, then by **Portfolio**, and then by a project code called **Financial Rating**. The table is sorted by **Project Name**.
❺	**EPS Gantt chart**: Displays project and EPS data in a Gantt chart format.
❻	**Detail Windows**: The **Funding** detail window for the project selected in the table. Additional detail windows appear along the bottom of the table.

Assigning OBS Elements to the EPS

You must specify a responsible manager for each node in the EPS to enable security rights and privileges; P6 EPPM uses the uppermost level of the OBS to which you have access as the default for all nodes. You can change the responsible manager (OBS element) for each level of the EPS.

> **Caution**: Users assigned to an OBS that is assigned to the root EPS have access to all nodes beneath the root.

To assign OBS elements to the EPS:

1) Click **Projects**.
2) On the **Projects** navigation bar, click **EPS**.
3) On the **EPS** page, select an EPS node, double-click the **Responsible Manager** field, and click the browse button.
4) In the **Select Responsible Manager** dialog box, select the appropriate OBS element and click **OK**.

> **Notes**:
>
> - The users associated with the responsible manager will have access rights to the selected EPS node and all nodes/projects within that branch. The specific data that can be accessed within the projects depend on the project profile that corresponds to the OBS element.
> - If more than one user is responsible for the same node of the EPS, you must assign each of those users to the corresponding OBS element.

Tips

▸ Once the EPS and OBS structures are defined and security is implemented at the EPS level, project managers can begin to add their own projects to the hierarchy. To further control security within projects, project managers can assign specific OBS elements to WBS levels.

▸ If the **Responsible Manager** field is not available in the table, open the **Customize Columns** dialog box and add **Responsible Manager** to the **Selected Columns** list.

▸ You may also assign an OBS element to the EPS from the **General** detail window on the **EPS** page.

Defining User Access to Resources in P6 EPPM

Resource security enables you to restrict a user's access to resources. Each user can have access to all resources, no resources, or a limited number of resources in the resource hierarchy. To provide access to a limited number of resources, you can designate each user's root resource by assigning each user to a resource in the resource hierarchy. The position of the assigned resource in the hierarchy determines the user's resource access. When the user logs in, the resource hierarchy displays only the assigned resource node and its children. Resources outside the user's root resource are not displayed.

> **Note:** Users with restricted resource access can still view and edit all current project resource assignments if they have the proper project privileges.

You can grant one of the following three types of resource access to each user:

▶ **No Resource Access** does not provide access to any resources. This is the default option for new users. With no resource access, the user cannot view any global resource data in the resource dictionary.

▶ **All Resource Access** disables resource security and provides access to all resources. With all resource access, the user can view all global resource data in the resource dictionary. This is the default option for upgrading users. Admin Superusers always have all resource access, no matter which option is selected.

▶ **Select Resource Access** provides access to one selected resource (root resource node) and all its children in the resource hierarchy. Users with this restricted access can view global resource data for resources they have access to.

> **Note:** You can assign only one resource node to each user. Multiple resource nodes are not supported.

The following example shows how resource access is determined by the root resource assigned to different users.
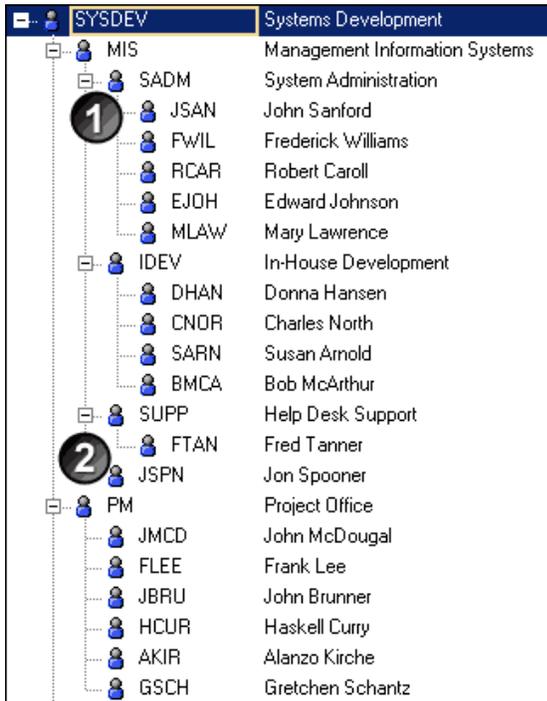
Item	Description
❶	If USER1 has restricted access with root resource SADM assigned, USER1 would see only these resources in the resource dictionary. Includes the following resources: SADM, JSAN, FWIL, RCAR, EJOH, and MLAW.
❷	If USER2 has restricted access with root resource SUPP assigned, USER2 would see only these resources in the resource dictionary. Includes the following resources: SUPP and FTAN.
❸	If USER3 has no resource access, USER3 would not see any resources in the resource dictionary.

See the *P6 Help* for more information on setting up the resource hierarchy.

Tip

All Resource Access is required for certain features in P6 EPPM. For example, you must have All Resource Access in order to import resources into the resource dictionary via Microsoft Excel (.xls) format.

Assigning Resource Access

You can control which resources a user can access.

To control resource access:

1) Click the **Administer** ▼ menu and select **User Access**.

2) In the **User Access** pane, click **Users**.

3) On the **Users** page:

    a. Select a user.

    b. In the **Resource Access** field, double-click 🔲.

4) In the **Specify Resource Access** dialog box, select one of the following and click **Assign**:

    ▸ **No Resources**: to deny the user access to resources. This is the default resource access setting for new users.

    ▸ **All Resources**: to grant the user access to all resources.

    ▸ **Select Resources**: to grant the user access to the selected resource node and its children.

> **Note**: You can assign only one node to a user.

5) On the **Users** page, click 💾 **Save**.

Tips

▸ Resource access settings are not applicable to Admin Superusers. Superusers always have access to all resources.

▸ Resource access changes go into effect almost immediately for P6 users. P6 Professional users should exit the application and log in again for the changes to take effect.

▸ If a resource is deleted from the resource hierarchy, users that previously had been assigned to the deleted resource will automatically be assigned to the **No Resources Access** option.

Application Settings and Global Enterprise Data in P6 EPPM

P6 enables your organization to define a series of module-wide parameters and values that apply globally and to all projects in an enterprise project structure (EPS). Use these settings to customize the module to meet specific project management requirements and standards.

This chapter highlights some of the settings that you can specify: Application Settings, which contains default administrative preferences, and the global category of the Enterprise Data pane, which contains standard values that apply to all projects.

> **Note:** All other categories of Enterprise Data are covered in the *P6 Help*.

The P6 Administrator can choose to hide Application Settings and Enterprise Data from users. Even if users can view Application Settings and Enterprise Data, they must have the proper security privileges to edit them.

Working with Application Settings

Use Application Settings to specify default administrative preferences established by the P6 Administrator. The P6 Administrator must give you access to Application Settings to view them and the 'Edit Application Settings' privilege for you to adjust them.
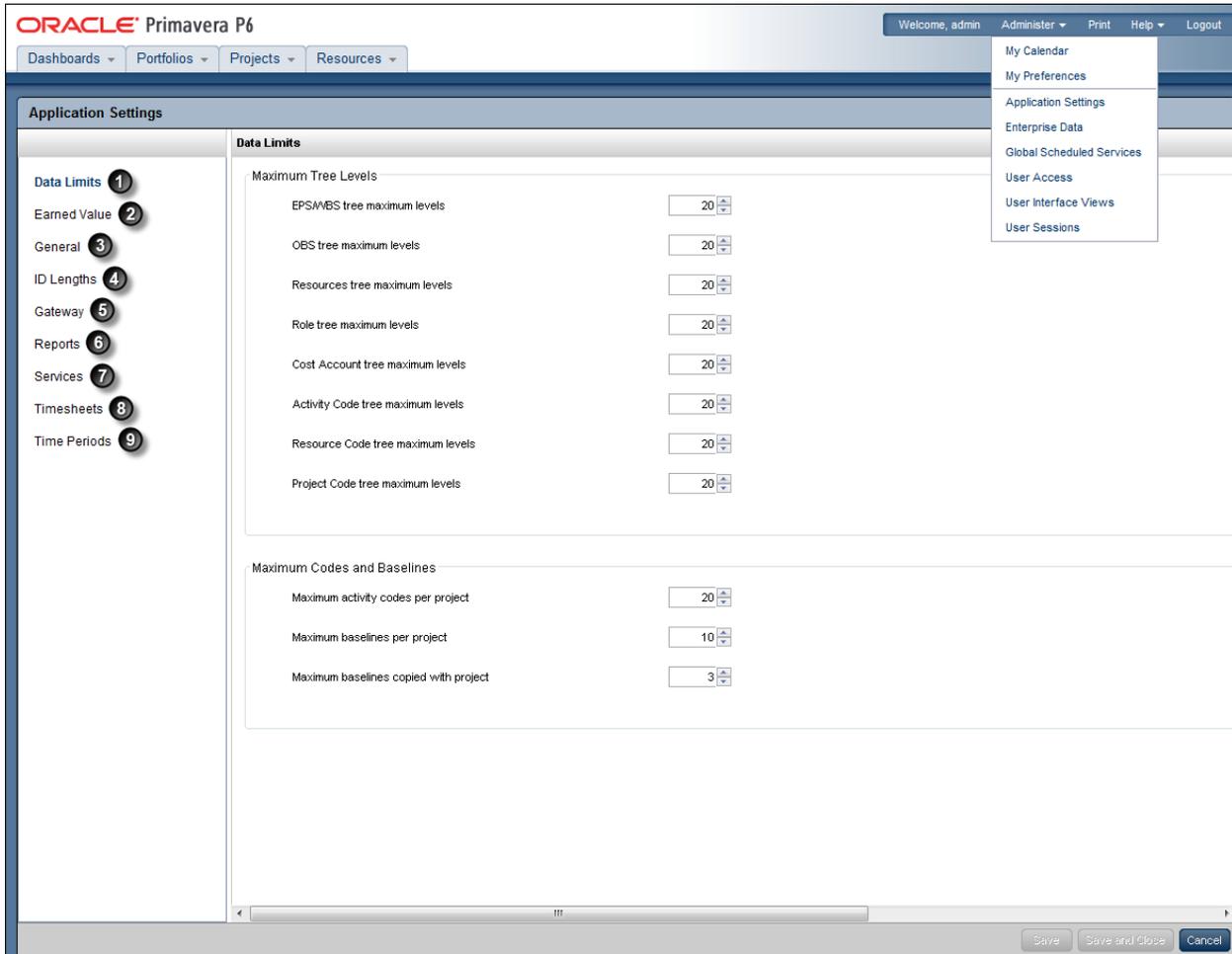
Table of Application Settings Elements

Item	Description
❶	**Data Limits**: Specify the maximum number of levels for hierarchical structures and the maximum number of codes and baselines.
❷	**Earned Value**: Specify default settings for calculating earned value.
❸	**General**: Specify general default options, such as the weekday on which the calendar week begins.
❹	**ID Lengths**: Specify the maximum number of characters for IDs and codes.

Item	Description
⑤	**Gateway**: Specify connection information and parameters for working with Primavera Gateway.
⑥	**Reports**: Specify the headers and footers available for reports in Oracle Primavera P6 Visualizer.
⑦	**Services**: Specify publication and summarization periods and configure project publication options.
⑧	**Timesheets**: Specify default setup options when using the Timesheets tab in P6 Team Member.
⑨	**Time Periods**: Define the default number of hours in a workday, workweek, workmonth, and workyear, or specify that the default number of work hours for each time period is defined per calendar.

Data Limits Page

Overview

Use this page to specify maximum levels for hierarchical structures. You can also specify baseline and activity code maximums.

Screen Elements

Maximum Tree Levels section

Select a value for each of the following fields:

EPS/WBS: Enter the maximum number of levels for the EPS and WBS hierarchies.

Cost Account: Enter the maximum number of levels for Cost Account hierarchies.

OBS: Enter the maximum number of levels for the OBS hierarchy.

Activity Code: Enter the maximum number of levels for Activity Code hierarchies.

Resources: Enter the maximum number of levels for Resources hierarchies.

Resource Code: Enter the maximum number of levels for Resource Code hierarchies.

Role: Enter the maximum number of levels for Role hierarchies.

Project Code: Enter the maximum number of levels for Project Code hierarchies.

Maximum Codes and Baselines section

Select a value for each of the following fields:

Activity Codes per Project: Enter the maximum number of activity codes allowable per project.

Baselines per Project: Enter the maximum number of baselines allowable per project.

Baselines copied with Project: Enter the maximum number of baselines to be copied per project.

Tips

If you change maximum hierarchy level settings, the new settings apply only when you add new elements or edit existing elements.

Getting Here

1) Click the **Administer** ▼ menu and select **Application Settings**.
2) On the **Application Settings** pane, click **Data Limits**.

Earned Value Page

Overview

Use this page to specify default settings for calculating earned value. You can change the settings for specific WBS elements in the Earned Value detail window in Activities page.

Screen Elements

Technique for computing performance percent complete section

In this section, choose one of the following for computing performance percent complete:

Activity Percent Complete: Select to calculate the earned value according to activity completion percentages.

WBS Milestones: Select to calculate the earned value by defining milestones at the WBS level and assigning a weight to each of them.

0/100: Select to calculate the earned value as 100 percent after the activity ends.

50/50: Select to calculate the earned value as 50 percent after the activity starts and until it ends. After the activity ends, the activity's earned value is 100 percent.

Custom Percent Complete: Select to enter a percent to calculate earned value after the activity starts and until the activity ends. After the activity ends, the activity's earned value is 100 percent.

Technique for computing estimate to complete (ETC) section

Determines whether estimate to complete (ETC) is equal to remaining cost or a performance factor (PF) multiplied by (Budget at Completion minus Earned Value).

Earned Value Calculation section

Determines how earned value is calculated from a baseline.

Getting Here

1) Click the **Administer** ▼ menu and select **Application Settings**.

2) On the **Application Settings** pane, click **Earned Value**.

General Page

Overview

Use this page to specify general default options.

Screen Elements

Starting Day of Week

First day of week for calendars list

Use the arrow to choose a day. The start day of the week affects how all days in a week are displayed in profiles, spreadsheets, and other layouts in which a weekly timescale can be displayed. For example, if Wednesday is selected as the starting day of the week, the week is displayed as WTFSSMT.

> **Note**: When using View Calendar or going to Calendar views in Enterprise Data, the **First day of week for calendars** setting is ignored.

Activity Duration

Default duration for new activities field

The default duration for new activities in all projects. Having a default duration simplifies the process of adding new activities.

Code Separator

Code separator character field

The character that separates hierarchy levels in roles, resource codes, project codes, cost accounts, issue codes, activity codes, and risk categories; it is also the default separator for WBS codes in all new projects.

Industry Selection

Select the industry to use for terminology and default calculation settings in the P6 Professional module list

Use the arrow to choose the type of industry in which you use this application. The industry you choose causes P6 Professional to use terminology and default settings for calculations that most closely align with the selected industry.

Engineering and Construction: Determines the use of terminology and default settings for calculations aligned with the engineering and construction industries.

Government, Aerospace, and Defense: Determines the use of terminology and default settings for calculations aligned with government and with aerospace and defense industries.

High Tech, Manufacturing, and Others: Determines the use of terminology and default settings for calculations aligned with high-technology, manufacturing, and other industries.

Utilities, Oil, and Gas: Determines the use of terminology and default settings for calculations aligned with the utility, oil, and gas industries.

> **Note**: Until an industry is selected P6 Professional users will see a message each time they log in which explains that this option has not been set.

Password Policy

Enable option

Determines whether to enable the password policy.

Use the Password Policy to authorize a password that is 8-20 characters long and that contains at least one letter and one number.

Online Help

Online Help URL for P6 Professional field

The help URL that will allow users to access help for P6 Professional. If this field is left blank, the Online Help option will not be available and Local help will always launch when the F1 key or Help shortcut are used.

Leave the default URL to launch the Oracle Technology Network (OTN) site when Online Help is selected from the Help menu.

Remove the URL to disable the Online Help option from the Help menu for all users. Users will only be able to access the local version of the help.

Specify a new URL location to launch when Online Help is selected from the Help menu.

Using OTN ensures that you always have the most current help content.

Always launch the Online Help for the F1 shortcut key and context sensitive help option

Switch on this option if your users have access to the internet and need to be able to see the most up to date version of Help. If this option is switched off, accessing Help via the F1 key and Help shortcuts will always show local help. This option is off by default.

Document Management

Enter the P6 URL to enable users to view content repository documents in the P6 Professional module field

The P6 URL that will enable users to view content repository documents in P6 Professional.

Contract Management

Contract Management URL field

The Contract Management URL that will enable access to Contract Management from P6.

Unifier**:**

Primavera Unifier URL field

The Primavera Unifier URL that will enable users to access Primavera Unifier from P6.

Company Short Name field

The Company Short Name for accessing the Primavera Unifier database.

Authentication Code field

The Authentication Code for accessing the Primavera Unifier database.

P6 Professional Applications

Use remote mode for P6 Professional Update Baseline, Schedule Compare and XML Import option

Switch on this option if you want P6 Professional to run Update Baseline, Schedule Compare, and XML Import procedures using the API in Remote Mode. If you choose to use this feature, ensure that P6 Professional users configure their connection to the P6 database using the P6 Pro Cloud Connect driver.

Integration API Server URL field

The URL of the Integration API server which will perform the calculations for Update Baseline, Schedule Compare, and XML Import for P6 Professional.

> **Note**:
>
> - Although these settings are intended for P6 Professional users who need or prefer to perform these functions using the API in Remote mode, performance for these features might also be improved for P6 users by running these features using the API in Remote mode.

Getting Here

1) Click the **Administer** ▾ menu and select **Application Settings**.
2) On the **Application Settings** pane, click **General**.

ID Lengths Page

Overview

Use this page to specify the maximum number of characters for IDs and codes.

Screen Elements

Project ID field

The maximum number of characters that a project ID may have.

WBS Code field

The maximum number of characters that a WBS code may have.

Resource ID field

The maximum number of characters that a resource ID may have.

Activity ID field

The maximum number of characters that an activity ID may have.

Cost Account ID field

The maximum number of characters that a cost account ID may have.

Role ID field

The maximum number of characters that a role ID may have.

Getting Here

1) Click the **Administer** ▾ menu and select **Application Settings**.
2) On the **Application Settings** pane, click **ID Lengths**.

Gateway Page

Overview

Use this page to specify general default options.

Screen Elements

Gateway Parameters:

API Url field

The Primavera Gateway URL that will allow you to integrate other products with P6 and P6 Professional.

Username field

The name of the Gateway user with the administrative privileges.

Password field

The password of the Gateway user who has administrative privileges.

Test Connection button

Tests that the address specified in the **API Url** field can be accessed using the **Username** and **Password** specified.

P6 Deployment field

Enter a name for the P6 deployment to be integrated with Primavera Gateway.

Integration Parameters:

Add button

Adds a new integration parameters line to the table.

Refresh button

Refreshes the list of selected deployments and synchronizations from Gateway.

Action Type list

Determines what action to take:

Import: Allows the import of the data specified in the **Source/Destination Deployment**, **Synchronization**, and **Action Name** columns.

Export: Allows the export of the data specified in the **Source/Destination Deployment**, **Synchronization**, and **Action Name** columns..

Source/Destination Deployment field

Determines the source or destination deployment to connect to.

Synchronization list

The synchronizations available based on the source or destination deployment selected.

Action Name field

The name that will appear on the Exchange Data menu.

Add button

Adds a new integration parameters line to the table.

❌ **Delete** (Delete)

Deletes the selected data items or table rows.

Getting Here

1) Click the **Administer** ▼ menu and select **Application Settings**.
2) On the **Application Settings** pane, click **Gateway**.

Reports Page

Overview

Use this page to define three sets of header, footers, and custom labels for P6 Professional reports and Visualizer diagrams.

Screen Elements

First Set area

Define a header, footer, or custom text label for reports or diagrams.

Second Set area

Define a second header, footer, or custom text label for reports or diagrams.

Third Set area

Define a third header, footer, or custom text label for reports or diagrams.

Header Label 1, 2, or 3 field

The custom text that will be inserted into any report or diagram containing a Header Label 1, Header Label 2, or Header Label 3 variable text cell, when printed or drawn. You can type new header text. The maximum number of characters is 255.

Footer Label 1, 2, or 3 field

The custom text that will be inserted into any report or diagram containing a Footer Label 1, Footer Label 2, or Footer Label 3 variable text cell, when printed or drawn. You can type new footer text. The maximum number of characters is 255.

Custom Label 1, 2, or 3 field

The custom text that will be inserted into any report or diagram containing a Custom Label 1, Custom Label 2, or Custom Label 3 variable text cell, when printed or drawn. You can type new custom text. The maximum number of characters is 255.

> **Note**: The labels can be used by choosing them as variables in Page Setup. Variables can be set in Visualizer on the Title Block tab of the Page Setup tab. Variables can be set in P6 Professional on the Header and Footer tabs of the Page Setup dialog box. These labels cannot be used in P6.

Getting Here

1) Click the **Administer** ▼ menu and select **Application Settings**.
2) On the **Application Settings** pane, click **Reports**.

Services Page

Overview

Use this page to configure publication and summarization period settings.

Screen Elements

Publication section:

Start date field

Determines the date on which publication for time-distributed data will begin. Oracle recommends that this value be set to the earliest project start date in the database so that time-distributed reports can be produced for any date range, if your organization reports against past project data. If this value is changed after data has been published, all project and global data will be automatically recalculated.

You must be assigned the *Admin Superuser* global security profile to edit this field.

Finish date is current date plus list

Determines the future period of time that is added to the current date of the service whenever it runs to determine the finish date for publication of time-distributed data. Data is published covering the period of time that begins with the start date and extends through the finish date. If this setting is changed after data has been published, all project and global data will be automatically republished. Set this value to an interval that will allow users to produce time-distributed reports for a reasonable amount of time in the future. This value should typically be in the 2-5 year range.

For example, if the value is 5 years, time-distributed data will always be published covering the period of time that begins with the value in the Start Date field and extends five years into the future each time a service runs.

You must be assigned the *Admin Superuser* global security profile to edit this field.

Time distributed interval list

Determines the interval by which time-distributed data will be calculated and stored. If this setting is changed after data has been published, all project and global data will be automatically republished. Set to Day if this level of granularity is required for spread data. Set to Week if performance of the services is most important (this may only be necessary for very large databases). The default setting is Day.

You must be assigned the *Admin Superuser* global security profile to edit this field.

Enable Publish Projects option

Determines whether Publish Projects is enabled. This option must be marked to publish projects and to run the Check Overallocation service. You should not enable Publish Projects until all projects are ready for publication.

You must be assigned the *Edit Application Settings* security privilege to modify this option.

Publish projects every list

Determines the interval by which projects are polled to be published. The interval should be set to a low number (less than 5 minutes) to ensure that ASAP Publish Project and Check Overallocation services are processed in a timely fashion. However, if your users will not be using these ASAP services, you can set this value higher.

Publish a changed project when the...

Number of changes exceeds field

Determines the number of edits that can be made to project tables before the Publish Projects service is automatically initiated. The number of changes resets each time the service is run for a project. Set this value to a low number if you want to ensure that changes to projects are reflected in the extended schema tables as soon as possible. Set to a higher number if changes to a project do not need to be reflected in the extended schema immediately, or if the time threshold is sufficient in most cases for publishing projects. The default setting is 100.

Time since last publication exceeds field

Determines the time interval that must elapse since a project was last published before the *Publish Projects* service is automatically initiated again. This setting only applies to projects that have changed during the time interval, but have not exceeded the number of changes threshold and therefore have not yet been automatically queued for publication. Set this value to a timeframe in which your project data must be current in the extended schema tables. For example, if you set this to 24h, this ensures that all projects actively being worked on will be published at least once a day, even if the edit threshold is not passed.

Publish idle projects option

Adds migrated projects to the service queue after your database is upgraded, if your organization is upgrading to P6.

This will publish all your projects in the queue and refresh the available data for reporting. After all projects have been published once, this setting is not applicable, and projects will be submitted to the queue based on the threshold values specified on the **Application Settings** page. Do not mark this checkbox if you only want to publish projects actively being worked on to the extended schema tables. If your organization does not report against completed projects, it may not be necessary to publish projects not actively being worked on.

Maximum number to publish field

Determines the maximum number of idle projects that can be added to the service queue. This setting is only applicable immediately following an upgrade, when all projects are considered idle.

When all projects have been published, the service queue will no longer be constrained based on this setting.

Enable Baseline Publication option

Determines whether to allow baseline data to be published for reporting.

Summarization section:

Summarize by Calendar option

Determines whether to display the summarization periods by calendar.

WBS Level list

Use the list arrow to choose Week or Month.

Resource/Role Assignment Level list

Use the list arrow to choose Week or Month.

Summarize by Financial Periods option

Determines whether to display the summarization periods by financial periods.

Getting Here

1) Click the **Administer** ▼ menu and select **Application Settings**.
2) On the **Application Settings** pane, click **Services**.

Timesheets Page

Overview

Use this page to specify default timesheet options and approval levels for P6 Team Member Web.

Screen Elements

General:

Allow resources to assign themselves to activities by default option

Determines whether you want every newly created project to grant permission for resources to assign themselves to activities. When you change this setting, it does not affect existing projects; the new setting is applied only when a new project is created. For individual projects, you can override this setting on the Project Preferences dialog box in the EPS page.

Enable timesheet auditing option

Determines whether you want to save the history of timesheet submission, approval, rejection, reviewers, and associated dates. To view the historical data, you must create reports using BI Publisher.

Approving Timesheets:

Auto Submission - No submission or approvals is required option

Select to indicate that resource timesheets do not need to be submitted or approved.

Auto Approval - Automatically approve upon submission option

Select to indicate that resource timesheets do not require management approval. Timesheets are approved automatically when they are submitted.

One approval level - Resource manager approval required option

Select to indicate that resource timesheets require approval by the resource manager only. If you select this option, the status of all submitted timesheets remains **Submitted** until the approving manager changes the timesheet's status. If you previously required both project manager and resource manager approval, and you select this option, the status of all current timesheets that have received one level of approval changes to **Approved**.

Two approval levels - Project and Resource managers' approval required option

Select to indicate that resource timesheets require approval by project and resource managers. If you select this option, the status of all submitted timesheets remains "Submitted" until both managers approve the timesheet.

Project manager must approve before Resource manager option

Determines whether project managers must approve timesheets before resource managers. The **Two Approval Levels** option must be selected to enable this option.

Default Resource manager approving timesheets when one or two approval levels required field

Select the approver you want to approve timesheets for resources. The default approver will be assigned each time you create a resource who uses timesheets.

Getting Here

1) Click the **Administer** ▼ menu and select **Application Settings**.
2) On the **Application Settings** pane, click **Timesheets**.

Time Periods Page

Overview

Use this page to define the number of hours in a given time period. You can also specify abbreviations for time units.

Screen Elements

Hours per Time Period fields

The values that will be used as conversion factors when users choose to display time units and durations in units other than hours.

For example, if the default Hours/Day is set to 8.0, when a user enters 1d as a duration, this value is stored as 8h in the database.

For this field, you can enter Hours/Day from 1.0-24.0, Hours/Week from 1.0-168.0, Hours/Month from 1.0-744.0, and Hours/Year from 1.0-8784.0.

Use assigned calendar to specify the number of work hours for each time period option

Determines whether to use the assigned calendar's Hours per Time Period values as the conversion factors when users choose to display time units and durations in units other than hours. If your resources and activities require different hours per time period settings, select this option, then specify the Hours per Time Period in each defined calendar.

If you select the **Use assigned calendar to specify the number of work hours for each time period** option, the **Hours per Time Period** values on this tab are ignored and the application converts units and durations using the **Hours per Time Period** values defined in the activity's or resource's assigned calendar. Using a task-dependent activity as an example, P6 converts units and durations for the activity using the settings defined in the activity's assigned calendar.

You should enter **Hours per Time Period** values on this tab even if you mark the **Use assigned calendar to specify the number of work hours for each time period** option since those values will still be used in the following cases:

▸ The **Planning** page of the Resources section in P6.
▸ The **Planning Resources** tab in the project and WBS views and Global Change in P6 Professional.

In these cases, the **Use assigned calendar to specify the number of work hours for each time period** option will be ignored even if selected.

If you clear the **Use assigned calendar to specify the number of work hours for each time period** option, the **Hours per Time Period** values that you specify on this tab are always used to convert time units and durations.

Time Period Abbreviations fields

The one-character abbreviations for minutes, hours, days, weeks, months, and years.

Getting Here

1) Click the **Administer** ▼ menu and select **Application Settings**.
2) On the **Application Settings** pane, click **Time Periods**.

Using Calendars to Define Hours Per Time Period Settings

P6 EPPM calculates and stores time unit values in hourly increments, but users can set preferences to display time units in other increments, such as days or weeks. The values specified for Hours per Time Period are used to convert hours to other time increments for display, and to convert all non-hourly time increments to hours for storage in the database. As an administrator, from Application Settings, Time Periods tab, you can define Hours per Time Period settings globally, or you can specify that the Hours per Time Period settings should be defined per calendar.

When Hours per Time Period settings are defined per calendar, units and durations are displayed more accurately. When Hours per Time Period settings are defined globally and users set preferences to display units and durations in time increments other than hours, units and durations will display unexpected values when the Application Settings for Hours per Time Period do not match the work hours specified in calendars assigned to projects, activities, and resources. This occurs because the display reflects the conversion factor of the Application Settings Hours per Time Period settings, not the hours per day defined by the project's, activity's, or resource's assigned calendar. For example:

▶ User Preferences, Time Units = day
▶ Application Settings, Hours per Time Period = 8h/d
▶ Activity calendar, Work hours per day = 10h/d
▶ User-entered activity duration = 30h
▶ Actual duration display = 3d6h (30h duration/8h per day, based on the conversion factor set in Application Settings)
▶ Expected duration display = 3d (30h duration/10h per day, based on the conversion factor set in the activity calendar)

To avoid unexpected display results:

1) Select the 'Use assigned calendar to specify the number of work hours for each time period' option on the Time Periods tab of Application Settings.
2) Specify the Hours per Time Period settings for each defined calendar.
3) Assign these calendars to the appropriate activities and resources.

Working with Enterprise Data

Use the **Enterprise Data** page to configure various types of data settings commonly used by other features in the application. Your settings reflect the data recognized by your industry or organization and help to meet your project management requirements and standards.

Table of Enterprise Data Elements

Item	Description
❶	**Global section**: Click **Global** to customize global data, such as currencies and financial periods.
❷	**Projects section**: Click **Projects** to customize project-specific data, such as baseline types and funding sources.
❸	**Activities section**: Click **Activities** to customize activity data, such as activity codes and cost accounts.
❹	**Resources section**: Click **Resources** to customize resource and role data, such as rate types and resource codes.
❺	**Risks section**: Click **Risks** to customize risk data, such as risk categories and thresholds.
❻	**Issues section**: Click **Issues** to customize issue data, such as issue codes and UDFs.
❼	**Documents section**: Click **Documents** to customize document data, such as document categories and statuses.

About Currencies

Currencies are the monetary units used to store costs for all projects in the database. Monetary units are stored in the database with a base currency that you select. The base currency is used to display costs in windows and dialog boxes. If you select a different currency than the base currency to view costs, the exchange rate for the base currency is always 1.0. The base currency value is multiplied by the current exchange rate for the view currency to calculate the values displayed in cost fields. For example, if the base currency is U.S. Dollars, the view currency is Euros, and the exchange rate for Euros is .75, a value of 10 dollars is displayed as 7.5 Euros in cost fields for windows and dialog boxes. Similarly, if you enter 7.5 Euros in a cost field, it is stored in the database as 10 dollars.

Admin Superusers and users with the 'Edit Currency' privilege can change the base currency and define additional view currency types. When you enter values in cost and price fields, they are always displayed in the user's view currency.

Use the Currencies view to set up the base and view currencies. For information on how a user can change the view currency, see the *P6 Help*.

> **Note:** If you are installing P6 EPPM for the first time, you should set up the base currency in the new version before you start adding and changing projects. It is not possible to change the base currency once projects are in progress.

The Base Currency

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

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

For example, if the base currency is US Dollars, the view currency is Euros, and the exchange rate for Euros is $1 = €0.75, a value of $10 stored in the database is displayed as €7.5 in cost and price fields. Similarly, if you enter €7.5 in a cost or price field, it is stored in the database as $10.

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

Defining a Base Currency

The base currency is U.S. dollars by default. The exchange rate for the base currency is always one.

To define a different currency as the base:

1) Click the **Administer** ▼ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Currencies**.
3) On the **Currencies** page:
    a. Select the row that has **BASE RATE** in the **Exchange Rate** field.
    b. Double-click in the **ID**, **Name**, and **Currency Symbol** fields and enter the base currency's information.

        For example, if you want the pound to be the new base currency, you can type in U.K. for the ID, British Pound for the name, and £ for the currency symbol.
    c. Display other fields, such as decimal digits and positive format, and edit as needed.
4) Click 💾 **Save** (Ctrl+S)

Adding a Currency

To add a currency:

1) Click the **Administer** ▼ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Currencies**.
3) On the **Currencies** page:
    a. Right-click on a row and choose ✛ **Add** (Insert).
    b. In the new row added at the bottom of the list, specify the appropriate values for the new currency.
    c. Click 💾 **Save** (Ctrl+S).

About Financial Periods

Financial periods are predefined time periods you can apply to financial or scheduling data throughout the application to consistently measure and compare that data. Customized financial periods provide more accurate display and reporting of actual costs and units according to time increments recognized by your finance and accounting staff. Users can focus on a financial period and pinpoint how actual costs were incurred during that time.

A calendar year with 355 days, a fiscal quarter ending July 15, and a week from Sunday to Saturday are all examples of financial periods.

You must have the 'Add/Edit/Delete Financial Period Dates' global privilege to create, modify, or remove data in the Financial Periods dialog box. To store past period actuals for a project's defined financial periods, you must have the Store Period Performance and 'Add/Edit Activities Except Relationships' project privileges. To edit past period actual data in P6 Professional after storing period performance, users must have the 'Edit Period Performance' project privilege.

Creating Financial Periods

Create financial periods to measure and compare financial data. You can create annual, monthly, or weekly periods.

To create a financial period:

1) Click the **Administer** ▼ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Financial Periods**.
3) On the **Financial Periods** page:
   a. Click the ✛ **Add** icon.
   b. To change the default name for the new financial period, click the **Name** field, and enter a name.
   c. To change the **Start Date** field, directly enter a new date, or select a date from the common calendar tool.
   d. To change the **Finish Date** field, directly enter a new date, or select a date from the common calendar tool.
4) Click 💾 **Save** (Ctrl+S).

Tips

▸ To save time, consider generating financial periods in a batch rather than individually.

Although the application will alert you in each case, be aware of the following constraints when creating or configuring financial periods:

▸ You cannot introduce gaps in a series of financial periods. Any new periods you create must start or end flush with any existing entries. For example, if October 7-13 and October 14-20 are existing financial periods, you can create a new one that either ends on October 6 or starts on October 21.
▸ You cannot overlap financial periods. In order to serve their purpose, financial periods must represent unique slices of time.

▸ You can create financial periods with a duration of fewer than seven days (one week); however, you cannot view them in timescales in P6. Use P6 Professional if you need to view data by financial periods spanning increments of fewer than seven days (one week).

Creating a Financial Period Batch

You can create annual or quarterly periods one at a time; however, to speed the time required to add monthly or weekly periods, consider using the Generate Financial Period Batch feature.

To create a financial period batch:

1) Click the **Administer** ▾ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Financial Periods**.
3) On the **Financial Periods** page, click 🏭 **Add Batch**.
4) In the **Generate Financial Periods** dialog box:

   a. In the **Batch Start Date** field, click 📅 **Select Batch Start Date** and select a date from the calendar or type a start date.

   > **Note**: For example, the 31st of January 2010 would be 31-Jan-10.

   b. In the **Batch Finish Date** field, click 📅 **Select Batch Finish Date** and select a date from the calendar or type a start date in day-month-year format.

   c. Select a **Period Cycle** and use the up and down arrows to specify a number of weeks or months.

   d. Click **Create**.

5) In the **Primavera P6** alert dialog box, click **OK** to acknowledge that one new financial period has been created.
6) On the **Financial Periods** page:

   a. In the **Name** field, double-click and type a name.

   b. Click 💾 **Save** (Ctrl+S).

Tips

Although you are alerted in each case, be aware of the following constraints when creating or configuring financial periods:

▸ You cannot introduce gaps in a series of financial periods. Any new periods you create must start or end flush with any existing entries. For example, if October 7-13 and October 14-20 are existing financial periods, you can create a new one that either ends on October 6 or starts on October 21.

▸ You cannot overlap financial periods. In order to serve their purpose, financial periods must represent unique slices of time.

▸ You can create financial periods with a duration of fewer than seven days (one week); however, you cannot view them in timescales in P6. Use P6 Professional if you need to view data by financial periods spanning increments of fewer than seven days (one week).

Deleting a Financial Period

To delete a financial period:

1) Click the **Administer** ▼ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Financial Periods**.
3) Select the financial periods you want to delete.
4) Right-click on the row and choose ✖ **Delete** (Delete).
5) Click 💾 **Save**.

Tips

▶ You cannot delete a financial period that stores past period actuals for any project. If you attempt to delete multiple financial periods at the same time, none of the financial periods will be deleted if any period stores past period actuals for any project. In this case, to delete a financial period, you must archive and delete the project containing past period actuals, then delete the financial period.

▶ You can delete a financial period that has high-level assignment planning values (as entered on the Plan Resources page of P6) as long as the financial period does not contain past period actuals. When you delete a financial period that has high-level assignment planning values, the values are deleted as well.

About Calendars

Calendars enable you to define available workdays and workhours in a day. You can also specify national holidays, recognized holidays, project-specific work/nonworkdays, and resource vacation days. You can establish an unlimited number of calendars to accommodate different work patterns. There are three calendar pools: global, project, and resource. The global calendar pool contains calendars that apply to all projects in the database. The project calendar pool is a separate pool of calendars for each project in the organization. The resource calendar pool is a separate pool of calendars for each resource. You can assign multiple users a resource calendar that they can share, but cannot edit. You can also assign a personal calendar to a resource that will show up in My Calendars and that the resource can customize. You can assign resource or global calendars to resources, and global or project calendars to activities.

Assign calendars to each resource and activity to determine time constraints in a uniform way. For example, based on its calendar, a resource might not be available; or, if the resource is available, the activity might not fit the calendar requirements.

The application uses your calendar assignments for leveling resources, scheduling, and tracking activities.

Creating Global Calendars

Create global calendars to identify global work or nonwork days. You can use global calendars as base calendars when creating a resource or project calendar. The exception days in a global calendar appear in the resource or project calendar and are identified by a 🌐 (globe).

To create a global calendar:

1) Click the **Administer** ▾ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Global Calendars**.
3) On the **Global Calendars** page, click ➕ **Add** (Insert).
4) In the **Select Calendar to Copy** dialog box:
   a. Select the **Global** or **Resource** option.

   > **Note**: This determines which list of calendars you can select.

   b. Select a calendar and click **OK**.
5) On the **Global Calendars** page, click the **Calendar** tab.
6) On the **Calendar** tab, triple-click the **Name** field and enter a name.

   > **Note**: The application automatically assigns the name *New Calendar*.

7) On the **Global Calendars** page, click 💾 **Save** (Ctrl+S).
8) Configure the global calendar.

Configuring Global Calendars

Perform the following tasks when creating or updating a global calendar:

Setting Work Hours Per Time Period for Global Calendars

Configure the work hours per time period settings to specify the default number of hours in a work period for a calendar.

To set the number of work hours for each time period:

1) Click the **Administer** ▾ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Global Calendars**.
3) On the **Global Calendars** page:
   a. Click on the calendar you want to modify.
   b. Click 📅 **Edit Hours Per Period**.
4) In the **Set Time Periods** dialog box, click and type an hour value in each field, and then click **OK**.
5) Click 💾 **Save** (Ctrl+S).

Configuring the Standard Work Week for Global Calendars

Configure the standard work week for the calendar to set the work and nonwork days and hours for a standard work week.

To modify the standard work week:

1) Click the **Administer** ▼ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Global Calendars**.
3) On the **Global Calendars** page:
    a. Click on the calendar you want to modify.
    b. Click the **Standard Work Week** tab.
4) On the **Standard Work Week** tab, right-click on a working or nonworking timeslot and use the menu options to adjust the workday. You can also resize the working time to increase or decrease the work hours.
5) Click 🖫 **Save** (Ctrl+S).

Modifying Calendar Days on Global Calendars

Modify calendar days to account for work or nonwork days or hours that are different than the standard hours defined on the Standard Work Week tab.

To modify work or nonwork calendar days:

1) Click the **Administer** ▼ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Global Calendars**.
3) On the **Global Calendars** page:
    a. Click on the calendar you want to modify.
    b. Click the **Calendar** tab.
4) On the **Calendar** tab, right-click on a working or nonworking day and use the menu options to adjust the workday.

Click 🖫 **Save** (Ctrl+S).

Setting the Default Global Calendar

Choose a calendar to use as the default when new calendars are created.

To set the default global calendar:

1) Click the **Administer** ▼ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Global Calendar**.
3) On the **Global Calendar** page:
    a. Click on the calendar you want to designate as the default calendar.
    b. Click 📅 **Set As Default Calendar**.
    c. Click 🖫 **Save** (Ctrl+S).

About Overhead Codes

Overhead codes provide P6 Team Member Web timesheets users with a way to categorize their time. When applied on their timesheets, the codes help users log hours that are not associated with project activities. For example, users can enter time for vacations, holidays, sick time, or general administrative work.

Creating Overhead Codes

Create overhead codes for P6 Team Member Web users to add overhead activities to their timesheets to log timesheet hours that are not associated with the project.

To create an overhead code:

1) Click the **Administer** ▼ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Overhead Codes**.
3) On the **Overhead Codes** page:
   a. Click ✛ **Add** (Insert).
   b. In the **Name** field, double-click and type a unique code.
   c. In the **Description** field, double-click and type a unique name.
   d. Click 🖫 **Save** (Ctrl+S).

Tips

When you specify that two approval levels are required to approve timesheets, timesheets that contain only overhead activities bypass project manager approval and are sent directly to the resource/cost manager for approval. For timesheets containing a mix of regular and overhead activities, project managers can view, but not approve, the overhead activities.

About Timesheet Periods

The timesheet period is the amount of time a timesheet covers. The administrator defines the time covered by timesheet periods; for example, every two weeks, every four weeks, or every month. The administrator must create timesheet periods before the user can view and enter time on their timesheets.

Creating Timesheet Periods

Use timesheet periods to create ranges for your timesheets.

To create a timesheet period:

1) Click the **Administer** ▼ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Timesheet Periods**.
3) On the **Timesheet Periods** page:
   a. Click ✛ **Add** (Insert).
   b. In the **Start Date** field, double-click, click the down arrow, and select a date.
   c. In the **End Date** field, double-click, click the down arrow, and select a date.
   d. Click 🖫 **Save** (Ctrl+S).

Using Oracle Secure Global Desktop

You can use Oracle Secure Global Desktop to publish P6 EPPM and P6 Professional to remote users.

Check the tested configurations for supported versions of Oracle Secure Global Desktop.

For details on publishing Windows desktops see the Oracle Secure Global Desktop Administration Guide. You will find the Secure Global Desktop documentation library here: http://www.oracle.com/technetwork/documentation/sgd-193668.html.

P6 Team Member Setup Tasks

This chapter covers the tasks for P6 Team Member Web, P6 mobile, E-mail Statusing Service, and Timesheets.

In This Section

About P6 Team Member

The P6 Team Member is designed for individual contributors, or team members, to record their statuses and report their time using timesheets. Team members can also use E-mail Statusing Service and P6 mobile to status their tasks. P6 mobile allows access to P6 Team Member Web functionality. P6 Team Member Web, E-mail Statusing Service and the P6 mobile apps provide quick, convenient, and easy access to assigned tasks using the platform or device that accommodates your line of work.

Your project manager uses P6 to create and update the project schedule and task list. Depending on the project preferences the manager selected when creating the project in P6, the updates you make in the P6 Team Member Web, E-mail Statusing Service or P6 mobile will either apply immediately or require approval before they are applied to the project.

Work assignments in P6 Team Member are based on work distribution filters, or a team member being named as a resource assignment or an activity owner. As a team member, the P6 Team Member interfaces and the P6 mobile apps enable you to:

▸ View only your assigned tasks.
▸ Provide status on your tasks. The project manager customizes the status fields in your view. These fields can include time spent, time left, % complete, remaining duration, start date, and finish date.

Timesheets enable project team members to use the web to communicate timesheets and activity statuses directly to their organization's database, regardless of their location. this ensure that project managers are always working with the most up-to-date project information, making it easier to plan resources or resolve conflicts.

P6 Team Member Web

You can use P6 Team Member Web to:

▶ Modify your view to display your task list by project and by current status, including Active, Due, Overdue, Starred, or Completed. You can refine your task list even further by filtering on the basis of specific parameters, entering a term by which to filter, or providing a sort order for your list.

▶ Mark a task with a star to signify its importance to you. You can view all your starred tasks in one list when you select the Starred task list view in the app menu.

▶ View a list of all your steps for a task. Add, edit, or delete steps to more accurately reflect your work, if you are given the privileges by your project manager. You can enter the % complete to show progress and mark a step as complete when you finish a step.

▶ View the codes and UDFs associated with a task for additional information about the task. Update codes and UDFs if your project manager requires you to update task status using these fields.

▶ View predecessor and successor tasks related to a task and contact resources associated with related tasks.

▶ Communicate with the project manager or other team members through e-mail.

▶ Communicate with the project manager about a task by viewing and posting messages in the Discussion dialog box. All messages are saved with the selected task.

▶ View and edit notebook topics associated with a task to see or provide more information about the task.

▶ View documents associated with a task and contact resources associated with project documents.

▶ Enter up-to-the-minute information about your assignments and to record the time you spent working on each one, by submitting timesheets. Timesheets helps you to focus on the work at hand with a simple cross-project to-do list of your upcoming assignments.

E-mail Statusing Service

You can use E-mail Statusing Service to:

▶ Request a list of your current tasks through e-mail using the e-mail account associated with your P6 user account. You can request a filtered list of tasks by project; time frame; current status, including Active, Due, Overdue, Completed, or Starting; or by all the tasks that you starred.

▶ Reply to the e-mail you receive with your task list, record your progress, and send your updates.

Project managers can use E-mail Statusing Service to:

▶ Send a Welcome e-mail to new E-mail Statusing Service users, which includes the e-mail address to the E-mail Statusing Service, and instructions for requesting a task list and updating the list through e-mail.

▶ Send team members an e-mail request for status updates. Project managers can customize the task list sent to team members using the available filter options. Team members can provide status by replying to the e-mail with their updates.

Creating a New P6 Admin Configuration for P6 Team Member Web

If you installed P6 Team Member and P6 at the same time, a configuration for P6 Team Member was not created and you will have to create your own P6 Team Member configuration.

The following sections include information about how you can create a new P6 admin configuration for P6 Team Member Web with `dbconfigpv.cmd` (sh).

If you do not create a configuration for P6 Team Member, you will not be able to set the P6 Team Member Help URL or configure UPK for P6 Team Member.

Creating a New Primavera P6 Administrator Configuration

To create a Primavera P6 Administrator configuration:

1) Do one of the following:

   ▸ On Windows platforms, run `dbconfigpv.cmd` (located in the *p6home* directory that you specified when installing P6).

   ▸ On UNIX platforms, change to the *p6home* directory that you specified when installing P6, and run `dbconfigpv.sh`.

2) On the Setup and Configuration of the Primavera P6 Database dialog box, select the database type.

3) On the Please enter the following information. . . dialog box:

   a. Specify the database connection parameters. Type your database user name (for example, pubuser) and password, the database name, host address, and host port. The database name, host address, and host port are specific to your database installation. The Database Host Port field displays the default port for the database type you selected. You can edit this port.

   b. To use the SSL protocol to securely communicate between the P6 application server and the database server, select the SSL option. If you select the SSL option, you must specify an SSL-enabled port number in the Database Host Port field.

      Notes:

      ▪ See the appropriate database server documentation and the My Oracle Support's Knowledge Articles for information on configuring SSL.

      ▪ Using the SSL protocol will impact database performance.

   c. Ensure that the Public Group ID is 1 for a standard configuration.

4) Select **Create a new configuration** and then enter the name of your new configuration (for example, Team Member Configuration).

5) Click **Next**.

6) Click **OK**.

Configuring P6 Team Member Web Settings

To configure the settings for P6 Team Member Web, you must have a P6 Team Member Admin Configuration. See *Installing and Configuring P6 EPPM* for more information on how to create this configuration during a new installation of P6 Team Member Web or *P6 EPPM Post Installation Administrator's Guide* for more information on how to create this configuration for existing P6 Team Member applications.

To configure the settings for P6 Team Member Web:

1) Launch **Primavera P6 Administrator**.
2) Navigate to your P6 Team Member configuration, and then expand it.
3) Expand **Application**:
   a. Set the Help server URL to one of the following:
   ‣ `http://localhost:`*listenport*`/`*ContextRoot*

      where *localhost* is your server's host name, *listenport* is your P6 Team Member port number, and *ContextRoot* is the root for your Help.
   ‣ http://docs.oracle.com/cd/E54397_01/team_member/web/help/

      > **Note:** Oracle recommends that you use the second URL option because it ensures that you always access the latest version of the P6 Team Member Help, including critical corrections and enhancements.

4) Expand **User Productivity Kit** (UPK):
   a. Set the User Productivity Kit URL to `http://`*localhost*`:listen`*port*`/`*ContextRoot*

      where *localhost* is your server's host name, *listenport* is your P6 port number, and *ContextRoot* is the root for your tutorials (for example, P6Tutorials).
5) Expand **Team Member**:
   a. Expand **Connection Pool** if you want to alter the following default values:
      - **Initial connection pool size:** *10*
      - **Maximum active database connections:** *150*
      - **Maximum idle database connections:** *-1*
      - **Minimum idle database connections:** *10*
   b. Expand **Logging** if you want to alter the following default:
      - **Enable:** *enabled*
      - **Severity Level:** *Error*
      - **Log File Name:** *p6tmweb.log*

      > **Note:** The **primavera.bootstrap.home** property determines the location of the log file.

Configuring E-mail Statusing Service for P6

To configure E-mail Statusing Service for P6:

1) From the P6 Team Member home directory (for example, C:\P6EPPM_1\tmws), extract the files from the **p6tm-email-service.zip** to any location on the application server. (That location will be referred to as EMAIL_HOME).

2) Make a backup copy of the **config.properties** file before you edit it.

3) Edit the **config.properties** file to configure the settings for the e-mail application.

> **Note:** 🛡 When you are finished editing the config.properties file, move it to a secure location.

4) In the **P6 Configuration** section, locate and specify the following:

   a. In the **p6.admin.user =** line, specify a P6 user who is assigned to at least one module access and has resource access.

   b. In the **p6.notify.user =** line, specify the email addresses, separated by commas, of users who can send Notify Task lists to other users. As you   See the *P6 Help* for more information on sending team members their tasks.

   c. In the **p6.max.tmusers =** line, specify the maximum number of e-mail recipients that can receive notification e-mails at one time. You should keep the number below 500 to avoid performance problems.

   d. In the **p6.bootstrap =** line, specify the location of the BREBootstrap.xml file.

   For example, the location could be one of the following: C:/P6EPPM_1/p6, C:/EMAIL_HOME, /usr/P6EPPM_1/p6, or /usr/EMAIL_HOME. Or you can use the following: C:\\P6EPPM_1\p6, C:\\EMAIL_HOME.

   e. In the **mail.read.schedule =** line, specify how often your e-mail should process new messages. Use cron expressions for your formatting. For example:

   `0 */5 * * * ?`

   will process new messages every five minutes.

   > **Note:** For more information on cron expressions, see http://www.quartz-scheduler.org/docs/tutorials/crontrigger.html.

5) In the **Outgoing mail (SMTP Settings)** section, locate and specify the following:

   a. In the **send.host =** line, specify the SMTP server hostname or IP address that you will use to send e-mails.

   b. In the **send.port =** line, specify the port number that connects to the SMTP server.

   c. In the **send.ssl =** line, specify **true** to use SSL or **false** if you will not use SSL.

   > **Note:** 🛡 Oracle recommends you always use SSL in a production environment for secure communications.

   d. In the **send.starttls =** line, specify **true** to use TLS or **false** if you will not use TLS.

   e. In the **send.email =** line, specify the e-mail address or User Principal Name (UPN) where team members will send their status update requests.

f. In the **send.replyto =** line, specify an email address for team members to respond to when they receive emails. If this field is left blank, the reply address will be the **send.email** address you specified above.

g. In the **send.password =** line, specify the password for the e-mail address or UPN you just specified.

> **Note:**
> - If you do not specify a password now, the e-mail application will ask you to specify one when it runs.
> - You can also specify a password by running the following parameter when you run the 'run.bat' or 'run.sh' file:
>   `-Dsend.password=`*YOUR_PASSWORD*
>   where *Your_Password* is the password for your status e-mail address.
>   For example:
>   In Windows: `./run.bat -Dsend.password=`*YOUR_PASSWORD*
>   In Unix: `./run.sh -Dsend.password=`*YOUR_PASSWORD*
> - Oracle recommends using the option in the **config.properties** file and then moving that file to a secure location when you are finished modifying it.

6) In the **Incoming Mail (IMAP Settings)** section, locate and specify the following:

a. In the **imap.host =** line, specify the IMAP protocol host to read e-mails.

b. In the **imap.port =** line, specify the IMAP port number.

c. In the **imap.ssl=** line, specify **true** to use SSL or **false** if you will not use SSL.

> **Note:** Oracle recommends you always use SSL in a production environment for secure communications.

d. In the **imap.username =** line, specify the IMAP user name (which will be your email address) or User Principal Name (UPN).

e. In the **imap.password =** line, specify the password for the user name you just specified.

> **Note:**
> - If you do not specify a password now, the e-mail application will ask you to specify one when it runs.
> - You can also specify a password by running the following parameter when you run the 'run.bat' or 'run.sh' file:
>   -Dimap.password=*YOUR_PASSWORD*
>   where *Your_Password* is the password for your status e-mail address.
>   For example:
>   In Windows: ./run.bat -Dimap.password=*YOUR_PASSWORD*
>   In Unix: ./run.sh -Dimap.password=*YOUR_PASSWORD*
> - Oracle recommends using the option in the **config.properties** file and then moving that file to a secure location when you are finished modifying it.

    f. In the **imap.search.folder =** line, specify the folder to use for processing incoming e-mails. For example:

```
imap.search.folder = inbox
```

> **Note:** The e-mail application will use this folder to search for incoming mail. Oracle recommends you use the inbox for this folder. If you choose another folder, you must ensure that all e-mails get filtered there, or the e-mail application will not be able to detect the messages.

7) In the **IMAP Folder configuration** section, locate and specify the following:

    a. In the **imap.success.folder =** line, specify the folder where messages that process successfully will go. For example:

```
imap.success.folder = P6Success
```

> **Note:** The e-mail application will automatically create this folder if you do not create it now.

    b. In the **imap.failure.folder =** line, specify the folder where messages that failed will go. For example:

```
imap.failure.folder = P6Fail
```

> **Note:** The e-mail application will automatically create this folder if you do not create it now.

    c. In the **imap.temp.folder =** line, specify the folder where messages that are being processed will go. For example:

```
imap.temp.folder = P6Temp
```

> **Note:** The e-mail application will automatically create this folder if you do not create it now.

8) In the **Task update options** section, locate and specify the following:

    a. In the **reply.label.cleanup** field, enter true if you want to remove HTML tags attached to the task field labels. Enter false if you don't want to remove the tags.

    b. In the **reply.label.tag.search** field, enter the regular expression to remove unexpected HTML tags during reply message parsing.

> Note: See information on "regular expression" for more details on this field. For example, see https://developer.mozilla.org/en-US/docs/JavaScript/Guide/Regular_Exp ressions#Writing_a_Regular_Expression_Pattern.

    c. In the **update.debug** field, enter true if you want to output the contents of the email message as it is parsed for updates. Enter false if you don't want to output the contents of the email message as it is parsed for updates. You should only enter true when you are troubleshooting issues with updating tasks.

9) In the **Message Format options** section, locate and specify the following:

a. In the **update.task.search.term =** line, specify the text that the e-mail application should search for in the subject line of incoming messages. For example:

```
update.task.search.term = Your Requested P6 Tasks
```

b. In the **notify.update.task.search.term =** line, specify the text that the e-mail application should search for in the subject line of incoming messages that originated from a Notify message. For example:

```
update.task.search.term = Your P6 Tasks
```

10) If the EMAIL_HOME is on a different server from your P6 home, copy the BREBootstrap.xml from your P6 home to your EMAIL_HOME.

If the EMAIL_HOME is on the same server as your P6 home, you will use the BREBootstrap.xml that is in your P6 home folder.

11) Run one of the following:

‣ In Windows, launch the **run.bat** file.

‣ In Unix, launch the **run.sh** file.

When you launch the run file, you may have to complete the following steps depending on how you configured your E-mail Statusing Service:

a. If the config.properties file and the run file are in different folders, you will need to specify the config.properties location with the -Dconfig.file parameter.

▪ In Windows (add a space between run.bat and -Dconfig):

```
run.bat –Dconfig.file=C:\home\auser\somelocation\config.properties
```

▪ In Unix (add a space between run.sh and -Dconfig):

```
./run.sh –Dconfig.file=/home/auser/somelocation/config.properties
```

b. If you didn't specify the **send.password=** or **imap.password=**, you can specify them now. If you do not specify them now, the e-mail application will prompt you to do so when it runs.

▪ In Windows:

```
run.bat –Dsend.password=YOUR_PASSWORD
```

▪ In Unix:

```
./run.sh –Dsend.password=YOUR_PASSWORD
```

▪ In Windows:

```
run.bat –Dimap.password=YOUR_PASSWORD
```

▪ In Unix:

```
./run.sh –Dimap.password=YOUR_PASSWORD
```

where *Your_Password* is the password for your status e-mail address

c. If your bootstrap file contains more than one database, you need to clarify which database you are using when you launch the run file.

▪ In Windows:

```
run.bat –Ddatabase.instance=db_id
```

where *db_id* is your database instance (for example, -Ddatabase.instance=2).

▪ In Unix:

```
./run.sh –Ddatabase.instance=db_id
```

where *db_id* is your database instance (for example, -Ddatabase.instance=2).

Once the run file finishes, you can verify that the e-mail status application works. See *Verifying E-mail Statusing Service* (on page 191).

Verifying E-mail Statusing Service

Once you have installed the e-mail status application, you can send an e-mail to verify that the server is setup properly.

1) Enter an e-mail address that P6 recognizes in the 'From' line.
2) Enter the e-mail address you specified in *Configuring E-mail Statusing Service for P6* (on page 186) in the 'To' line.
3) Enter **Ping** in the subject line.
4) Send the message.

If the message is successful, you will receive a message containing the status of the e-mail service. The message will tell you how many users have a blank e-mail address in the database.

If the message failed, you will not receive a message. The failed message will appear in the failure folder that you specified in the **config.properties** file. See *Configuring E-mail Statusing Service for P6* (on page 186).

Setting P6 to Support E-mail Statusing Service Users

Projects may require that P6 users temporarily work in remote locations without access to the private network where the P6 server resides. Diverse project teams may also exist with some members updating their tasks using P6, and others using e-mail.

> **Note**: Timesheet users can request a list of their tasks using E-mail Statusing Service; however, timesheet users can only update their tasks using P6 Team Member Web.

To support updating assignment status by e-mail, you will need to:

1) Ensure the users you want to use E-mail Statusing Service have a valid account in P6.

> **Note**: Each user with a valid user account can be assigned to activities as a resource assignment if the account is associated with a labor resource, as an activity owner, or by being assigned a Team Member work distribution filter.

2) Assign users to at least one module access option.
3) Ensure the user's account specifies their unique e-mail address.
4) Assign users to one or more activity assignments (or *tasks*) for at least one active project. E-mail Statusing Service will show tasks that have not yet started, active tasks, and tasks completed in the last 30 days.

> **Note**: OBS access to a project is not required for resource assignments or activity owners using P6 Team Member Web, E-mail Statusing Service, or P6 mobile to view and update their assigned tasks. OBS access is required for each user with a Team Member work distribution filter assigned.

5) Ensure your users download and install an e-mail client application or browser to access web mail.

6) Have your teams and managers plan their e-mail process. For example, consider details such as the timing of updates by e-mail versus updates made in P6 to avoid conflicts, network access hot spots, and what equipment or mobile devices you will be using.

Known Issues

Yahoo and Hotmail web clients are not supported. If the user's e-mail address is assigned to one of these accounts, have them access their account within an SMTP e-mail client.

Error Messages

Users may receive error messages when updating tasks if their e-mail application is set to return e-mail messages in HTML format.

One of the following situations will occur:

▶ An e-mail will be returned with the message "Date or unit format specified was invalid or missing.".
▶ If there is an error in the Time Spent, Time Left, or Remaining Duration fields, an e-mail will be returned with a message that the updated value is incorrect because only part of the updated value was parsed by the E-mail Statusing Service.

The following methods can be used to avoid this issue:

▶ When entering task updates, delete the original value in its entirety before entering an updated value.
▶ Set the e-mail application to reply to messages in text format.
▶ Click the **Update this task** link to update tasks individually.

Downloading P6 mobile Apps

To download the P6 mobile apps, do one of the following:

▶ If you are using an iOS device, go to the App Store to download the mobile application.
▶ If you are using an Android device, go to the Google Play App Store to download the mobile application.

Team Member Setup Tasks

Configuring Login and Authentication Settings to Use P6 for iOS

Follow these steps to start the app for the first time. When you return to the app after working in other apps, the last page you were on will appear. Once you configure these settings, you won't need to perform these steps again unless your SSO cookies expire. If your cookies expire, you will need to enter your user name and password again.

> **Note**: You may need to activate your device's VPN feature to access your company's deployment of P6. Contact your administrator for more information.

To start the app:

1) On your device's **Home** screen, tap 📱 **P6**.
2) On the **Welcome to P6 Team Member** page, slide the **Single Sign On** (SSO) switch to either **ON** or **OFF**.

   > **Note**: Team Member Web Services supports LDAP, Native, or SSO mode. Your administrator will select the authentication mode when they configure P6.

3) If you turn SSO on:
   a. Tap the **URL** field and enter the URL to your server (for example, http://*server:port*/p6tmws).

      > **Note**: You will need to specify the server name and port number in the URL.

   b. Tap **Authenticate**.
   c. Enter your SSO username and password.
4) If you turn SSO off:
   a. Tap the **URL** field and enter the URL to your server (for example, http://*server:port*/p6tmws).
   b. Enter your P6 username.
   c. Enter your P6 password.
   d. Tap **Sign In**.

Tips

▸ To access server information in the app—which includes the SSO setting, the URL to access the server, and your user name—navigate to the **app menu**, and then tap **Settings**.
▸ For more information on the different types of authentication modes (Single Sign-On, Native, or LDAP), see "Authentication Modes in P6 EPPM" in the *P6 EPPM Post Installation Administrator's Guide*.
▸ You can modify the settings for the app from the **Settings** page on your iPhone. See the *P6 Team Member User's Guide* for more information.

Configuring Login and Authentication Settings to Use P6 for Android

Follow these steps to start the app for the first time. When you return to the app after working in other apps, the last page you were on will appear. Once you configure these settings, you won't need to perform these steps again unless your SSO cookies expire. If your cookies expire, you will need to enter your user name and password again.

> **Note**: You may need to activate your device's VPN feature to access your company's deployment of P6. Contact your administrator for more information.

To start the app:

1) On your device's **Home** screen, tap **P6**.
2) On the **Welcome to P6 Team Member** page, slide the **Single Sign On** (SSO) switch to either **ON** or **OFF**.

> **Note**: Team Member Web Services supports LDAP, Native, or SSO mode. Your administrator will select the authentication mode when they configure P6.

3) If you turn SSO on:
   a. Tap the **URL** field and enter the URL to your server (for example, http://*server:port*/p6tmws).

> **Note**: You will need to specify the server name and port number in the URL.

   b. Tap **Authenticate**.
   c. Enter your SSO username and password.
4) If you turn SSO off:
   a. Tap the **URL** field and enter the URL to your server (for example, http://*server:port*/p6tmws).
   b. Enter your P6 username.
   c. Enter your P6 password.
   d. Tap **Sign In**.

Tips

▶ To access server information in the app—which includes the SSO setting, the URL to access the server, and your user name—navigate to the **app menu**, and then tap **Settings**.
▶ For more information on the different types of authentication modes (Single Sign-On, Native, or LDAP), see "Authentication Modes in P6 EPPM" in the *P6 EPPM Post Installation Administrator's Guide*.
▶ You can modify the settings for the app from the **Settings** button in the app. See the *P6 Team Member User's Guide* for more information.

> **Note:** P6 for Android only accepts SSL certificates from a certifying authority and must use an HTTPS connection.

Setting P6 to Support P6 mobile Users

For users to perform tasks in P6 for iOS or P6 for Android, you will need to:

1) Ensure the users you want to use the P6 mobile apps have a valid account in P6.

   > **Note**: Each user with a valid user account can be assigned to activities as a resource assignment if the account is associated with a labor resource, as an activity owner, or by being assigned a Team Member work distribution filter.

2) Assign users to at least one module access option.
3) Assign users to one or more activity assignments (or *tasks*) for at least one active project. P6 mobile apps will show tasks that have not yet started, active tasks, and tasks completed in the last 30 days.

   > **Note**: OBS access to a project is not required for resource assignments or activity owners using P6 Team Member Web, E-mail Statusing Service, or P6 mobile to view and update their assigned tasks. OBS access is required for each user with a Team Member work distribution filter assigned.

Have your P6 mobile app users download and install P6 for iOS from the Apple App Store or P6 for Android from the Google Play Store to their mobile device.

> **Note**: The users will need to know the P6 server and their SSO username and password (if using SSO) or their P6 username and password (if using native authentication).

Upgrading Notes - P6 for iOS only

When upgrading from release 8.1 to a later release, Starred tasks are not transferred. The user will need to star their tasks again once the latest version is installed.

If your company is running P6 EPPM 8.1 or 8.2, users can install and use this updated version of P6 for iOS; however, they will not be able to use any of the new features for this release.

Error Message

If users receive one of the following messages, an SSL certificate may need to be obtained from a trusted certificate authority.

▶ iOS: "Server URL points to an invalid web application."
▶ Android: "Cannot connect to server."

Known Issues

▶ If users are in a time zone that observes daylight savings time, the hours displayed in their tasks may be incorrect by one hour.
▶ If users do not have any tasks assigned to them, they might receive the message "Some data failed to load. Refresh to try again." on the Home page of the app. This issue will only occur if your company has version 8.2 deployed on the P6 application server.

Configuring IIS 8.5 for P6 Team Member

To ensure that your instance of P6 Team Member works correctly with IIS 8.5, you will need to update your `web.config` file; otherwise, you might experience an error when attempting to select an option from the drop-down menu of My Tasks.

To configure IIS 8.5 for P6 Team Member:

1) Navigate to *%SystemDrive%*`\inetpub\wwwroot`.
2) Open **web.config**.
3) Add `<modules><remove name="WebDAVModule" /></modules>` to the inside of the `<system.webServer></system.webServer>` tag.
4) Add `<remove name="WebDAV" />` beneath the `<handlers></handlers>` tag, which can be found inside the `<system.webServer></system.webServer>` tag.
5) Save the file and the close it.

Timesheets Setup Tasks

This section covers the tasks you should complete before you let other users begin working in the Timesheets tab, such as configuring resources in the application and configuring access to timesheet approval.

Timesheets Settings

The information below details all application settings available for Timesheets.

P6 Team Member Web Application Settings

Use the application page to view and modify application settings for Timesheets, such as which privileges are assigned to users for logging time, how long users can access activities, and how often users must report their time, which timesheets users can view.

General Settings

Name and Description	Default	Valid Ranges/Values
Maximum search results Maximum number of records displayed in search results in the 'Assign to New Activity' window.	100	1 - 500
Enable timesheet auditing Select to save the history of timesheet submission, approval, rejection, reviewers, and associated dates. This setting can also be managed from P6.	no	yes/no
Allow editing of subordinate timesheets Select to permit supervisors to modify subordinate resources' timesheets.	no	yes/no

Privileges for Entering Hours on Timesheets

Setting Name and Description	Default	Valid Ranges/Values
Log hours on future activities Select to indicate that users can report hours on timesheets with dates after the current timesheet period (for example, entering vacation time in advance).	yes	yes/no
Log hours on non-started activities Select to indicate that users can report hours for activities that have not been started.	yes	yes/no
Log hours on completed Select to indicate that users can report hours for either 'Activities and Assignments' or 'Assignments only' that have been marked as completed. 'Assignments only' is the default selection.	yes	yes/no
Log hours on activities before the activity start date Select to indicate that users can report hours for activities on dates before their start dates.	yes	yes/no
Log hours on activities after the activity finish date Select to indicate that users can report hours for activities on dates after their finish dates.	yes	yes/no
Allow users to enter negative hours Select to permit users to enter hours less than zero.	no	yes/no

Entering Timesheets

Setting Name and Description	Default	Valid Ranges/Values
Users enter timesheet hours Select 'Daily' to require all resources report their hours on a daily basis for each assigned activity. If you choose this setting, you can also specify a maximum number of hours resources can enter per day for all of their assigned activities (minimum 0.5, maximum 24). For example, if you set this value to 12, for all of the resource's activities, a resource cannot report more than 12 hours per day. Select 'By Reporting Period' to require that all resources report their hours as a single time value for each assigned activity in a timesheet reporting period, regardless of the number of days included in the timesheet period.	Daily	Daily, By Reporting Period
Number of decimal digits for recording hours in timesheets The number of decimal places a resource can use when entering hours in timesheets.	0	0 - 2
Number of future timesheets users are allowed to access The number of future timesheets a resource can view beyond the current timesheet period.	30	0 - 200
Number of past timesheets users are allowed to access The number of past timesheets a resource can view before the current timesheet period.	4	0 - 200

Note: If there is a discrepancy between the number of decimal places you enter in the 'Maximum hours a resource can enter per day' and 'Number of decimal digits for recording hours in timesheets' fields, the values a user enters in a timesheet field might round up or down. The rounding of values is for display purposes only; the entered value is stored in the database. For example, if you specify 10.5 as the maximum hours per day but specify 0 (zero) as the maximum number of decimal places for recording hours in Timesheets, the value will round up to 11 in the timesheet. Since the value 10.5 is stored in the database, the resource does not exceed the maximum hours per day setting.

Timesheets Implementation

Project team members can submit timesheets that update their activities in P6 and P6 Professional. This chapter describes how to configure P6 to use Timesheets with P6 Team Member Web, how to run Timesheets once it is configured, and how to configure access to the Timesheet Approval application for timesheet approval managers.

In This Section

Timesheets Page

Overview

Use this page to specify default timesheet options and approval levels for P6 Team Member Web.

Screen Elements

General:

Allow resources to assign themselves to activities by default option

Determines whether you want every newly created project to grant permission for resources to assign themselves to activities. When you change this setting, it does not affect existing projects; the new setting is applied only when a new project is created. For individual projects, you can override this setting on the Project Preferences dialog box in the EPS page.

Enable timesheet auditing option

Determines whether you want to save the history of timesheet submission, approval, rejection, reviewers, and associated dates. To view the historical data, you must create reports using BI Publisher.

Approving Timesheets:

Auto Submission - No submission or approvals is required option

Select to indicate that resource timesheets do not need to be submitted or approved.

Auto Approval - Automatically approve upon submission option

Select to indicate that resource timesheets do not require management approval. Timesheets are approved automatically when they are submitted.

One approval level - Resource manager approval required option

Select to indicate that resource timesheets require approval by the resource manager only. If you select this option, the status of all submitted timesheets remains **Submitted** until the approving manager changes the timesheet's status. If you previously required both project manager and resource manager approval, and you select this option, the status of all current timesheets that have received one level of approval changes to **Approved**.

Two approval levels - Project and Resource managers' approval required option

Select to indicate that resource timesheets require approval by project and resource managers. If you select this option, the status of all submitted timesheets remains "Submitted" until both managers approve the timesheet.

Project manager must approve before Resource manager option

Determines whether project managers must approve timesheets before resource managers. The **Two Approval Levels** option must be selected to enable this option.

Default Resource manager approving timesheets when one or two approval levels required field

Select the approver you want to approve timesheets for resources. The default approver will be assigned each time you create a resource who uses timesheets.

Getting Here

1) Click the **Administer** ▼ menu and select **Application Settings**.
2) On the **Application Settings** pane, click **Timesheets**.

Configuring Resources for Timesheets

To enable a project resource to use Timesheets functionality, you must assign a user login account to the resource and set the resource to use timesheets. Follow the steps below to complete these requirements.

Assigning Associated Resources

Assign an associated resource to the user profile to connect the user with a resource in the application. Each user can have only one resource assigned, and a resource cannot be assigned to more than one user at the same time. Not all users require an associated resource, but users must have a resource assigned to enable them to edit their personal resource calendars and use P6 Team Member Web or P6 mobile. Also, by associating a resource with a user, the user will be able to see all projects to which the resource is assigned using the Activities page in P6 if the user is assigned Contributor module access.

To assign an associated resource:

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **Users**.
3) On the **Users** page:
   a. Select a user.
   b. In the **Associated Resource** field, double-click and click 🔲.
4) In the **Select Resource** dialog box, select a resource and click **Assign**.
5) On the **Users** page, click 💾 **Save**.

Tip:

If the resource you need to assign to the user does not yet exist, you can create one quickly by clicking 👤**Create Resource from Selected Users**.

Configuring Resource Settings for Timesheet Reporting

Configure timesheet reporting settings if some users will report progress using the **Timesheets** tab in P6 Team Member Web and are implementing non-automatic approval.

To configure resource settings for timesheet reporting:

> **Note**: You must perform these steps in order when configuring these settings for the first time for each new resource.

1) Click the **Administer** ▼ menu and select **User Access**.
2) In the **User Access** pane, click **Users**.
3) In the **Users** pane, click the **Module Access** detail window.
4) In the **Module Access** detail window, select **Timesheet**.
5) Click **Resources**.
6) On the **Resources** navigation bar, click **Administration**.
7) On the **Administration** page, click the **Resources** tab.
8) On the **Resources** tab, click the **Settings** detail window.
9) In the **Settings** detail window, next to the **Timesheet User Login** field, click 🔳.
10) In the **Select User** dialog box, select the resources name from the list and click **OK**.
11) In the **Settings** detail window:
    a. In the **Timesheet Approval Manager** field, click 🔳.

12) In the **Select User** dialog box, choose a manager to assign to the resource and click **OK**.

13) On the **Resources** tab, click 🔲 **Save** (Ctrl+S).

> **Note**: Users designated as timesheet approval managers are not automatically granted access to P6 Team Member Web, even if they are assigned the required module access. To enable timesheet approval managers to access timesheets in P6 Team Member Web, you must configure them as timesheet resources, as you would any other resource that requires access to timesheets in P6 Team Member Web. Configuring timesheet approval managers as timesheet resources enables approval managers to log into P6 Team Member Web to edit the timesheets of their reporting resources.

Setting Overtime Policy

To set overtime policy, which enables users to enter overtime in their timesheets:

1) Click **Resources**.
2) On the **Resources** navigation bar, click **Administration**.
3) On the **Administration** page, click the **Resources** tab.
4) On the **Resources** tab, click the **Settings** detail window.
5) In the **Settings** detail window, select the **Overtime Allowed** option.
6) In the **Overtime Factor** field, type the overtime factor by which the resource's standard price is multiplied to determine the overtime price (standard price * overtime factor = overtime price).

> **Note:** In P6 and P6 Team Member, resources can enter overtime using separate overtime fields.

Working with Timesheet Periods

Use the timesheet periods page to add a timesheet period or batch of timesheet periods.
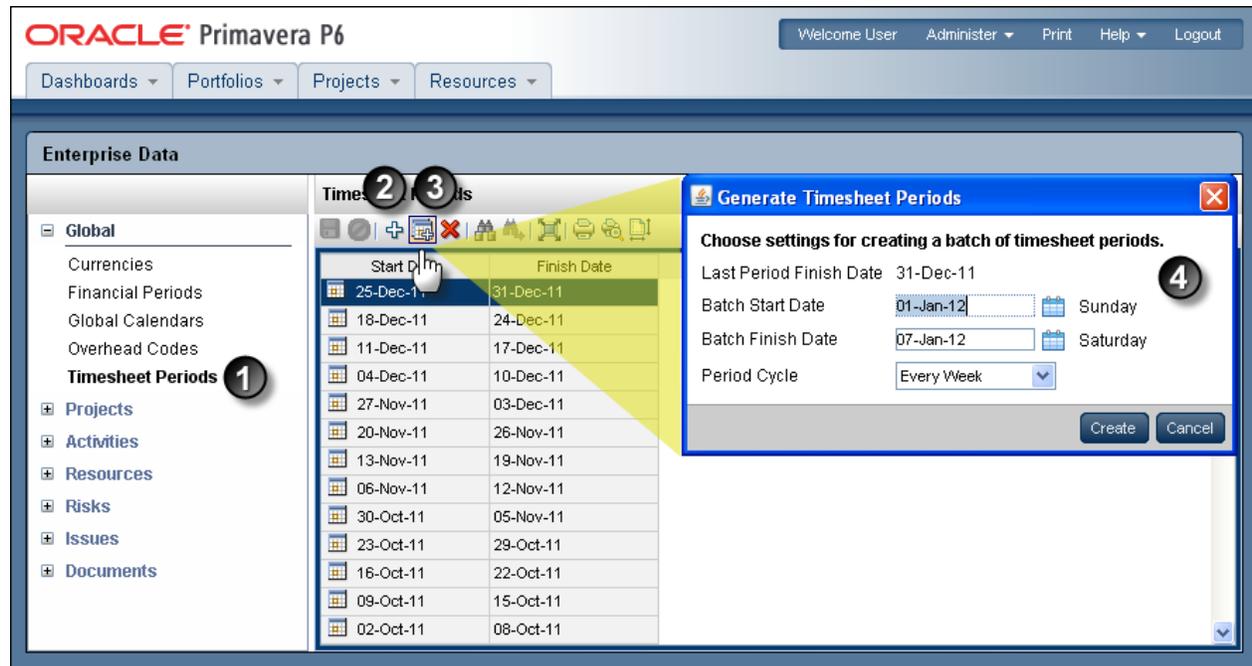
Table of Timesheet Periods

Item	Description
❶	**Timesheet Periods**: You can use the **Timesheet Periods** page to view the timesheet periods already created or to add new timesheet periods.
❷	**Add Timesheet Periods**: When you add a timesheet period, you can double-click in the **Start Date** and **End Date** fields to customize the dates. Once you have set the dates, you cannot edit them; however, you can delete financial periods that you will no longer use.
❸	**Add a Batch of Timesheet Periods**: To add a batch of timesheet periods, you will click **Add Batch**.
❹	**Generate Timesheet Periods dialog box**: In the **Generate Timesheet Periods** dialog box, you can customize the start and end date and the period cycle, which shows the amount of time the timesheet will cover. From the Period Cycle list, you can choose every week, every two weeks, every four weeks, and every month. The timesheet periods you create must be unique; they cannot overlap with an existing timesheet period.

Creating Overhead Codes

Create overhead codes for P6 Team Member Web users to add overhead activities to their timesheets to log timesheet hours that are not associated with the project.

To create an overhead code:

1) Click the **Administer** ▼ menu and select **Enterprise Data**.
2) In the **Enterprise Data** pane, expand **Global** and click **Overhead Codes**.
3) On the **Overhead Codes** page:
   a. Click ✛ **Add** (Insert).
   b. In the **Name** field, double-click and type a unique code.
   c. In the **Description** field, double-click and type a unique name.
   d. Click 💾 **Save** (Ctrl+S).

Tips

When you specify that two approval levels are required to approve timesheets, timesheets that contain only overhead activities bypass project manager approval and are sent directly to the resource/cost manager for approval. For timesheets containing a mix of regular and overhead activities, project managers can view, but not approve, the overhead activities.

About Timesheet Approval

If your organization requires resource timesheets to be approved by resource/cost managers and/or project managers, timesheets can be reviewed from the Timesheet Approval page in P6. When properly configured, any user with the appropriate module access and security privilege can access Timesheet Approval.

> **Note**: In P6 EPPM R8.0 or later, Timesheet Approval is only available from P6.

Before configuring access to Timesheet Approval, be sure to complete the following:

▶ Configure user module access.

 To access Timesheet Approval, users must be assigned at least one of the following module access rights: Contributor, Portfolios, Projects, or Resources.

▶ Assign global and/or project profiles to timesheet approval managers, as described in Assigning Global Security Profiles and Assigning OBS Elements to Users in *P6 Post Installation Administrator's Guide*, that include the required security privilege to enable approval managers to access Timesheet Approval to review timesheets.

 To enable a user to approve resource timesheets as a resource/cost manager, the user must be assigned the Approve Resource Timesheets global privilege. To enable a user to approve resource timesheets as a project manager, the user must have the Approve Timesheets as Project Manager project privilege.

▶ Specify the required timesheet approval levels, as described in *Timesheets Page* (on page 169).

Tips

For information on using the Timesheet Approval application, click Help in Timesheet Approval, or refer to the *P6 Help*.

Configuring Access to Timesheet Approval

To configure access to Timesheet Approval, follow these guidelines:

1) If not already specified when reviewing *Timesheets Page* (on page 169), set the default Resource manager that will be assigned to new resources who use timesheets.

2) From the Settings detail window of the Administration Resource tab, assign the appropriate Resource manager (Timesheet Approval Manager) for resources who use timesheets, if different than the default or if no default was set prior to adding resources. See *Configuring Resource Settings for Timesheet Reporting* (on page 203).

3) If requiring two approval levels for timesheets, verify that the users associated with the responsible manager for each project is accurate; these users will be the Project manager for the timesheets related to those projects.

4) Include the Approve Timesheets menu item in each approval manager's assigned user interface view.

5) Users with the appropriate module access and security privilege, can now choose **Approve Timesheets** from the Dashboards menu to access Timesheet Approval.

Tips

▶ For new user interface views you create, and for organizations that do not utilize user interface views, the Approve Timesheets menu item appears by default; if a user does not have rights to access Timesheet Approval, the menu item will not appear, even if you include it in the user's assigned user interface view. See Defining User Interface Views in *P6 Post Installation Administrator's Guide* for information on creating and assigning user interface views.

▶ For users upgrading from P6 EPPM version 6.1 and later, the Approve Timesheets menu item appears for users who had rights to approve timesheets in previous releases.

▶ For detailed information on the Timesheet Approval page, including Resource and Project manager delegates, refer to the *P6 Help*.

Assigning the P6 Team Member Web Module if You Upgrade from R8.2 or Earlier

If you upgrade P6 EPPM from R8.2 or earlier, the team members that use P6 Team Member Web will lose their module access. You need to assign the new P6 Team Member Web module access option to your users.

To assign Team Member module access to your users:

1) Click the **Administer** ▼ menu and select **User Access**.

2) In the **User Access** pane, click **Users**.

3) On the **Users** page, click the **Module Access** detail window.

4) Assign users the **Team Member** module access option.

P6 Integration API Post Installation Tasks

This chapter covers the tasks you should complete to finish enabling P6 Integration API, including using the Primavera P6 Administrator to connect P6 and P6 Integration API.

In This Section

Changing Database Configuration Settings for P6 Integration API

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 configurations, you can choose an existing configuration or create a new one. After configuration, 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, go to the <API_INSTALL_HOME> directory and run the **dbconfig.cmd** script. Depending on your installation, the home directory may be: **C:\P6EPPM_1\api**.

‣ On UNIX, change to the <API_INSTALL_HOME> directory and run the **dbconfig.sh** script. Depending on your installation, the home directory may be: **/usr/P6EPPM_1/api**.

Enabling Access to P6 Integration API from P6

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 ***Configuring Users in P6 EPPM*** (on page 122).

To enable access to the P6 Integration API:

1) Login to 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.

Enabling the Java Security Manager

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

> **Note**: The Java security manager does not support IBM WebSphere Application Server v 7.0.

Unless you enable the security manager before you start the P6 Integration API server, 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 or comment the appropriate command:

1) For Windows, edit the **startAppServer.cmd** file.

   For Solaris/Linux, edit the **startAppServer.sh** file.
2) Uncomment or comment one of the following:

   In 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.

Configuring Integration API Server Settings

To configure P6 Integration API and P6 to work together, you will need to set the P6 Integration API settings in the Primavera P6 Administrator.

> **Note**: For more information on the Primavera P6 Administrator see ***About the Primavera P6 Administrator*** (on page 21).

To set your Integration API server settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Integration API Server/RMI**.
   a. In the **Enable** field, choose whether to enable the RMI server. You need to enable the RMI server only if you are using P6 Integration API.
   b. In the **Registry Port** field, enter the port for the RMI Registry. This value is usually set to at least 1024.

   The default is 9099.

   You can enter anything from 1-65535.
   c. P6 Integration API supports three modes. Depending on the mode you are using, enable one of the following:
      - In the **Enable Compression** field, choose whether to enable compression service mode.
      - In the **Enable SSL** field, choose whether to enable SSL service mode.
      - In the **Enable Standard Service** field, choose whether to enable Standard service mode.
   d. Depending on which mode you enable, set the corresponding port for that mode:
      - In the **Compression Service Port** field, enter 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.

        The default is 0.

        You can enter anything from 1-65535.
      - In the **SSL Service Port** field, enter 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.

        The default is 0.

        You can enter anything from 1-65535.
      - In the **Standard Service Port** field, enter 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.

        The default is 0.

        You can enter anything from 1-65535.
4) In the **Session Timeout** field, enter the amount of time when the connection for an idle will end.

The default is 120.

Enter anything from 1-24d.

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 Primavera P6 Administrator, you can 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 Professional 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 Primavera P6 Administrator to specify these configuration settings.

> **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.

P6 EPPM Web Services Setup Tasks

This chapter covers the tasks you should complete to finish enabling P6 EPPM Web Services, including using the Primavera P6 Administrator to connect P6 and P6 EPPM Web Services.

In This Section

Changing Database Configuration Settings for P6 EPPM Web Services

The Primavera Database Configuration wizard lets you create a new configuration or switch to a different configuration than the one specified during P6 EPPM Web Services installation.

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

> **Note**: After selecting a different P6 EPPM Web Services 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, go to the <WS_INSTALL_HOME>/bin directory and run the **dbconfig.cmd** script. Depending on your installation, the home directory may be: **C:\P6EPPM_1\ws\bin**.

▸ On UNIX, change to the <WS_INSTALL_HOME>/bin directory and run the **dbconfig.sh** script. Depending on your installation, the home directory may be: **/usr/P6EPPM_1/ws/bin**.

Enabling Access to P6 EPPM Web Services

You can enable access to P6 EPPM Web Services for any user defined in P6.

> **Note**: For more information on creating users and enabling access to applications, see Configuring Users in P6 EPPM.

To enable access to P6 EPPM Web Services:

1) Login to P6 as a user with administrative privileges.
2) On the **Administer** menu, 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** detail window.
5) In the **Module Access** detail window, select the **Access** option for **Web Services**.
6) On the **Users** page, click 🖫 **Save**.

About Configuring P6 EPPM Web Services in the Primavera P6 Administrator

One P6 EPPM Web Services server instance can control more than one database and you can specify an authentication mode for a database through the Authentication Configuration wizard.

You can use the Primavera P6 Administrator to set the authentication mode, token profiles and message protection settings. If you use SAML for P6 EPPM Web Services, you must use Single Sign-on or LDAP authentication for P6 EPPM. You must configure additional settings for LDAP authentication with secure communication (SSL) between the P6 EPPM Web Services server and the LDAP server.

To configure P6 EPPM Web Services and P6 to work together, you will need to set the P6 EPPM Web Services settings in the Primavera P6 Administrator.

> **Note**:
> - A P6 EPPM Web Services configuration might include database instances that are not set to the same authentication mode as the P6 EPPM Web Services server. If a user connects and requests a database that is set to a different authentication mode than the P6 EPPM Web Services server, an error message displays. The user must select a database that matches the authentication mode set for the P6 EPPM Web Services server.
> - For more information on the Primavera P6 Administrator see *About the Primavera P6 Administrator* (on page 21).
> - See the *P6 Web Services Programmer's Guide* for more information.

Configuring Authentication Mode for P6 EPPM Web Services

To set your authentication mode:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Web Services/Security/Authentication**.
4) In the **Mode** field, choose the method clients use for authentication. The default is Username Token Profile. You can choose one of the following:

   ‣ **Username Token Profile** - Oracle recommends using this authentication mode. It defines how a web service client application can supply a user name and an optional password in the message request that the web service server can use to authenticate the requester's identity.

   ‣ **SAML Token Profile** - Security Assertion Markup Language (SAML) defines an XML-based mechanism for exchanging messages that contain security information in the form of assertions.

   ‣ **Cookies** - This option requires you to call the Authentication service Login operation to establish a session and obtain a cookie before you can use any other P6 web service.

   > **Note**: See the *P6 Web Services Programmer's Guide* for more information.

Configuring Username Token Profile Settings for P6 EPPM Web Services

To set your Username Token Profile settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Web Services/Security/Authentication/Username Token Profile/Nonce**.
   a. In the **Require Nonce** field, choose **true** to enable nonce or **false** to disable it.

      Nonce is a token that contains a random value and is used to prevent attacks.

   b. In the **Nonce Cache Timeout** field, enter the value, in the format 1d1h1m1s, for the Nonce cache timeout. The value specified indicates how long the nonce remains cached before it is deleted.

      The default is 600 seconds (10m).

      Enter anything from 5m-24d.

4) Expand **Web Services/Security/Authentication/Username Token Profile/Created**.
   a. In the **Require Created** field, choose **true** to enable the Username token timestamp or **false** to disable it.

      Requiring a Created element allows the server to determine whether the difference between two timestamps falls within an allowable window of time and can then reject any messages that exceed the window.

   b. In the **Timeout** field, enter the value, in the format 1d1h1m1s, for the Created timestamp timeout. You can specify a minimum of 300 seconds (5m).

      The default is 600 seconds (10m).

Enter anything from 5m-24d.

Configuring SAML Token Profile Settings for P6 EPPM Web Services

To set your SAML Token Profile settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Web Services/Security/Authentication/SAML Token Profile.**
   a. In the **SAML Version** field, choose the SAML version of the token.
   b. In the **Require Signed SAML Token** field, choose **true** to require signed SAML tokens or **false** to require unsigned SAML tokens.
4) Expand **Web Services/Security/Authentication/SAML Token Profile/SAML Tokens**.
   a. In the **Issuer** field, enter the valid issuer for the SAML token. Use a space to separate multiple valid issuers.
      Default Example:
      http://your.saml.issuer.com
   b. In the **IssueInstant Timeout** field, enter the value, in the format 1d1h1m1s, 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.
      The default is 300 seconds (5m).
      Enter anything from 5m-24d.
   c. In the **AuthenticationInstant Timeout** field, enter the value, in the format 1d1h1m1s, for the AuthenticationIssueInstant timeout. The value specified indicates the maximum time allowed between the time the token is issued, the time the user is authenticated, and the time the token is received by the web service.
      The default is 300 seconds (5m).
      Enter anything from 5m-24d.
5) Expand **Web Services/Security/Authentication/SAML Token Profile/Signed SAML Tokens**.
   a. In the **KeyStore Type** field, choose the KeyStore type.
      The default is JKS.
   b. In the **File Location** field, enter the absolute path to the key store file. This file must exist on the local filesystem.
      Default Example:
      c:\keystore\keystore.jks.
   c. In the **KeyStore Password** field, enter KeyStore password.
   d. In the **Certificate Alias** field, enter alias for the client certificate containing the public key.
      The default is alias.

Configuring Message Protection Settings for P6 EPPM Web Services

To set your message protection settings:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Web Services/Security/Message Protection.**

   a. In the **Require Timestamp** field, choose **true** if incoming SOAP messages must contain the WS-Security Timestamp. Choose false if it does not need the WS-Security Timestamp.

   b. In the **Require Digital Signatures for Incoming Messages** field, choose **true** to require that incoming SOAP messages are signed and conform to Web Service Security 1.1 standards. Choose false if 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.

   c. In the **Require Encryption for Incoming Messages** field, choose 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 EPPM Web Services request message must be encrypted. Choose false if incoming SOAP messages must not be encrypted.

   > **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.
   > - 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.

   d. In the **KeyStore Type** field, choose the KeyStore type.

   The default is JKS.

   e. In the **File Location** field, enter the absolute path to the key store file. This file must exist on the local filesystem.

   Default Example:

   c:\keystore\keystore.jks.

   f. In the **KeyStore Password** field, enter KeyStore password.

   g. In the **Private Key Alias** field, enter alias for the private key in KeyStore.

   The default is alias.

   h. In the **Private Key Password** field, enter password for the private key.

   i. In the **Encrypt Response** field, choose whether to encrypt outgoing messages. You can use this setting only when you enable encryption 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.

Troubleshooting for P6 EPPM

The following sections detail solutions for problems you may encounter with P6 EPPM.

In This Section

Troubleshooting for Connecting Contract Management

If Contract Management has SSL enabled, P6 may not be able to connect to Contract Management because it is trying to access a remote resource and will decide Contract Management is not a trusted location. To resolve this issue, you need to ensure that P6 contains Contract Management's server certificate in the trust list in WebLogic.

To import Contract Management's server certificate:

1) Go to the Contract Management https URL and export the certificate to a location with .cer extension or other extension file type.

   ▸ To export from Internet Explorer, go to **Tools**, **Internet Options**, **Content**, **Certificates**, **Personal**, **Export** and follow the steps in the wizard.

   ▸ To export from Mozilla Firefox, go to **Tools**, **Options**, **Advanced**, **Encryption**, **View Certificates**, **Your Certificates**, **Backup** and follow the steps in the wizard.

2) Note the location of .cer file or other extension file.

3) Import the certificate into the Weblogic keystore.

   a. Login to the Weblogic server machine where you deployed P6.

   b. Copy the exported certificate to <JRE_HOME>/lib/security.

      > **Note**: Ensure the JRE_HOME location is the one used by Weblogic.

   c. Execute the following command:

   ```
   keytool import keystore cacerts alias myCMCert file file_name.cer
   ```

      ▪ where *file_name* is the name of your exported .cer file.
      ▪ The default password for java keystore is **changeit**.

Troubleshooting for Connecting the Content Repository

An enhancement was made with P6 R8.4 to store documents in folders using the short name of the project instead of the database object ID. The P6 users' documents will now be stored in a folder called 'P6Users' instead of 'Users'. If you were using a previous version of the content repository P6 but did not run the migration utility provided in the media pack when you upgraded your environment, the content repository will not work.

To fix this issue:

1) Shutdown the P6 server.
2) Go to the **P6EPPM_Home/p6** folder.
3) Run **migrationtool.cmd** or **migrationtool.sh** (based on your operating system).
4) After the utility finishes:
    a. Go to the **P6EPPM_Home/p6/webaccesslogs** folder and ensure it contains **Document-migration.html**.
    b. Open the **Document-migration.html** file and ensure all the folder names changed successfully. Ensure nothing failed.
    c. If anything failed, log into the content repository and manually move the documents that failed to move from the older document folders to the new document folders.

    Project Documents example:

    Assume there is a Project called 'Business Development Processes' whose Database ID is '4321' and Project ID 'BDP001'. In the content repository, you would be able to see two folders: one with the name '4321' and one with the name 'BDP001'.

    1. Open the **4321** folder and copy all the documents in this folder.
    2. Open folder **BDP001** and paste all the documents in this folder.
    3. After you finish copying the documents, you can safely delete the **4321** folder from the content repository.

    User Documents example:

    If you login into the content repository and navigate to the Project Document home, you would see only 2 folders: 'Projects' and 'P6Users' . If you see a third folder called 'Users', follow these steps:

    4. Open the **P6Users** folder and make a note of the folder names.
    5. Open the **Users** folder and check if the above folder names are present.
    6. If a folder name is not present in the **Users** folder, copy that missing folder from **P6Users** to **Users**. Repeat this step for all the missing folders.
    7. If a folder name is present in the **Users** folder, manually move the documents from that folder in **P6Users** to the same folder in **Users** folder. Repeat this step for all the matching folders.
    d. Delete the **P6Users** folder.
5) Rename the **Users** folder to **P6Users** in the content repository.
6) Start the P6 server and ensure you can see all the documents.

For More Information

Where to Get Documentation

Complete documentation libraries for P6 EPPM releases are available on the Oracle Technology Network (OTN) at:

http://www.oracle.com/technetwork/documentation/primavera-093289.html

From this location you can either view libraries online or download them to have local copies. We recommend viewing them from OTN to ensure you always access the latest versions, including critical corrections and enhancements.

P6 EPPM is configured to access its help systems on OTN. However, you can also install local versions when you install the software.

The documentation assumes a standard setup of the product, with full access rights to all features and functions.

The following table describes the core documents available for P6 EPPM and lists the recommended readers by role. P6 EPPM roles are described in the *Planning Your P6 EPPM Implementation* guide.

Title	Description
What's New in P6 EPPM	Highlights the new and enhanced features included in this release.
	You can also use the *P6 EPPM Cumulative Feature Overview Tool* to identify the features that have been added since a specific release level.
	All users should read this guide.
Planning Your P6 EPPM Implementation	Explains planning your implementation and provides an installation process overview, frequently asked questions, client and server requirements, and security information.
	The P6 EPPM network administrator/database administrator and P6 administrator should read this guide.
P6 EPPM Installation and Configuration Guide	Explains how to install and configure P6 EPPM using the P6 EPPM Installation and Configuration wizards.
	The P6 EPPM network administrator/database administrator and P6 administrator should read this guide.

Title	Description
P6 EPPM Installation and Manual Configuration Guide	Explains how to install and configure the P6 EPPM using the P6 EPPM Installation wizards, and how to manually configure individual components.
	The P6 EPPM network administrator/database administrator and P6 administrator should read this guide.
P6 EPPM Post Installation Administrator's Guide	Describes how to get started using P6 EPPM applications after you have installed and configured them. Complete the tasks in this guide before letting your users work with these applications. These tasks include information about configuring your users and security settings and privileges, configuring your Primavera P6 Administrator settings, and finalizing your P6 Integration API and P6 EPPM Web Services settings.
	The P6 EPPM network administrator/database administrator and P6 administrator should read this guide.
Tested Configurations	Lists the configurations that have been tested and verified to work with P6 EPPM.
	The network administrator/database administrator and P6 EPPM administrator should read this document.
P6 User's Guide	Explains how to plan, set up, and manage projects in a multiuser environment. If you are new to P6, start with this guide to learn how to use the software effectively to plan and manage projects. When you need more detail, refer to the P6 Help.
	The program manager, project manager, resource/cost manager, team leader, and all P6 users should read this guide.
P6 Help	Explains how to use P6 to administer, plan, set up, and manage projects, portfolios, workflows, timesheets, documents, and reports in a multiuser environment. Describes how to analyze performance and ROI, and analyze budgets. If you are new to P6, use this Help to learn how to use the software effectively.
	The operations executive, P6 EPPM and P6 administrator, program manager, project manager, resource/cost manager, team leader, and all users should read this Help.
P6 Data Dictionary	Defines fields used in P6.
	All P6 users should refer to this guide if they need a field definition.

Title	Description
P6 Team Member Web Help	Describes how to use P6 Team Member Web to provide status on activities. P6 Team Member Web users should read this Help.
P6 EPPM Web Services Programmer's Guide	Describes how to invoke, use, and troubleshoot the available services and operations within supported environments. When you need specific information about the services and operations available, refer to the P6 EPPM Web Services Reference Manual. Anyone who wants to develop applications that interact with P6 should read this guide.
P6 EPPM Web Services Reference Manual	Describes all services and operations available in P6 EPPM Web Services. Anyone who wants to develop applications that interact with P6 should read this guide.
P3 to P6 EPPM Migration Guide	Provides best practices for migrating your P3 data to P6 EPPM and details how P3 functionality maps to P6 EPPM functionality. All administrators should read this guide if your organization is moving from P3 to P6.

Distributing Information to the Team

You can copy the online documentation to a network drive for access by project participants. Team members can then view or print those portions that specifically relate to their roles in the organization.

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

Where to Get Training

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

http://education.oracle.com

Oracle Learning Library

The Oracle Learning Library (OLL) provides online learning content covering Primavera products. Content includes whitepapers, videos, tutorials, articles, demos, step-by-step instructions to accomplish specific tasks, and self-paced interactive learning modules.

To access the learning library's Primavera content, go to:

http://www.oracle.com/oll/primavera

Where to Get Support

If you have a question about using Oracle products that you or your network administrator cannot resolve with information in the documentation or help, visit http://support.oracle.com/. This page provides the latest information on contacting Oracle Global Customer Support, knowledge articles, and the support renewals process. For more information about working with Support, visit https://support.oracle.com/epmos/faces/DocumentDisplay?id=888813.2 to view **Support Tools & Tips**.

The following knowledge articles are a good place to start your research because they link to the most frequently referenced articles about P6 EPPM

▸ Primavera Product Master Notes [ID 1489367.1]
▸ Master Note For Primavera P6 Common Application Questions Or Issues [ID 1292929.1]

P6 EPPM integrates with different Oracle applications; when you create a Service Request, be sure to open the request with the proper Support team. To ensure you reach the proper Support team, enter the correct product information when you create the Service Request. Each product has its own support line.

▸ Use the **Primavera P6 EPPM** support line when you are having installation, configuration, or connection issues related to P6 EPPM.
▸ Use one of the following support lines when you are having installation or configuration issues that do not relate to P6 EPPM.
  ▸ Oracle WebLogic Server
  ▸ Oracle Database Server
  ▸ BI Publisher
  ▸ BPM
  ▸ Oracle Webcenter Content Core Capabilities (formerly Universal Content Management)
  ▸ Oracle Enterprise Manager
  ▸ Oracle Access Manager
  ▸ Oracle AutoVue

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/us/support/contact-068555.html or visit http://www.oracle.com/us/corporate/accessibility/support/index.html if you are hearing impaired.

Using Primavera's Support Resource Centers

Primavera's Support Resource Center provides links to important support and product information. Primavera's Product Information Centers (PICs) organize documents found on My Oracle Support (MOS), providing quick access to product and version specific information such as important knowledge documents, Release Value Propositions, and Oracle University training. PICs also offer documentation on Lifetime Management, from planning to installs, upgrades, and maintenance.

Visit https://support.oracle.com/epmos/faces/DocumentDisplay?id=1486951.1 to access links to all of the current PICs.

PICs also provide access to:

▶ **Communities** which are moderated by Oracle providing a place for collaboration among industry peers to share best practices.
▶ **News** from our development and strategy groups.
▶ **Education** via a list of available Primavera product trainings through Oracle University. The Oracle Advisor Webcast program brings interactive expertise straight to the desktop using Oracle Web Conferencing technology. This capability brings you and Oracle experts together to access information about support services, products, technologies, best practices, and more.

Legal Notices

Oracle Primavera P6 EPPM Post Installation Administrator's Guide