Oracle
Primavera
P6 EPPM Application Administration Guide

Version 21
March 2023

ORACLE®

Contents

About the P6 EPPM Application Administration Guide

Use this guide to understand how to begin using your P6 EPPM applications. 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, security settings, and privileges as well as finalizing your P6, P6 Team Member, P6 Integration API (on-premises only) and P6 EPPM Web Services configurations.

Within our documentation, some content might be specific for cloud deployments while other content is relevant for on-premises deployments. Any content that applies to only one of these deployments is labeled accordingly.

Managing Personal Information in P6 EPPM

About Consent Notices

Consent notices inform users how personal information (PI) is collected, processed, stored, and transmitted, along with details related to applicable regulations and policies. Consent notices also alert users that the action they are taking may risk exposing PI. P6 EPPM helps you to ensure that you have requested the appropriate consent to collect, process, store, and transmit the PI your organization holds as part of P6 EPPM data.

Consent notices should:

- be written in clear language which is easy to understand.
- provide the right level of detail.
- identify the purpose and legal basis for your collection, processing, storage, and transmission of PI.
- identify whether data will be transferred to named third parties.
- identify PI categories and list the data which will be collected, processed, stored, and transmitted.

About Personal Information

P6 EPPMPersonal information (PI) is any piece of data which can be used on its own or with other information to identify, contact, or locate an individual or identify an individual in context. This information is not limited to a person's name, address, and contact details. For example a person's IP address, phone IMEI number, gender, and location at a particular time could all be personal information. Depending on local data protection laws, organizations may be responsible for ensuring the privacy of PI wherever it is stored, including in backups, locally stored downloads, and data stored in development environments.

As part of P6 EPPM Cloud Services, you may be using Oracle Identity Cloud Service ("Oracle IDCS") to manage your user access and entitlements across a number of cloud and on-premises applications and services. If you are using or accessing Oracle IDCS, you are responsible for deleting your details and data from the Oracle IDCS environment. You are responsible for retrieving your content in Oracle IDCS during your applicable services period.

Cookies Usage in P6 EPPM

View the details below for information on cookies in P6 and P6 Team Member Web.

Cookies Usage in P6

Oracle might use cookies for authentication, session management, remembering application behavior preferences and performance characteristics, and to provide documentation support.

Also, Oracle might use cookies to remember your log-in details, collect statistics to optimize site functionality, and deliver marketing based on your interests.

Cookies Usage in P6 Team Member Web

Oracle might use cookies for authentication, session management, remembering application behavior preferences and performance characteristics, and to provide documentation support.

Also, Oracle might use cookies to remember your log-in details, collect statistics to optimize site functionality, and deliver marketing based on your interests.

Cookies Usage in P6 Professional

Oracle might use cookies for authentication, session management, remembering application behavior preferences and performance characteristics, and to provide documentation support.

Also, Oracle might use cookies to remember your log-in details, collect statistics to optimize site functionality, and deliver marketing based on your interests.

Your Responsibilities

Information security and privacy laws can carry heavy penalties and fines for organizations which do not adequately protect PI they gather and store. If these laws apply to your organization, it is your responsibility to configure consent notices before they are required. You should work with your data security and legal teams to determine the wording of the consent notices you will configure in P6 EPPM.

If a consent notice is declined, it is your responsibility to take any necessary action. For example, you may be required to ensure that the data is not stored or shared.

Personal Information (PI) Data in P6 EPPM

PI may be visible in multiple areas of P6 EPPM including but not limited to user administration, resource and role administration, assignments, work products and documents, reports, issues, risks, user defined fields, codes, and timesheets.

PI may be at risk of exposure in multiple areas of P6 EPPM including but not limited to project export, downloaded tables, reports, documents, P6 Integration API (on-premises only), P6 EPPM Web Services and P6 mobile.

As part of P6 EPPM Cloud Services, you may be using Oracle Identity Cloud Service ("Oracle IDCS") to manage your user access and entitlements across a number of cloud and on-premises applications and services. If you are using or accessing Oracle IDCS, you are responsible for deleting your details and data from the Oracle IDCS environment. You are responsible for retrieving your content in Oracle IDCS during your applicable services period.

Configuring Consent Notices for P6

To configure consent notices for P6:

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) In the Application Settings pane, click **Consent Notice**.
4) On the Consent Notice page, click **P6 EPPM and P6 Professional**.
5) In the **P6 EPPM and P6 Professional** tab:
   a. Enter and format the text for the consent notice in the **Consent Message** area.

      Note: Work with your data security and legal teams to determine the wording of the consent notice.

   b. Select which actions will show the consent notice to users from the **Enable Consent Notice** list.
6) Click **Save**.

Configuring Consent Notices for P6 Team Member

To configure consent notices for P6 Team Member:

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) In the Application Settings pane, click **Consent Notice**.
4) On the Consent Notice page, click **Team Member and P6 Mobile**.
5) In the **Team Member and P6 Mobile** tab:
   a. Select **Copy P6 EPPM and P6 Professional message** or enter and format the text for the consent notice in the **Consent Message** area.

      Note: Work with your data security and legal teams to determine the

wording of the consent notice.

b. Select which actions will show the consent notice to users from the **Enable Consent Notice** list.

6) Click **Save**.

Configuring Consent Notices for P6 Professional

To configure consent notices for P6 Professional:

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) In the Application Settings pane, click **Consent Notice**.
4) On the Consent Notice page, click **P6 EPPM and P6 Professional**.
5) In the **P6 EPPM and P6 Professional** tab:
   a. Enter and format the text for the consent notice in the **Consent Message** area.

   > **Note**: Work with your data security and legal teams to determine the wording of the consent notice.

   b. Select which actions will show the consent notice to users from the **Enable Consent Notice** list.

6) Click **Save**.

Auditing Consent Status

You can see the status of consent acceptance for users. You can also reset consent acceptance for all users if there is a need to regain consent after a consent notice has changed.

To audit consent status:

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) In the Application Settings pane, click **Consent Notice**.
4) On the Consent Notice page, click a tab to select the product to audit.
   ▸ To see the consent status of each user, view the column for each of the consent notice trigger actions.
   ▸ To force the consent notice to be displayed again for all users the next time they access an area of the software, click **Forget all user acceptance**.
5) Click Save.

Security Considerations in P6 EPPM

For any company that deals with sensitive data, keeping it secure is crucial to success. While hosting P6 EPPM data on the Oracle Cloud provides security measures, it cannot do everything. For example, it cannot prevent phishing attempts or other attacks that exploit gaps in its users' security awareness. That is why it is important for everyone who works with P6 EPPM, whether hosted on-premises or on the Oracle Cloud, to understand what they can do to keep data secure.

Security is everyone's business. This chapter is for anyone who uses, manages, or is just interested in P6 EPPM. If you are a security expert or administrator, this is a good place to start. It should help you see the big security picture and understand the most important guidelines related to security in P6 EPPM.

For further information on configuring your on-premises P6 EPPM environment securely, see the P6 EPPM Security Guide for On-Premises.

Some Security Basics

We will use the term administrator to refer to anyone who is responsible for managing a company's data and who can access that data. For our purposes, administrators includes a wide variety of IT professionals, from those who define roles in the P6 EPPM application to those who manage company servers.

An end user is anyone who uses P6 EPPM to do their job. This includes project managers, subcontractors, general contractors, and everyone else who logs into P6 EPPM from an office or jobsite to get their work done.

Administrators should:

▸ Set up Single Sign-On (SSO) with SAML to minimize the number of passwords that users have to remember and to consolidate risk.
▸ Educate users on how they can avoid unwittingly helping hackers. One of the best ways application administrators and security advocates can help users is by helping them to prevent security breaches.
▸ Use a VPN to encrypt data being sent over the internet.
▸ Configure the Site Allow List to prevent access to unnecessary sites and the Web Services Allow List to restrict access to P6 EPPM Web Services to specified client IP addresses.
▸ Stay up-to-date about security trends and best practices.

End users should:

▸ Follow security guidelines created by their companies and the administrators of any network applications they use.
▸ Use strong passwords. The more random-looking the better, and avoid reusing passwords.

▸ Learn to recognize phishing. Phishing is when someone disguises an email or some other transmission as a legitimate message in an attempt to get a user to reveal sensitive information. For example, a hacker may send you an email disguised to look like an email from your employer requesting login information. These attacks are becoming more sophisticated, but you can still protect yourself by making sure any emails you receive or websites you visit are legitimate before using them to share sensitive information.

Authentication: How Users Sign On

Authentication refers to the way users sign on. If your installation of P6 EPPM is hosted on the Oracle Cloud and configured to use Oracle Identity Cloud Service (IDCS), administrators can — and should — implement Single Sign-On (SSO) with SAML. SSO with SAML reduces the number of passwords users have to remember. It can also be used to enable multi-factor login, which is when users are asked to provide some verification in addition to their passwords, like a code that they receive via text or email.

If your P6 EPPM environment is hosted on the Oracle Cloud, it comes with IDCS.

Authorization: What Users Can Access

Authorization refers to what users can access. There are several ways to manage this in P6 EPPM.

Module Access: Module access grants users access to different parts of P6 EPPM. Administrators can determine which users have access to which modules.

Project Security Profiles: In P6 EPPM,project security profiles help administrators view and set permissions for many users by assigning privileges to profiles and then assigning profiles to users and projects.

Global Security Profiles: Global security profiles make it easier for administrators to assign permission sets to multiple users at the same time. In P6 EPPM, administrators can create global security profiles with permission sets, and then assign these profiles to users.

For more information on user authorization, see these sections and topics of this guide:

▸ Users and Security in P6 EPPM
▸ Defining Global Security Profiles in P6 EPPM
▸ Defining Project Security Profiles in P6 EPPM
▸ Configuring Users in P6 EPPM

On-premises customers should also see the P6 EPPM Security Guide for On-Premises.

Endpoint Security

From laptops to cellphones, organizations have to keep track of data on more devices than ever, and more devices means more risk. That is why it is important to implement Enterprise Mobility Management (EMM) tools and policies.

Inherent Risks and Practical Policies

No automated security system or protocol can make a system fully secure if those with legitimate access exploit it for illegitimate purposes or if a device falls into the wrong hands. Here are some general common sense guidelines you should follow when it comes to endpoint security:

Use good mobile device management (MDM) software. MDM systems can help your organization secure the devices where its sensitive data might end up.

Grant security permission conservatively. Do not give everyone permission to everything just to avoid perceived complexity. Remember, one breach can be many times more costly and time consuming than setting and following standard security protocols.

Organize security profiles so they can be edited quickly. Keep security profiles and their permissions organized and easy to manage. Use descriptive names for security profiles, and organize them logically to make it easier for you or anyone else to manage them quickly and confidently.

Keep up with organizational changes. If a user no longer needs access to a part of the app, for whatever reason, update that user's permissions accordingly.

Privacy and Personal Information

Closely related to security are matters of privacy and personal information.

View the section Managing Personal Information in P6 EPPM section of this guide to learn about what information is collected and what you can do to monitor personal information in P6 EPPM.

Data Export and Integration with Other Applications

The ability to connect and exchange information with other apps is powerful, but it also presents some potential security issues that administrators must manage. Your company probably already has guidelines for where file-based exported data should reside on users' desktops, as well as when it should be expunged. However if no such guidelines currently exist, consider creating them.

It is important to understand which data flows between applications to ensure compliance with policies and regulations related to security and privacy.

For more information on data export, refer to the P6 EPPM Importing and Exporting Guide.

For more information on integration, refer to these sections of P6 Help:

▸ Working With Primavera Unifier
▸ Working With Oracle Primavera Cloud
▸ Working With Primavera Gateway

Security for Developers - Web Services Security

With P6 EPPM Web Services, developers can use some of the data and functionality of P6 EPPM outside of the limitations — and relative safety — of the P6 EPPM environment. This opens many possibilities. But as with any situation where data can move in potentially unpredictable ways, it presents risk. That is why anyone who uses P6 EPPM Web Services should understand the security fundamentals provided in this section.

Refer to these sections and topics from the P6 EPPM Web Services Programming Guide:

▸ Security
▸ Authentication and Session Management
▸ Authentication Using HTTP Cookies (On-Premises Only)
▸ WS-Security

Establishing Security Contacts

While the apps used by your organization may have some security features of their own, most security issues ultimately come down to the people who use them. When your company establishes its security procedures, it is important also to establish in-house security experts to whom other members can turn when they have security questions. Security points of contact should be continuously learning about security trends and how they can educate users to keep their data and network secure. Security contacts should also routinely update and maintain protocols that suit the security needs of their organizations.

Implementation Strategy

In This Section

About Roles and Responsibilities

The following section describes the organizational roles as they typically apply to P6 EPPM. Roles can vary or overlap, depending on the organization and industry.

Network administrators (on-premises only)

Network administrators configure an organization's network environment (local and wide area networks) for optimal performance with P6 EPPM. They install and maintain the server and client modules in P6 EPPM. They manage user access to project data and develop and maintain a comprehensive security policy to ensure that project data is protected from unauthorized access, theft, or damage.

Network administrators ensure that the hardware and software supporting P6 EPPM function reliably by:

- Setting up and maintaining the network to ensure reliable connections and the fastest possible data transfer;
- Creating and maintaining accurate lists of network resources and users so that each has a unique network identity.

Database administrators (on-premises only)

Database administrators (DBAs) are responsible for setting up, managing, and assigning access rights for the P6 EPPM databases. They set and oversee rules governing the use of corporate databases, maintain data integrity, and set interoperability standards.

Database administrators ensure reliable access to the databases by:

- Installing, configuring, and upgrading database server software and related products as required;
- Creating and implementing the databases;
- Monitoring database performance and tuning as needed;
- Planning for growth and changes and establishing and maintaining backup and recovery policies and procedures.

Program managers

Program managers are responsible for strategic planning and ongoing performance analysis. They use P6 to identify and monitor problem areas in current projects and analyze past projects to apply lessons learned when planning future projects.

Program managers might be responsible for:

▶ Initiating, prioritizing, and budgeting projects;
▶ The profit/loss for a specific business unit;
▶ Funding and go/no-go decisions about projects.

Project managers and schedulers

Project managers and/or project schedulers are responsible for managing multiple small, repetitive projects or a single, complex project.They use P6 Professional and/or P6 to:

▶ Add projects to the database;
▶ Determine resource requirements for a project;
▶ Perform cross-project analysis;
▶ Perform baseline analysis;
▶ Manage projects to on-time and on-budget completion;
▶ Plan projects before they are funded.

They might also perform detailed financial analysis of projects, handle project billing, and integrate financial information within the company.

Crew foreman

Crew foremen manage the work for a project that might be a portion of a larger project.   They are managers who produce work and manage a team, and they often use P6 and P6 Progress Reporter to prioritize short-term tasks or objectives, typically when the duration is less than the planning period of the project.

Crew members

Crews are trained in a specific skill required on a project. They work with their manager to develop activities and durations for incorporation into the schedule. Once activities are added to the schedule, crew members update them using P6 or P6 Progress Reporter to indicate the work they performed during designated accounting periods.

Set Your Goals and Business Objectives

In most companies, though their scope and duration can vary, projects tend to have similar goals: improve quality, reduce costs, increase productivity and revenue, reduce delivery time, and streamline operations. Often, the ultimate goal is to gain a competitive advantage. Controlling these projects is becoming increasingly difficult, especially if they are planned and run by project teams that are distributed across multiple locations. Organizations need to ensure that each team stays on track with its projects without losing sight of company objectives.

Company-wide project management using P6 EPPM enables project teams to plan and control their work while providing a continuous, centralized understanding of progress and performance. To begin the process of implementing P6 EPPM, you might want to broaden your project management goals to focus on the multi-user, role-based environment.

Specific objectives could include:

▶ Providing the project office with access to dynamic status information that they can use to make timely decisions.

▶ Improving efficiency of resource use by properly allocating skilled labor, communicating methodologies, and forecasting resource needs more accurately.

▶ Improving productivity across the project team as a result of continuous collaboration.

▶ Improving communication with all project participants through the use of integrated, organizational-wide products that put project information on individual's desktops.

▶ Increasing accountability by making consistent, summarized project status information available to top management.

▶ Increasing quality and client satisfaction through the use and reuse of best practices.

▶ Enabling maintenance of performance data on completed projects to confirm estimating metrics, generate new or revise existing templates, and collect job cost data.

▶ Integrating with other business systems to provide a total information system.

These goals are specific to project management. You can include additional goals that are particular to your company or industry. For example, one specific objective for a construction company might be to complete the inspection process in a more timely manner. Use best practices from your industry as a guide to setting your goals.

Develop an Implementation Strategy

Implementing P6 EPPM successfully requires that an appropriate "culture" be established within your organization. Instead of having many independent projects with no ability to aggregate and control them, you can now have a consolidated, organized project information system.

Creating the culture requires an understanding of the data and how it flows, and the roles and responsibilities of individuals as project participants and managers. Your challenge will be to create an open environment in which all these participants share data and performance information.

You would not think of allowing construction workers to work on a job site without designating a field manager to oversee the work, nor would you implement a new project without assigning a general contractor. The project management environment is best created by your own expert staff, who would perform an equivalent function—if you don't have such a person, you need one. Designate one person or a team of people to plan and coordinate the implementation. The responsibility of this team will be to develop an implementation strategy that includes helping participants understand the organizational project management approach. You might decide you need help with your implementation from Oracle Primavera Consulting or one of our business partners. Contact Oracle for more information.

While the implementation strategy will be specific to your organization, it will most likely include a needs assessment as one of the first steps. Even though you are already using project management software, take the opportunity to analyze and determine your company's business requirements, along with system requirements and the processes necessary to fulfill those requirements. You will also need to determine how to structure data to facilitate those processes. It is important to document the processes and procedures that you define. Assessing needs is discussed in more detail in *Assess Needs* (on page 20).

To ensure that data is flowing as planned, create a prototype. Use real project data to set up structures in a test database or development environment and run your processes through a typical work cycle. The prototype should include all modules of P6 EPPM you'll be using, along with any interfaces to external applications. Develop a plan that identifies all the possible scenarios to test. Include a method for collecting test data and a way to resolve issues. Use this step to make sure your system requirements are sufficient to meet the needs of all users.

A prototype can be followed by a pilot program, where you establish a small group of users to work with P6 in their environment. They can be introduced to the software using familiar project data while performing their daily work tasks. More than likely, the pilot users will identify flaws in the processes and have suggestions and questions. Make refinements and changes based on their feedback. You can also begin internal training programs at this time, using your pilot group of users. Ongoing performance monitoring should continue during this stage and adjustments made as necessary.

When the pilot program is satisfactory, a rollout of P6 EPPM to your entire company can begin. This step might involve installing the client software on all necessary desktops and populating the database with project data. You should develop a rollout schedule and get the appropriate approvals. Be sure to include the lessons learned from the pilot testing. Communicate the rollout schedule to ensure its success.

Assess Needs

A needs assessment is a crucial step to a successful P6 EPPM implementation. It will provide the basis for the entire system design, how it will operate, and who will use it.

Assessing needs can range from an evaluation of the corporate culture to analyzing hardware/software requirements to reviewing existing processes and developing new ones. Most of your information will come from interviewing key personnel. Meet with representatives from all areas of the company who participate in the project management process, from the owners to the individuals doing the actual work. Ask questions about the tasks they need to perform and the project information they need to know to do their jobs effectively.

Determine corporate culture

As mentioned, understanding the corporate culture plays an important role in any major implementation. You need to know ahead of time whether your company is ready, willing and capable for the change. Evaluate your company's state of readiness for company-wide project management. For example:

▸ Does your organization have a clear understanding of project management?
▸ Are they familiar with computers and software?
▸ Are standard processes in place for managing projects?

If the answer to these questions is no, include a training program in your implementation plan. Depending on the degree of readiness, you might also need to address issues that involve preparing employees mentally for dealing with change.

Define hardware/software requirements (on-premises only)

Review the system requirements necessary to run P6 EPPM. Then, conduct interviews with your Information Technology (IT) personnel, or those responsible for maintaining network integrity and new hardware/software installations to inquire about the current technical environment. Include questions, such as:

- Do you have servers or hardware in place? If so, what kind?
- How are remote locations managed?
- Do you have separate servers for development and production?
- Are you running Oracle or SQL server on one or more servers? If so, which version?
- Are you running any other database software?
- Do you have a LAN and/or WAN in place?
- Do you have mobile user requirements?

Answers to these types of questions will help you determine your hardware specifications. Be sure to identify items such as database server requirements, application server requirements, LAN requirements, and PC requirements. This step should be performed early in the process, since you might need to order new equipment or upgrade existing software before installing P6 EPPM.

Define integration requirements

While examining hardware requirements, review any integration requirements.

- Will you be interfacing with other software systems, such as Gateway?
- Will custom integration to an existing financial system or asset management system be required?
- Do you have resources who are skilled to develop necessary interfaces or are consultants required?

If you are integrating P6 EPPM with third-party applications or legacy systems, you should identify interface points that provide continuous flow of data while minimizing data loss.

Define how data is structured

To manage projects successfully in P6 EPPM, you first need to set up data structures for your organization, projects, resources, and costs. You might also want to define special codes to help you organize and report on data more effectively. To structure data properly, review how you handle data currently along with how you want to handle it. For example:

- How do you group projects? How many levels of projects do you have?
- Are projects cross-departmental? Do they have multiple locations?
- What is your typical project scope, size, and cost?
- How many projects are you managing at one time?
- What is your organizational structure?

- How do you group resources? Are resources assigned to projects as groups or individuals? Are resources shared across projects?
- Do you track skills for each resource?
- Do you have a work breakdown structure already in place?
- Do you have a need for multiple calendars? Do resources need calendars?
- What types of reports do you use? How often are they produced?

When you answer these types of questions, you can define the necessary data structures, such as the project hierarchy, organizational breakdown structure, and the work breakdown structure.

Determine current procedures/processes

To define how data will flow in P6 EPPM, you need to understand how your business operates. Look at your current processes and procedures and modify them to suit your project management objectives. Making decisions early about process changes saves time and money. Answer the following types of questions when you analyze business processes.

- Do you have a project methodology in place? If so, is it working?
- What is the life cycle of a project?
- What are the determining factors in deciding if a project is go or no-go?
- How are decisions made regarding project selection and budgeting?
- Is your budgeting/planning process top-down or bottom-up oriented?
- How do you estimate and track costs?
- Do you have a Project Management Office or something similar?
- What time reporting mechanism do you use?
- How do you track and measure progress?
- How do project participants get work assignments?
- What is your process for communicating project information to others?
- What information do you require or expect from the project management process?
- Who controls security? What security is required for project information? Do you need to restrict data access on a group or individual basis?

Communicate the Plan

In successful P6 EPPM implementations, people accept the changes and use the new system. Any new system or business process means a change to the way people are currently doing their jobs. Employees who are affected by the change need to know what to expect. Top management also needs to know what is going on if they are to provide support and commitment.

Communicate the implementation plan early and repeat it often. Set expectations and manage them continuously, being careful to avoid disappointing, frustrating, or surprising people.

There are many ways to communicate the implementation plan. You could introduce the plan at a company meeting along with a demonstration of P6 EPPM to show how it will benefit the entire organization. Explain any changes to business processes that might occur and what it means to individuals. Define a time-frame so everyone knows when the changes will happen. Encourage people use the software and experiment hands-on to increase their comfort level when it comes time for them to make the change. Publicize commitment by ensuring that the implementation team has support and by providing training programs and seminars. Provide a method for all levels of the organization to address concerns, questions, and suggestions.

See the subjects in *Implementation Process* (on page 25) to learn about the data structures and how they fit together in P6 EPPM.

If you foster a challenging workplace that can develop individual careers along with open communication, those individuals will want to make the process successful.

Implementation Process

In This Section

Understanding Data Structures in P6 EPPM

P6 EPPM contains many data structures to support your project management needs and business processes. Well-defined structures make entering data faster and easier; they enable you to organize and summarize data more effectively. Review the following definitions to help you better understand the data structures in P6 EPPM.

Enterprise project structure (EPS)

The EPS is a hierarchy that represents the breakdown of projects in a company. Nodes at the highest, or root, level might represent divisions within your company, phases of projects, 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 the EPS.

Resource hierarchy

The resource hierarchy represents the people, materials, and/or equipment used to perform work on activities. The resource hierarchy includes the resources across all projects in the organization. Resources are assigned to activities in P6 EPPM and can be set up to report actual work hours.

Role hierarchy

The role hierarchy represents the roles, or job titles, that exist in your organization and have some responsibility to complete project requirements. You can associate resources with roles. In the planning stages of a project, you can assign roles to activities to establish an initial project plan without committing individual resources to activities; then, before work on an activity begins, you can assign a resource that meets the defined role requirements. You are not required to define a role hierarchy.

Work breakdown structure (WBS)

The WBS is 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.

Organizational breakdown structure (OBS)

The OBS is an outline of managers responsible for the projects in your company. There is one OBS for the entire organization. It is used to control access to projects and data.

Project, activity, and resource codes

In addition to the EPS, WBS, and resource hierarchy, you can also create coding structures. Codes allow you to categorize projects, activities, and resources that have similar attributes; you can group, sort, filter, and aggregate data based on these codes.

Calendars

Calendars define standard workdays and the available number of hours in each day, along with holidays, vacations, and other nonworktime. You can create global, project-specific, and resource-specific calendars. Calendars are assigned to activities and/or resources; they determine start and end dates during scheduling and resource leveling.

Connecting Data Structures

The following diagram illustrates how the data structures relate to each other in P6 EPPM.
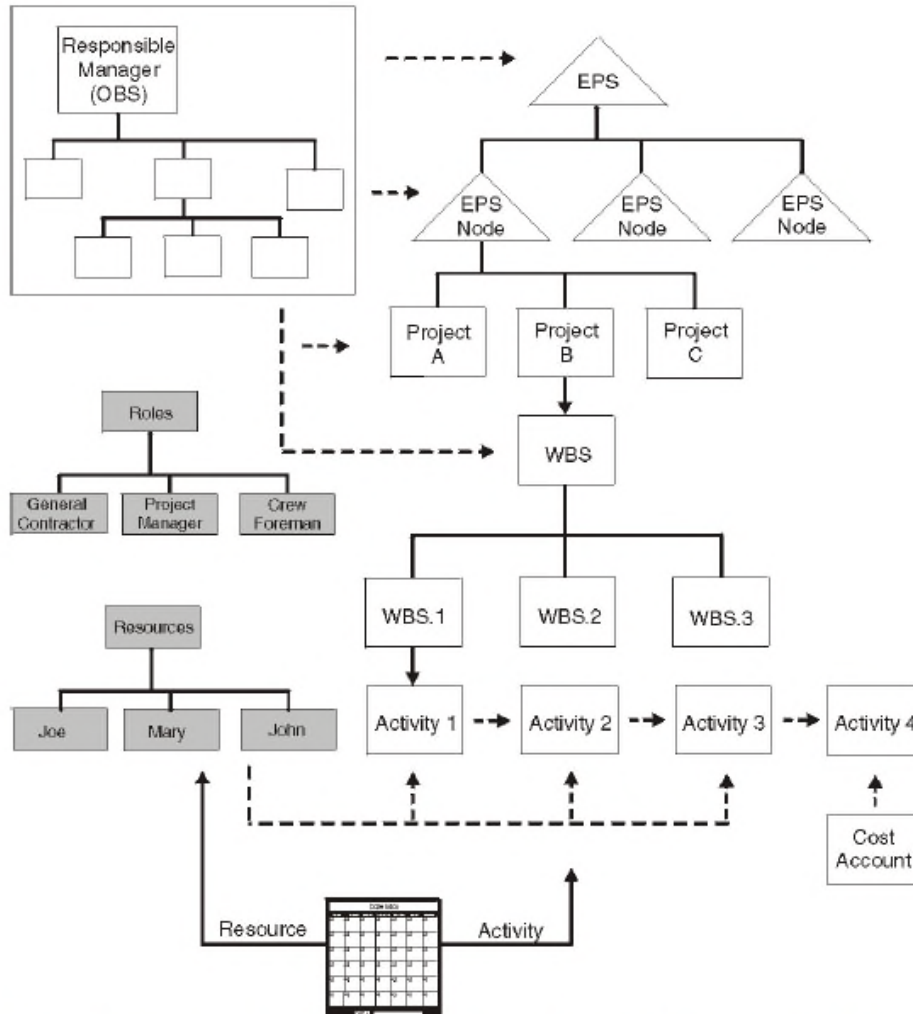
The EPS categorizes work in your company. Projects belong to EPS nodes. Each project has its own WBS that further breaks down the work in that project. Activities are the lowest level of the WBS. Additional structures include resources, roles, calendars, and cost accounts, which are assigned to activities. The OBS represents the responsible managers in your company and can be assigned at the EPS, project, and/or WBS level.

P6 Setup Tasks

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

▸ Setting a base currency

> **Note:** You must set the base currency. You cannot change it once you begin using projects.

▸ Adding users
▸ Assigning Security Settings

In This Section

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.
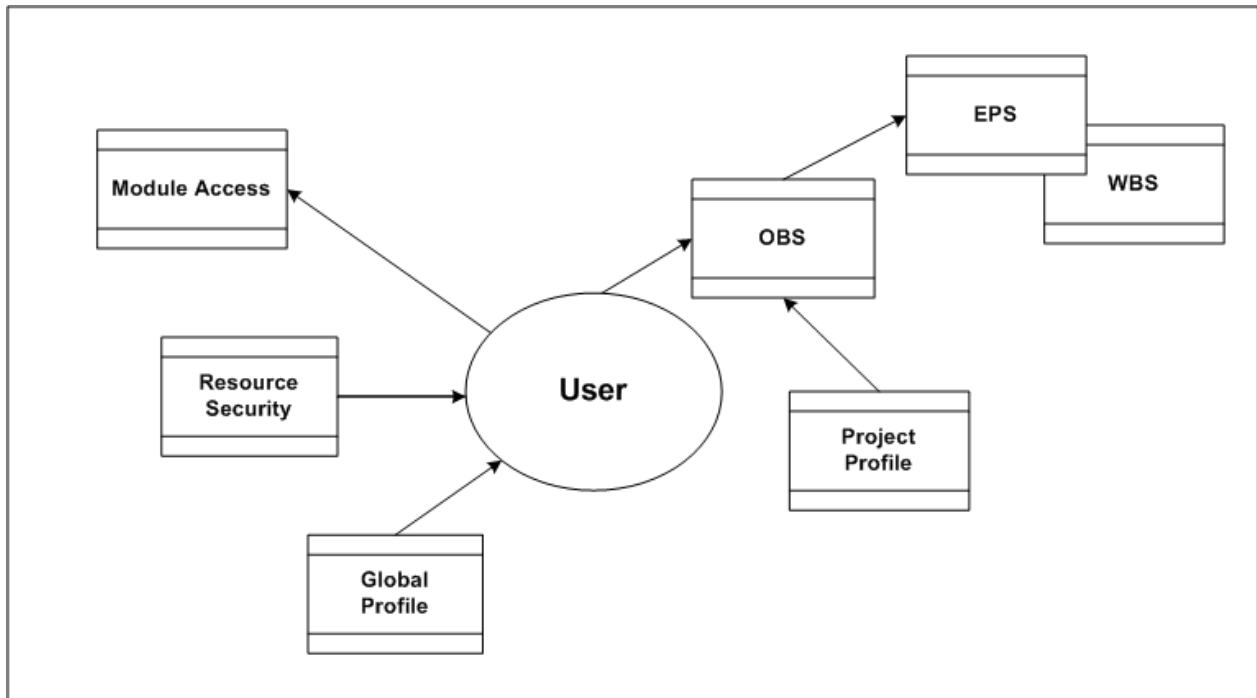
Security Samples

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

Enterprise Project Structure (EPS)

Organizational Breakdown Structure (OBS)

```
                          State of PA

                        Labor Mgmt.
                         President

      Dept. of                              Water/Sewer
   Transportation                             Division

  Management      Engineering         Management      Engineering
                    Division                            Division

Director   Project    Project   Design
           Controls   Manager   Team
           Engineer
```
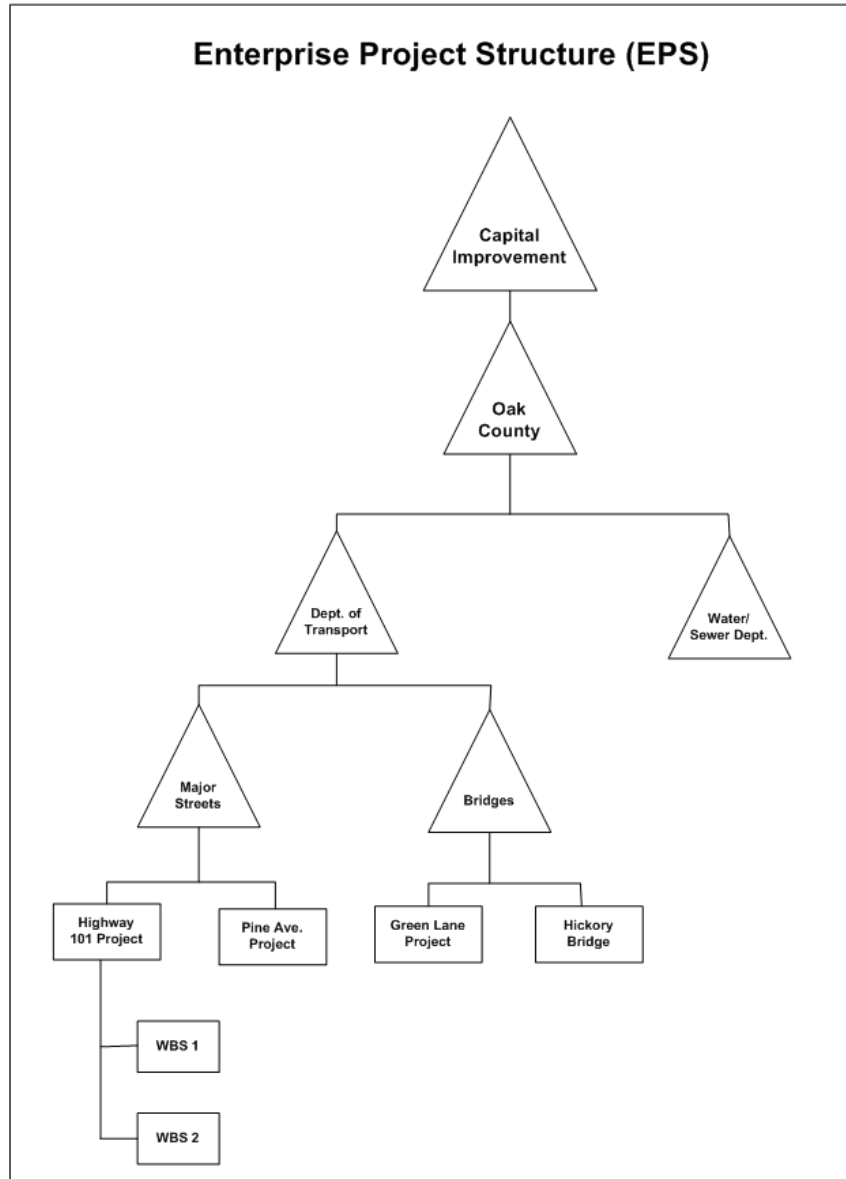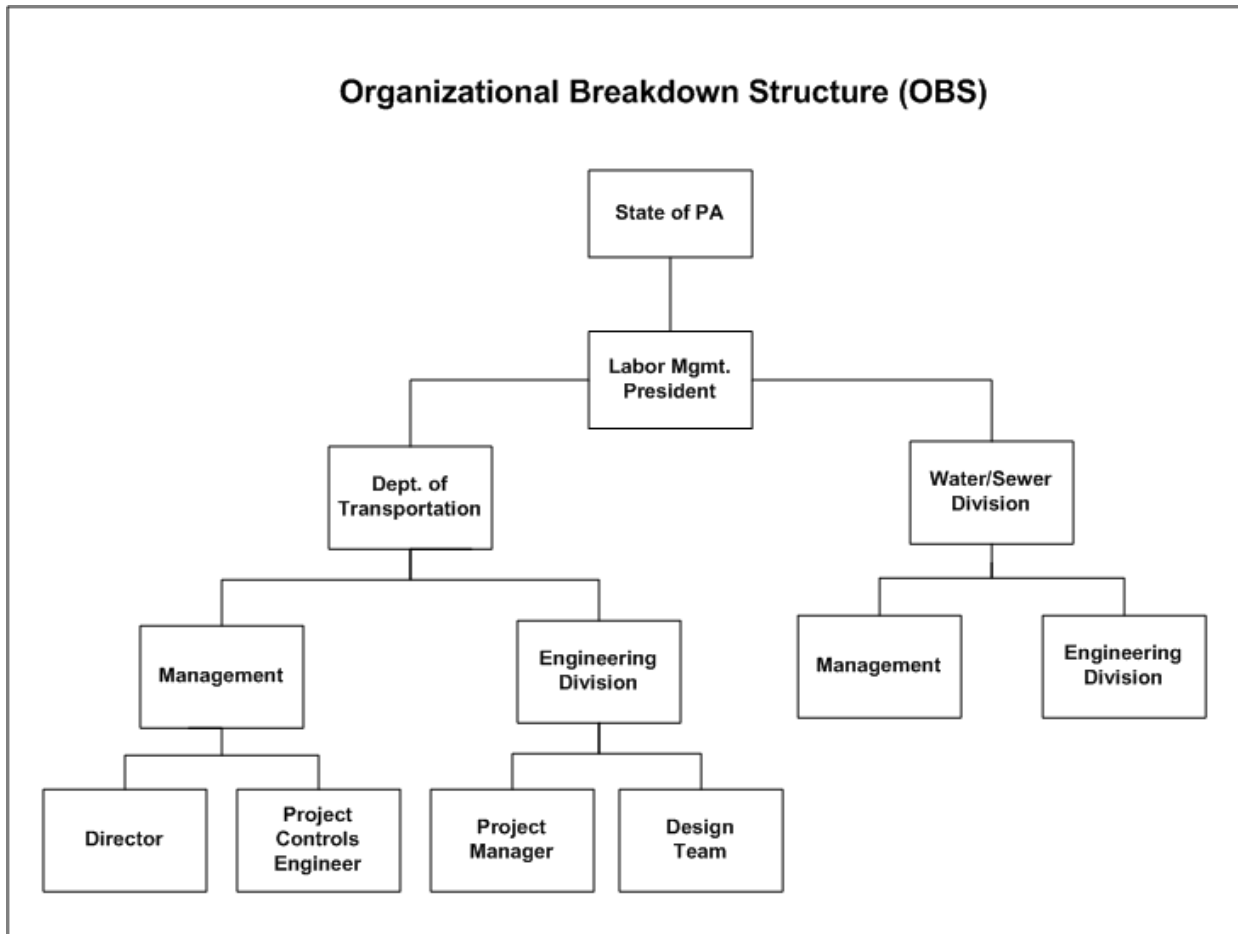
With these structures defined, you can map users to their corresponding roles in the OBS, which in turn can be assigned to each level in the EPS. The EPS level to which you assign the OBS determines the nodes/projects the associated user can access. For example, if you assign an OBS element to the root 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.
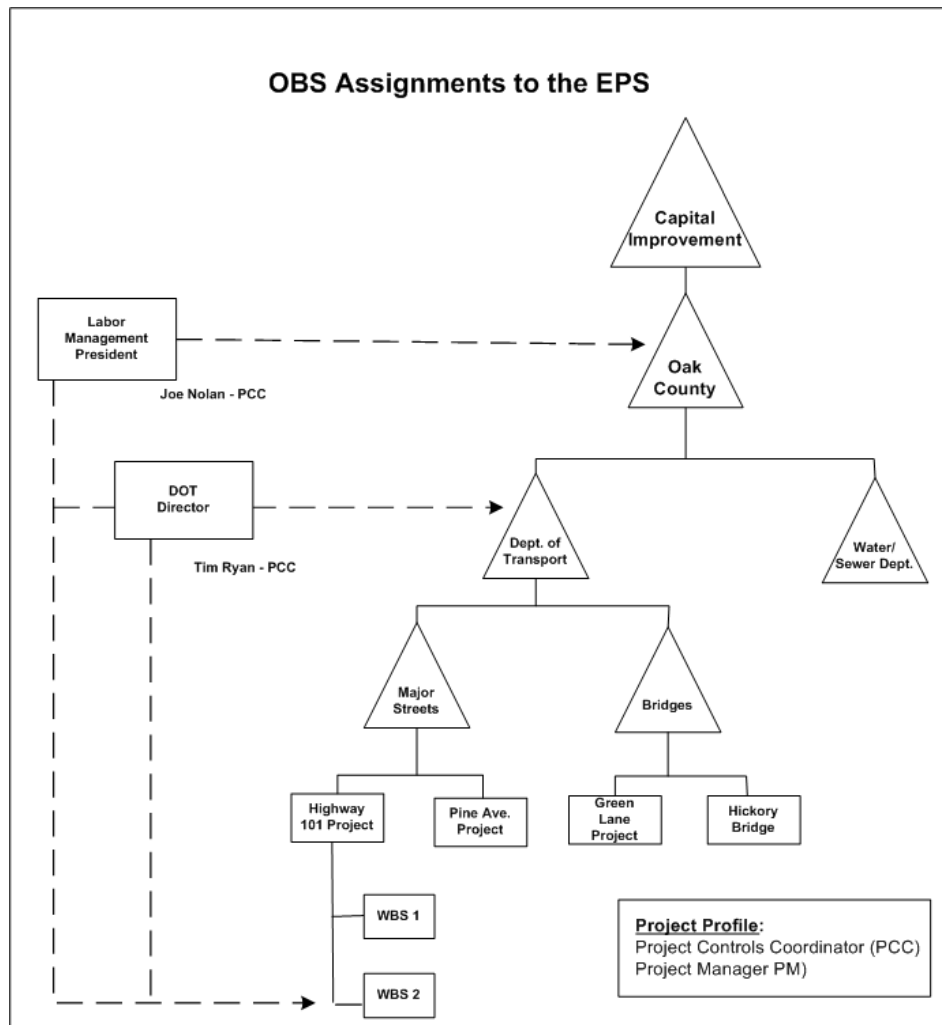
You can further control the access to projects by assigning OBS elements at the project and/or WBS level. In the previous example, if Marie Ross is the Project Manager in the Engineering Division responsible for the Highway 101 project, you can assign her to that OBS element with a Project Manager profile. 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:
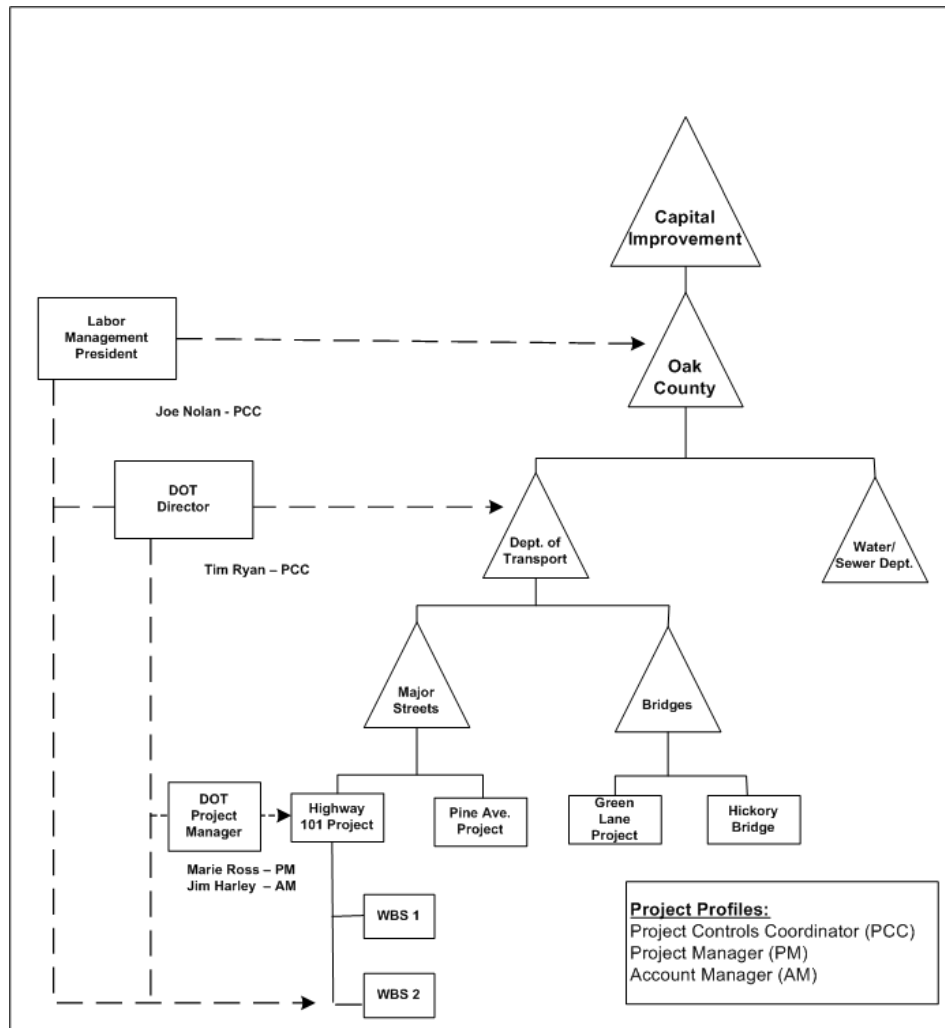
To designate that Jim Harkey has Project Manager rights to the Pine Avenue project and Marie Ross has Account Manager rights to the Pine Avenue project, you would need to add another element to the OBS.
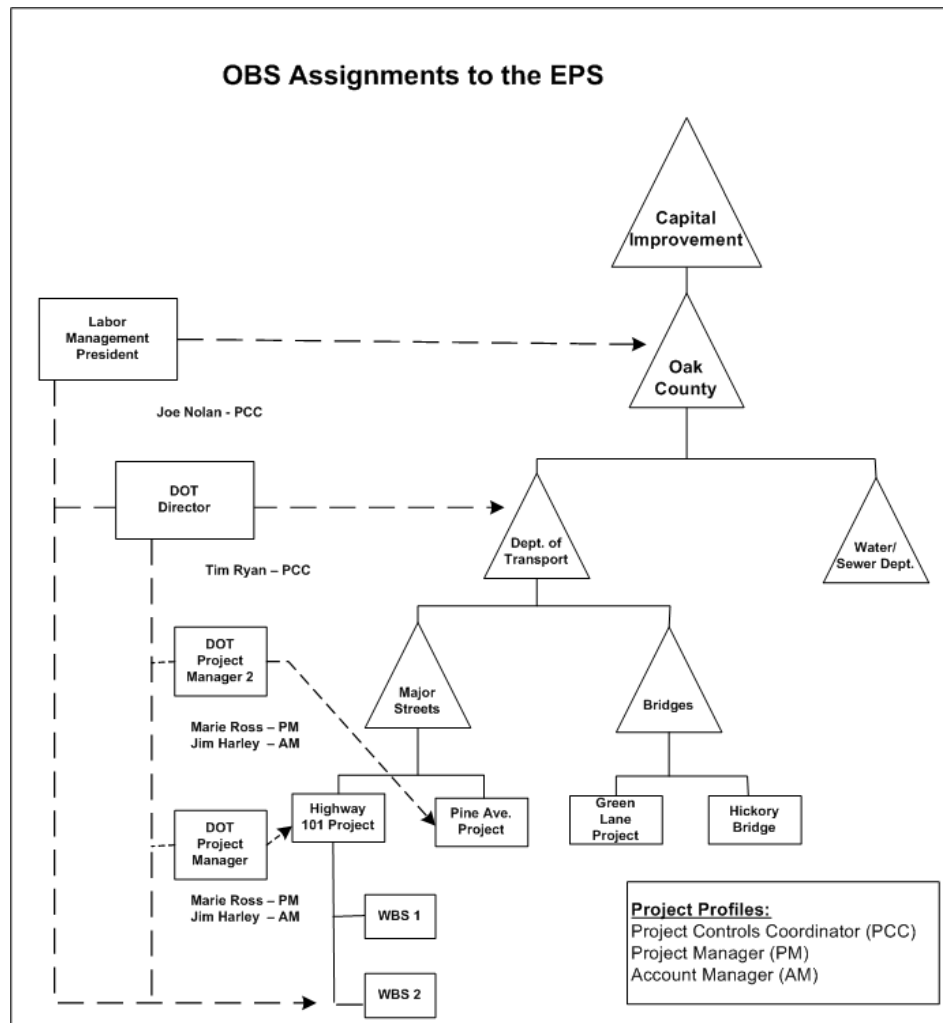
With these assignments, Jim Harkey and Marie Ross now have Project Manager rights to their primary projects and Account Manager rights to their secondary projects.

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** (on page 54).

▶ 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 67).

▶ 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 75).

▶ 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 80).

▶ 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 81).

▶ 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 83).

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 on-premises users 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, Role, 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 56) 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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Global Security Profiles**.
4) 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. Click each detail window and select options to assign privileges to the profile.

e. Click ✿**Row Actions** and click **Set As Default** if you want this profile to be the new default.

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

5) On the **Global Security Profiles** page, click **Save**.

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✿**Row Actions** and click **Duplicate**. All privilege options are also duplicated. The new profile will appear with a unique name based on the original. For example, if you duplicated *PM Set*, the duplicate 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.

View Published Audit Data option

Determines whether the profile will enable users to view published table auditing data.

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 Role Codes option

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

Edit Role Codes option

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

Delete Role Codes option

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

Add Assignment Codes option

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

Edit Assignment Codes option

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

Delete Assignment Codes option

Determines whether the profile will enable users to remove assignment codes and code values data. This privilege also selects the 'Add Assignment Codes' and 'Edit Assignment 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, resource codes, role codes, 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, resource codes, role codes, 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, resource codes role codes, 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, resource codes, role codes, 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 Calendar option

Determines whether the profile will enable users to create, modify, and remove financial period calendar 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 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.

Add/Edit/Delete Stored Images option

Determines whether the profile will enable users to create, modify, and remove stored images in P6 EPPM and P6 Professional.

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 P6 Professional XER and MPX option

Determines whether the profile will enable users to import projects, resources, and roles from XER and MPX 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 an XER file.

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.

Enable Work Offline option

Determines whether the profile will enable users to work offline in P6 Professional configured to a database with a P6 Pro Cloud Connect alias. To work offline, the database alias must have the Enable Client-side Cache option selected. To see this privilege, select the Enable offline mode option in the General pane of Application Settings.

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 75) 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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) In the User Administration pane, click **Project Security Profiles**.
4) 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. Click ✿**Row Actions** and click **Set As Default** 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 header to assign all privileges in the window. Clear the **Privilege** option to disable all privileges in the window.

5) Click **Save**.

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✿**Row Actions** and click **Duplicate**. All privilege options are also duplicated. The new profile will appear with a unique name based on the original. For example, if you duplicated *PM Set*, the duplicate 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.

Delete Discussion Comments option

Determines whether the profile will enable users to delete discussion comments assigned to activities.

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 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 and other WBS level data including notebook entries, earned value settings, milestones, and dates. This privilege does not allow users to edit cost and financial data at the WBS level.

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. 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.

Delete Published Project Data option

Determines whether the profile will enable users to delete published project data using the Delete Published Data action on the EPS page.

Export Project Data option

Determines whether the profile will enable users to export project data and download data to Excel using the Download link below grids.

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 P6 users to check out and start reviews for project template documents. P6 Professional users cannot open documents added via a P6 installation with a configured content repository. 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.

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.

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.

Related Applications Privileges

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 Oracle Primavera Cloud option

Determines whether the profile will enable users to exchange project data with a linked Oracle Primavera Cloud project.

Exchange Project Data with Gateway option

Determines whether the profile will enable users to exchange project data with a project linked via Primavera Gateway.

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 add, edit, or delete resource assignments on the Planning Page of the Resources Section.

Add/Edit/Delete Role Assignments for Resource Planning option

Determines whether the profile will enable users to add, edit, or delete role assignments on the Planning Page of the Resources Section.

Edit Committed Flag for Resource Planning option

Determines whether profile will enable the users to edit the committed flag on the Planning Page of the Resources Section.

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.

Tools Privileges for Projects

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.

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.

Perform Global Search & Replace option

Determines whether the profile will enable users to use Global Search & Replace to update project, WBS, and activity information in P6.

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 email 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* (on page 75).

About User Access

User access helps you create user accounts, assign access, manage the organizational breakdown structure (OBS) and configure profiles:

Users: Enables you to modify security attributes and project and module access for all users of P6 EPPM modules.

OBS: Enables you to configure the OBS hierarchy.

Global Security Profiles: Enables you to assign or omit global privileges to profiles.

Project Security Profiles: Enables you 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
❶	**Users**: Use the **Users** page to assign users access to the module and to projects.
❷	**OBS**: Use the **OBS** page to assign managers to an OBS.
❸	**Global Security Profiles**: Use the **Global Security Profiles** page to assign global privileges to users.
❹	**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, follow the procedures below in the order specified.

1) Follow the steps in *Creating User Accounts for P6 EPPM* (on page 56) to create a new user.
2) Follow the steps in *Assigning Global Security Profiles* (on page 60) to assign "Admin Superuser" as the global profile for the new user.
3) Follow the steps in *Assigning Module Access* (on page 65) 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".

> **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 (including multiple user views), EPS Toolbars, EPS Views (including multiple user views), Resource Assignment Toolbars, and Resource Assignment Views (including multiple user views) as the copied user. The user's Associated Resource, email 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 **Administration**.
3) On the Administration navigation bar, click **User Administration**.
4) On the User Administration page, click **Users**.
5) On the **Users** page, click the ＋**Add** button.
6) What appears next depends on your security configuration:

To add users in Native authentication mode see ***Adding Users in Native Authentication Mode for On-Premises*** (on page 57).

To add users in LDAP or SSO authentication mode see ***Adding Users in LDAP or SSO Authentication Mode for On-Premises*** (on page 58).

> **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.
- For example, a global organization has three users with the following Login Name field values to uniquely identify them: *tharris*, *tjharris*, and *tsharris*. The following Personal Name values are added to assist the entire organization in identifying the users:

  tharris Thomas Harris in Accounting (USA)

  tjharris Thomas J. Harris in Legal (ESP)

  tsharris Tina S. Harris in Design (CAN)
- Cloud only: To configure a default email address for users without an email address, submit a Service Request in My Oracle Support.
- 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 on-premises users 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 for On-Premises

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 **Email** 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 Oracle Analytics Publisher (formerly 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 for On-Premises

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:

> **Note**: If you intend to use Oracle Analytics Publisher (formerly 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.

1) Click **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) Click the **Add** ▼ menu and select **Users from LDAP**.
4) In the Add Users From LDAP dialog box:
   a. Enter an LDAP query or accept the query in the search field and click 🔍**Search**.

   > **Note**: Depending on your P6 administrative configuration settings, you might be prompted to log into the LDAP server. For more information about P6 administrative configuration settings, refer to the *P6 EPPM System Administration Guide for On-Premises*.

   b. Select the users to add and click ⟩**Select Items**.
   c. Click **Add**.
5) On the Users page, click **Save**.

Tips:

▶ You can also add users from an LDIF file. When you add users from an LDIF file all users in the file are added to the Available Users list.

▶ You must have the Add/Edit/Delete Users and Provision Users from LDAP privileges 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 the settings of another user in the Copy Preferences from (optional) field. If you select to copy the settings from another user, the project and global security pofiles, OBS assignments, project access, and module access will be copied from the other user. The LDAP repository will remain the source for the name, ID, phone number, and email even if you copy the preferences from another user. Copying preferences from another user does not copy the associated resource to the new user.

▶ If you select the Create Resource option, the resources are created and the Associated Resource column is populated when you save the changes in the User Administration page.

Updating Users in LDAP or SSO Authentication Mode for On-Premises

If P6 is configured for LDAP or SSO authentication mode you update users that have already been added to P6 from the LDAP repository. The Update Users From LDAP dialog box only shows users that have different data in any of the matched fields in P6 from the corresponding matched field in the LDAP repository. When you update users from LDAP, the data for the selected users in P6 is replaced with the data from the LDAP repository.

To update users in LDAP or SSO authentication mode:

1) Click **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.
4) Click the **Actions** ▼ menu and select **Update Users From LDAP**.
5) In the Update Users From LDAP dialog box:
    a. Enter an LDAP query or accept the query in the search field and click 🔍 **Search**.
    b. Choose to update **All Users** or **Selected Users**.
    c. If you chose to update Selected Users, select the users to update and click ❯ **Select Items**.
    d. Click **Update**.

Tips

▶ The matched fields in P6 are Login Name, Personal Name, Email, and Phone. The fields in the LDAP repository that are matched is determined in Primavera P6 Administrator. For more information about configuring the LDAP Field Map see *P6 EPPM System Administration Guide for On-Premises*.

Configuring User Access

For security purposes, configure user access controls to grant or deny user's access to data.

To configure user access, see:

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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.
4) On the **Users** page:
    a. Select a user.
    b. In the **Associated Resource** field, double-click and click **···Select**.
5) In the **Select Resource** dialog box, select a resource and click **Select**.

> **Note**: In Native Authentication mode, the user's Personal Name will be updated to match the Resource Name. Otherwise, the Resource Name will be updated to match the user's Personal Name.

6) 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 **✿Row Actions** and then click **Create Resource**.

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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.

4) 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 Email 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 (on-premises only), 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 (on-premises only), and the data that is displayed in the Dashboards portlets are dependent on each user's security privileges. For more information about Primavera P6 Administrator, refer to *P6 EPPM System Administration Guide* (on-premises only).

Contributor option

Determines limited user access to P6, such as the Dashboards and Projects sections (Activities page). 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 run. See th*e P6 EPPM BI Publisher Configuration 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 Email Statusing Service. All modules provide access rights to Email 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

▸ 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 63).

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
> 67) 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 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 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.

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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.
4) On the **Users** page:
   a. Select a user.
5) In the **Module Access** detail window, select options to grant access to each module or feature set.
6) On the **Users** page, click **Save**.

Assigning Application Access to P6 EPPM for Cloud

Before assigning application access in P6 EPPM, you should configure the OBS, Global Security Profiles, and Project Security Profiles in P6.

> **Caution:** Personal information (PI) may be at risk of exposure. Depending on local data protection laws organizations may be responsible for mitigating any risk of exposure.

To assign application access to P6 EPPM applications:

1) Log in to Primavera Administration and do the following:

a. Add a user.

b. Assign application access for that user to **Primavera P6 Production**.

> **Note**: For details on using Primavera Administration, see the *Primavera Administration Identity Management Guide*.

2) Log in to P6 as an administrator and do the following:

a. From the **Administer** menu, select **User Access**.

b. From the **User Access** window, select a user and then specify their privileges (for example, Module Access and Project Access). Privileges determine the different functionalities and projects that a user can access and utilize in P6 EPPM.

c. Click **Save**.

3) Repeat these steps for each user that requires access to P6 EPPM.

Assigning OBS Elements to Users

Assign OBS elements to a user to control their access to the EPS and projects.

> **Note**: 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 **Administration**.

2) On the Administration navigation bar, click **User Administration**.

3) On the User Administration page, click **Users**.

4) On the **Users** page, select a user.

5) In the **Project Access** detail window:

a. Click **Assign OBS**.

6) In the **Select Responsible Manager** dialog box:

a. Select a **Project Security Profile**.

b. Select OBS elements from the list and click **Select**.

c. Select additional Project Security Profiles and additional OBS elements as necessary.

d. Click **Select** when finished.

7) On the **Users** page, click **Save**.

Tips

▸ You can also assign users to OBS elements using the Users Detail Window of the OBS Page.

▸ 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, select ✿**Row Actions** and click **Delete**.

Assigning Resource Access

You can control which resources a user can access.

To control resource access:

1) Click **Administration**.

2) On the Administration navigation bar, click **User Administration**.

3) On the User Administration page, click **Users**.

4) On the **Users** page:

   a. Select a user.

   b. In the **Resource Access** field, double-click and click **•••Select**.

5) In the **Select Resource Access** dialog box, select one of the following and click **Select**:

   ▶ **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 up to five resource nodes and their children.

6) On the **Users** page, click **Save**.

Tips

▶ Resource access settings are not applicable to Admin Superusers. Admin Superusers always have access to all resources.

▶ Resource access changes go into effect when you click **Save**, however P6 users must exit the application and log in again to see the changes.

▶ If a resource is deleted from the resource hierarchy, users that previously had been assigned only 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, Resources, and Administer). 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. You can designate one user interface view as the default view for new users.

> **Note:** 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. 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 **Administration**.
2) On the Administration navigation bar, click **User Interface Views**.
3) On the User Interface Views page, click +**Add**.
4) Click the **Content** tab.
5) On the Content tab:
   a. Enter a unique name in the Name field.
   b. Select which section the new user interface view should show when it is first opened from the Start Page list.
   c. Configure the Menu Items and Dashboards for the view on the Dashboards tab.
   d. Configure the Menu Items and Pages for the view on the Portfolios tab.
   e. Configure the Menu Items and Pages for the view on the Projects tab.
   f. Optionally select views to open when the EPS, Activities, and Assignments pages are opened.
   g. Configure the Pages for the view on the Resources tab.
   h. Optionally select a view to open when the Assignments page is opened.
   i. Configure the Menu Items for the view on the Administration tab.

   > **Note**:
   >
   > - 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.
   > - To configure the sequence of pages and dashboards, select a page or dashboard and click Move Up or Move Down. The first item listed in each section is designated as the left-most item for that section.

6) Click the **Activity Editing** tab.
7) On the Activity Editing tab:
   a. Expand each section and select the option in the **Edit** field to allow the user to edit that type of data in the view.

   > **Note**: 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.

8) Click the **Users** tab.
9) On the Users tab:
   a. Configure the list of users for the view.

10) Click **Save**.

Tips

▶ To create a new view which shares some features with an existing view, select the view and click ✿**Row Actions** and select Duplicate, then configure the new view.

▶ 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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.
4) On the **Users** page:
   a. Select a user.
   b. In the **User Interface View** field, double-click and click •••**Select**.
5) In the **Select User Interface View** dialog box, select a user interface view and click **Select**.
6) On the **Users** page, click **Save**.

Updating Users

You can update multiple users at the same time by copying settings from an existing user. The settings which are copied include global and project security profiles, module access, OBS access, resource access and User Interface View access. You must be logged in as an admin superuser to update users.

To update users:

1) Click **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.
4) Click the **Actions**▾ menu and select **Update User Settings**.
5) In the Update User Settings Dialog Box:
   a. In the **Copy settings from** field, select a user whose settings you want to copy to other users.
   b. In the grid, select all the users you want to update.

    c. Select **Apply**.

6) On the User Administration page, select **Save**.

Tips

▶ You can search the user list by any visible column.

▶ If you use the Select All option, all users are selected even if the user list is filtered to a set of users matching search criteria you entered.

▶ The personal user interface view is not copied to the updated users.

Deleting User Accounts

Delete a user account when an employee has left the organization or the user no longer requires access to P6.

> **Note**: Deleting a user will cause historical data to change. 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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.
4) On the **Users** page:
    a. Click on the user.
    b. Click ⚙**Row Actions** and 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.

▶ When you delete a global security profile, P6 assigns the default global security profile to any users who were assigned to the deleted profile.

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 user accounts

1) Click **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.

4) On the **Users** page:
    a. Select the user accounts to deactivate.
    b. Click ✿**Row Actions** .
    c. Select **Deactivate User**.
5) Click   **Save**.

Tips

▸ You can deactivate the user by de-provisioning the user in Primavera Administration (cloud only).
▸ If the users are assigned an associated resource, the resource and the resource assignments remain in the database.
▸ To reactivate a user account, select the user then click the Module Access detail window and select the Access option for at least one module.

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. Select the resource.
    b. Click✿**Row Actions**   and select **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. In the **Confirm** dialog box, click **Yes**.
4) Click **Save**.

Changing Passwords

Administrators can change a user's password and users can change their own passwords.

▸ Administrators: See *Changing User Passwords* (on page 72).
▸ Users: See Changing Your Own Password.

Changing User Passwords

Administrators can change users' passwords.

> **Note**:You cannot change passwords if P6 EPPM is running in LDAP or SSO authentication mode.

To change a user password:

1) Click **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.
4) On the **Users** page:
   a. Select a user.
   b. Click ✿**Row Actions** and click **Change Password**.
5) In the **Change Password** dialog box:
   a. In the **New Password** field, enter a new password.
   b. In the **Confirm New Password** field, enter the new password again for verification and click **Change**.
6) On the **Users** page, click **Save**.

Tips

▶ 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.

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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.
4) On the **Users** page, click **Actions**▾ menu and select **User Count**.
5) In the **User Count** dialog box, view the user count by module.

> **Note**: You can output the results of this process to Excel or print the view.

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:

- For on-premises deployments, system administrators can use the Primavera P6 Administrator to specify the number of times a user can fail to log in before P6 locks them out. The default setting is 5.
- For on-premises deployments, 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.
- For more information about Primavera P6 Administrator, refer to *P6 EPPM System Administration Guide* (on-premises only).

To reset user sessions:

1) Click the **User** ▼ menu and select **User Sessions**.
2) On the User Sessions page:

> **Caution**: Oracle recommends that users only be reset if they are locked out. Once a user session has been reset, the user will be returned to the login screen.

   ▶ 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.
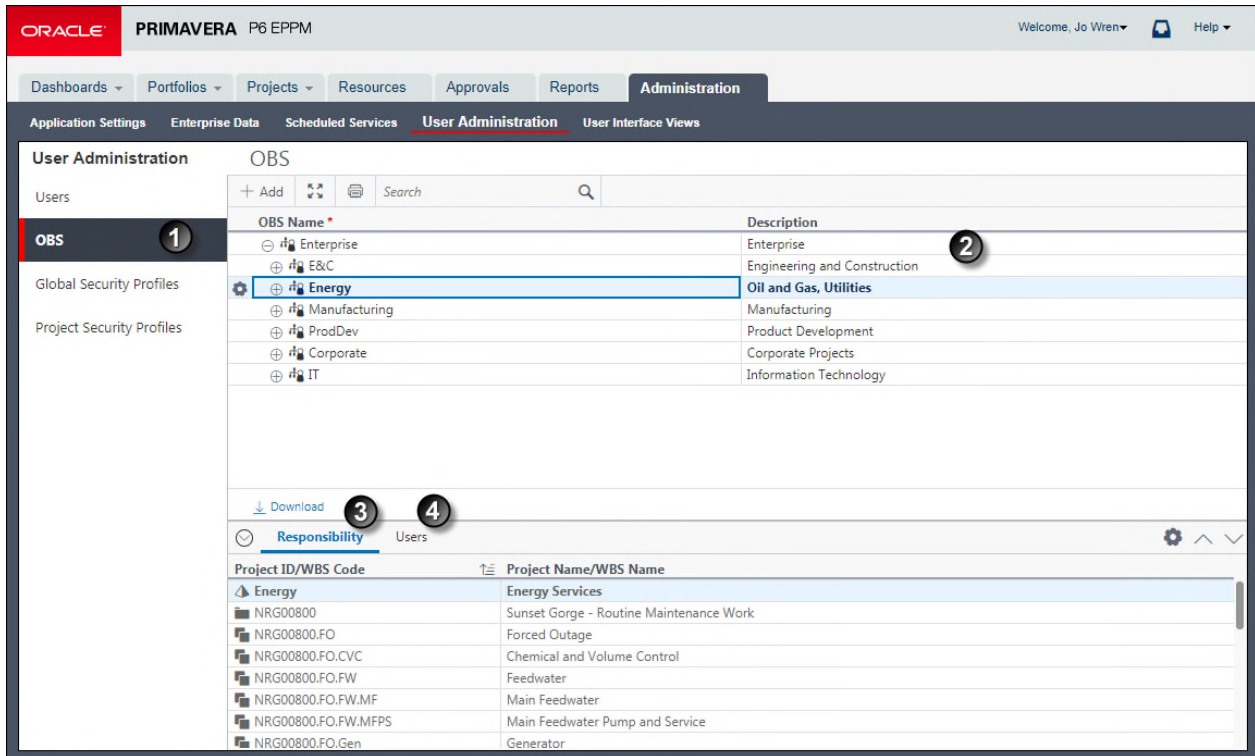
Table of OBS Page

Item	Description
①	**OBS page**: Use the **OBS** page to assign responsible managers to a project.
②	**Description column**: Use this column 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.
③	**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.
④	**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.

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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **OBS**.
4) 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 ✿**Row Actions** and selecting ︿**Move Item Up** and ﹀**Move Item Down** arrows.
   c. In the **OBS Name** field, double-click and type a unique name.
   d. Click the **Users** detail window.
5) In the **Users** detail window, remove or assign users to the OBS.
   ▸ To remove a user from the OBS, select a user, click ✿**Row Actions** and click **Delete**.
   ▸ To assign users to the OBS, click **Assign...**.
6) In the **Select Users** dialog box:
   a. Select a **Project Security Profile**.
   b. Select users and click **Select**.
   c. When you are finished assigning users, click **Close**.
7) 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 less restrictive profiles assigned higher up in the project structure override more restrictive profiles lower down. For example a user assigned a profile which allows them to modify data at the project level, will also be able to modify data in all of the WBS elements of that project, even if they are assigned a profile at the WBS level which would ordinarily not allow them to modify data. If you need a user to be able to modify the data in some WBS nodes of a project but not others, you must assign the user a more restrictive profile at the project level to restrict their access, then assign a less restrictive profile to only the WBS elements to which the user requires modify access. Bear in mind that a less restrictive profile assigned at the EPS level will also override more restrictive profile assignments at the project and WBS levels. Similarly a less restrictive profile assigned at a higher WBS level, will override more restrictive security profile assignments at lower WBS levels. For this reason it is important to take care in designing the WBS structure of any project where users will require differing access to differing parts of the project.

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 46) 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.

> **Note**: 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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **OBS**.
4) On the **OBS** page, select an OBS and click the **Users** detail window.

5) In the **Users** detail window, click **Assign...**.

6) 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 **Select**.

    c. Select additional Project Security Profiles and assign additional users as necessary.

    d. Click **Close** when finished.

7) On the **OBS** page, click **Save**.

Tip:

You can also select multiple OBS elements in the OBS page then assign multiple 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.

> **Note**: 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 **Administration**.

2) On the Administration navigation bar, click **User Administration**.

3) On the User Administration page, click **Users**.

4) On the **Users** page, select a user.

5) In the **Project Access** detail window:

    a. Click **Assign OBS**.

6) In the **Select Responsible Manager** dialog box:

    a. Select a **Project Security Profile**.

    b. Select OBS elements from the list and click **Select**.

    c. Select additional Project Security Profiles and additional OBS elements as necessary.

    d. Click **Select** when finished.

7) On the **Users** page, click **Save**.

Tips

▸ You can also assign users to OBS elements using the Users Detail Window of the OBS Page.

▸ 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, select ⚙**Row Actions** 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.
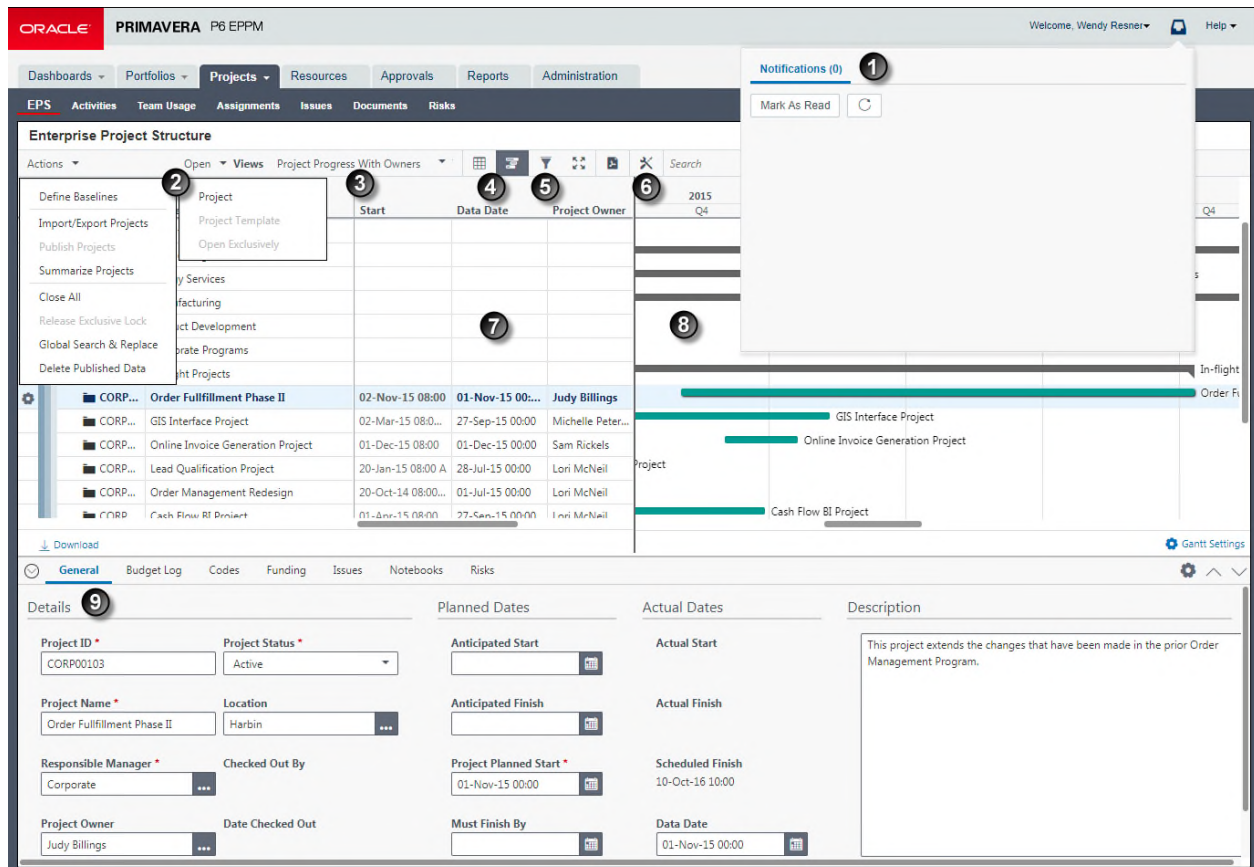
Table of Key EPS Page Elements

Item	Description
①	**Notifications area**: When background services, for example project summarization, finish running you will be notified here.
②	**Actions and Open menus**: Use these menus to work with the **EPS** page.
③	**EPS Views list**: Determines how you see data on the **EPS** page.
④	**Grid and Gantt view buttons**: Determines whether you see a grid of EPS data, or a grid and a graphical representation of dates on a timeline.

Item	Description
⑤	**Filter button**: Enables you to customize the **EPS** page.
⑥	**Customize View button**: Enables you to customize the **EPS** page
⑦	**EPS/Project Grid**: 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**.
⑧	**EPS Gantt** : Displays project and EPS data in a Gantt format.
⑨	**Detail Windows**: The **General** detail window for the project selected in the table. You can customize which detail windows appear in the view.

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 one more root resources in the resource hierarchy. The position of the assigned resources in the hierarchy determines the user's resource access. When the user logs in, the resource hierarchy displays only the assigned resource nodes and their children. Resources outside the user's root resources 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.Admin Superusers always have all resource access, no matter which option is selected.

▸ **Select Resources Access** provides access to up to five selected resources and all their children in the resource hierarchy. Users with this restricted access can view global resource data for resources they have access to.

The following example shows how resource access is determined by the root resource assigned to different users.

Item	Description
❶	Shannon Zhu has restricted access with the root resource *IT - Information Technology Group* assigned. Shannon sees the following resources in the resource dictionary: IT, MathiasL, RiceB, LiR, AbrahamM, WrenJ, AndersonG, SharpeD, VincentI, ChopraA, BennettC, ZhuS, SinghD, CharlesM, LaffertyV, PaxsonD, and ITCon.
❷	Vanessa Lafferty has restricted access with the root resources *AndersonG - Glen Anderson, VP Development* and *CharlesM - Mandy Charles, VP IT Ops* assigned. Vanessa sees the following resources in the resource dictionary: AndersonG, SharpeD, VincentI, ChopraA, BennettC, ZhuS, SinghD, CharlesM, LaffertyV, PaxsonD, and ITCon.
❸	Roy Li has no resource access. Roy cannot see any resources in the Resource Administration page. Roy can see resources assigned to a project he has open in the Assignments detail window and in the Projects Assignments and Resource Assignments pages.
	Lane Mathis has access to *All Resources*. Lane can see all of the resources in the entire resource dictionary.

See the *P6 Help* for more information on setting up the resource hierarchy.

Tips

▸ 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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.
4) On the **Users** page:
   a. Select a user.
   b. In the **Resource Access** field, double-click and click •••**Select**.
5) In the **Select Resource Access** dialog box, select one of the following and click **Select**:
   ▸ **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 up to five resource nodes and their children.
6) On the **Users** page, click **Save**.

Tips

▸ Resource access settings are not applicable to Admin Superusers. Admin Superusers always have access to all resources.

▸ Resource access changes go into effect when you click **Save**, however P6 users must exit the application and log in again to see the changes.

▸ If a resource is deleted from the resource hierarchy, users that previously had been assigned only 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.
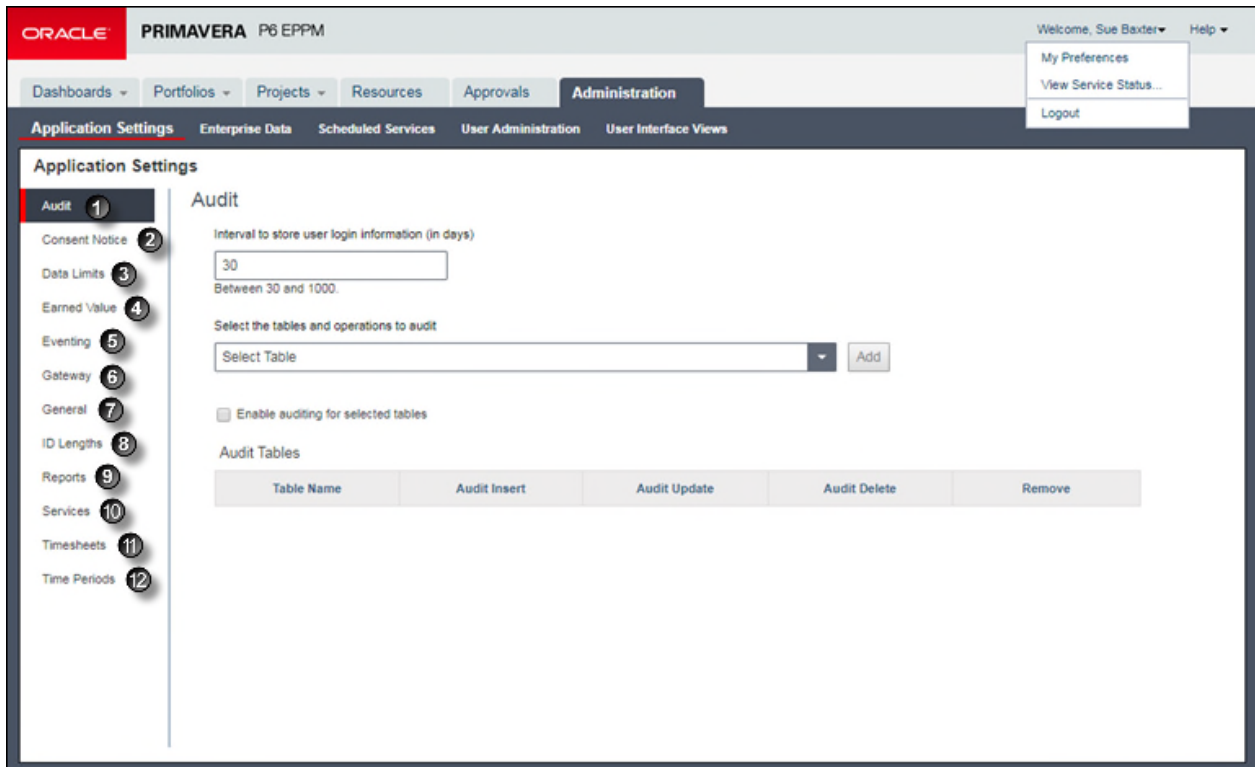
Table of Application Settings Elements

Item	Description
❶	**Audit**: Specify the tables to audit and the operation to audit against each table.
❷	**Consent Notice**: Specify the consent notice to be shown to users and the actions which will trigger consent.
❸	**Data Limits**: Specify the maximum number of levels for hierarchical structures, the maximum number of codes and baselines, the maximum number and size of stored images, as well as several other maximum limits.

Item	Description
④	**Earned Value**: Specify default settings for calculating earned value.
⑤	**Eventing**: Specify connection information and parameters for working with events and configure the Business Objects and Special Operations which can trigger events.
⑥	**Gateway**: Specify connection information and parameters for working with Primavera Gateway.
⑦	**General**: Specify general default options, such as the weekday on which the calendar week begins.
⑧	**ID Lengths**: Specify the maximum number of characters for IDs and codes.
⑨	**Reports**: Specify the headers and footers available for reports in Oracle Primavera P6 Visualizer.
⑩	**Services**: Specify publication and summarization periods and configure project publication options.
⑪	**Timesheets**: Specify default setup options when using the Timesheets tab in P6 Team Member.
⑫	**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.

Audit Page

Overview

Use this page to configure table auditing.

Screen Elements

Interval to store user login information (in days) field

The default duration for user login and consent data to be stored. This setting is used to store data for reports which show user login information.

Interval to store audit information (in days) field

The default duration for audit table data to be stored.

Select the tables and operations to audit list

Enables you to select a table or operation to configure for auditing.

Add button

Adds a table to the Audit Tables section.

Enable auditing for selected tables option

Switches on auditing for the tables you add to the Audit Tables section and configure for auditing.

Table Name field

The name of the table to be configured for auditing.

Audit Insert option

Determines whether insertions to this table will be audited.

Audit Update option

Determines whether updates to this table will be audited.

Audit Delete option

Determines whether deletions on this table will be audited.

Remove field

Removes the table from the section.

Getting Here

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, click **Audit**.

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.

OBS: Enter the maximum number of levels for the OBS hierarchy.

Resource: Enter the maximum number of levels for Resources hierarchies.

Role: Enter the maximum number of levels for Role hierarchies.

Cost Account: Enter the maximum number of levels for Cost Account hierarchies.

Activity Code: Enter the maximum number of levels for Activity Code hierarchies.

Assignment Code: Enter the maximum number of levels for Assignment Code hierarchies.

Resource Code: Enter the maximum number of levels for Resource Code hierarchies.

Role Code: Enter the maximum number of levels for Role Code 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.

Stored Images section

Select a value for each of the following fields:

Maximum Count: Enter the maximum number of images to store in the database.

Maximum Height: Enter the maximum allowable height for stored images (in pixels).

Maximum Width: Enter the maximum allowable width for stored images (in pixels).

Maximum Limit section

Select a value for each of the following fields:

Excel Import File Size (KB): Enter the maximum size (in KB) of the .xls or .csv file uploaded during import.

Filter Portfolio Stale Period: 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.

Loaded Resource/Role in Team Usage and Resource Analysis: Enter the maximum number of resources or roles that can open in the Team Usage and Resource Analysis views.

Portlets per Dashboard: Enter the maximum number of portlets that can be added to a dashboard on the Dashboards Home page. If this number is smaller than the existing number of portlets on some dashboards, you will not be able to add any more portlets to those dashboards until you remove some of the existing portlets from them.

Resource Chart Group Limit: Enter the maximum number of charts that are allowed while grouping the project in Resource Analysis views.

MRU List Items: Enter the maximum number of items that can display in the Projects and Portfolios Most Recently Used (MRU) lists.

Financial Period Calendars: Enter the maximum number of financial period calendars that can be created.

Maximum Views and Portfolios section

Select a value for each of the following fields:

Users for Shared View and Portfolio: Enter the maximum number of users that can be added to a shared view or portfolio in the Manage Portfolios dialog box or the Create Portfolios dialog box.

Projects per Portfolio View: 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.

Projects In Portfolio: Enter the maximum number of projects returned when creating a portfolio with a filter.

Activities per Activity View: Enter the maximum number of activities that can display in the Activities tab of the Projects section.

Financial Periods per Activity View: Enter the maximum number of financial periods that can display in the Activities tab of the Projects section.

Assignments per Assignment View: Enter the maximum number of assignments that can appear in an assignment view.

Assignments per Resource Planning View: Enter the maximum number of assignments that can appear in a resource planning view.

EPS and Projects per EPS View: Enter the maximum number of EPS nodes and projects that can appear in an EPS view.

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 **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, 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 and whether updating baselines will update with planned or current dates.

Getting Here

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, click **Earned Value**.

General Tab of the Eventing Page

Overview

Use this page to configure eventing parameters and directory services to allow business objects and special operations to trigger events (on premises only).

Screen Elements

Eventing section

Eventing option

Determines whether to send events for P6, P6 EPPM Web Services, and P6 Integration API.

Interval

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.

Max Queue Size

The amount of memory allocated to the queue for events. Once exceeded, events will publish immediately.

Show Costs option

Determines whether to enable the display of cost fields in event notifications.

JMS Destination Security option

Determines whether enable security.

JMS Connection Factory

The JNDI name of the JMS Connection Factory

JMS Connection Username

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

JMS Connection Name

The JNDI name of the queue or topic where events publish.

JMS Connection Password

The password to use when sending events to the specified JMS destination.

Test Connection button

Tests the connection to the JMS destination using the **Username** and **Password** specified.

Directory Services section

Provider URL

The URL of the JNDI provider used for eventing.

Security Principle

The WebLogic administrative user connected to the JNDI provider for eventing.

Initial Context Factory

The class name of the initial context factory for the JNDI connection for eventing.

Security Credentials

The password for the WebLogic administrative user connected to the JNDI provider for eventing.

Lookup Name

The JNDI queue name used when testing the directory connection for eventing.

Security Level list

The security level used to authenticate to the directory service for eventing. The available options are **SIMPLE**, **STRONG**, or **NONE**.

Test Connection button

Tests the connection to the directory service using the **Username** and **Password** specified.

Getting Here

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, click **Eventing**.
4) Click the **General** tab.

Configuration Tab of the Eventing Page

Overview

Use this page to configure the business objects and special operations which trigger events (on premises only). Refer to the *P6 EPPM Business Object Events Guide* for additional information.

Screen Elements

Business Objects page.

Business Object field

The name of the business object to be used for eventing.

Create option

Determines whether to trigger an event when business objects are created.

Update option

Determines whether to trigger an event when business objects are updated.

Special Operations page.

Operation field

The name of the operation to be used for eventing.

Enabled option

Determines whether to trigger an event when a special operation is performed.

Getting Here

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, click **Eventing**.
4) Click the **Configuration** tab.

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 in the format: *<https: or http>//<hostName>:<portNumber>/gatewayapi/restapi/v1/<service>*

This field is also used when integrating with a Oracle Primavera Cloud workspace assigned to a P6 connection.

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.

✕**Delete**

Deletes the selected data items or table rows.

Getting Here

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, click **Gateway**.

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.

Codes

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.

Specify how to display code values options

Determines whether to show the code value name or code value description when displaying code values in the grid.

This option does not change the way that code values are displayed in the Project Statistics portlet, My Issues portlet, Capacity Planning page, Portfolio Analysis page, and Status Updates page.

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.

What's New Dialog

Display What's New Dialog option

Determines whether the dialog describing the new features in P6 EPPM is shown to users when they log into P6 for the first time after an update.

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 version of the help hosted by Oracle 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 the hosted version 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.

P6 Professional Applications

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.

Run in Secure Global Desktop environment option

Switch on this option if you want P6 Professional users to run the application in Secure Global Desktop.

> **Note**: If this option is selected, P6 Professional users will not be able to see database details and system information on the **System** tab of the **About** page.

Enable offline mode option

Switch on this option if your users need to be able to use offline mode. If this option is switched off, you cannot change assign the *Enable Work Offline* global security profile privilege.

Exception Site List

Lists the websites you have specified that users can launch from user defined fields (UDFs), projects websites, Team Member Web, or Notebook topics. Click **Edit Site List** to modify the list.

Cost Spread

Spread cost based on options

Determines how costs are spread in resource analysis, capacity planning, team usage, and assignments pages as well as the usage chart in the resource and role assignment pickers. Other affected areas of P6 EPPM are publishing, summarizing, live assignment spreads, integration with Primavera Unifier, reports, and Analytics. If you have P6 Professional connected to your P6 EPPM database, the resource spreadsheets and histograms in Resource Analysis, Resource Assignments, and Team Usage views are affected.

‣ Select **Linear Spread** to spread costs evenly across the time period, regardless of any changes in resource or role rates.

‣ Select **Units Spread** to calculate cost spreads to account for periodic changes in resource or role rates.

> **Notes**:
>
> ▪ If you select to change from Linear Spread to Units Spread, you must run Recalculate Assignment Costs for all projects.
>
> If your projects are integrated with Primavera Unifier, you must use linear spread.

Identify Baseline Activities

Identify baseline activities using options

Determines whether to match activities in the project with their corresponding activities in the baseline using the **Activity ID/Code** or the internal **GUID (Globally Unique ID)** of the activity.

Getting Here

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, click **General**.

Integration and Allow Lists Page

Overview

Use this page to configure integration with other applications and specify which sites can be used with P6 and which client IP addresses have permission to connect to P6 EPPM Web Services.

Screen Elements

Document Management

P6 URL field

This URL enables P6 Professional users to download exported Primavera XML files.

Security Policy field

The default security policy for adding documents.

Invalid Document Types field

A comma-separated list of file types P6 EPPM should not accept for upload or download to the content repository. Oracle recommends that at least the default values of .exe, .com, .bat, .cmd, .vbs, .js, and .msi should be entered in this field.

Unifier

Primavera Unifier URL field

The Primavera Unifier URL that will enable users to access Primavera Unifier from P6.

Integration User Name field

The User Name for accessing the Primavera Unifier integration.

Password field

The password for accessing the Primavera Unifier integration.

Site Allow List

Site Allow List list

The list of sites which have been allowed. To see this list, there must be sites in the list.

Edit List button

Opens the Edit Allow List dialog box.

Web Services Allow List

These settings are available if you are accessing P6 on the cloud.

Enable allow list filtering for web services option

Select this option to restrict access to web services only to those client IPs shown in the Web Services Allow List.

Web Services Allow List list

The list of client IP addresses (in CIDR notation) permitted to connect to P6 Web Services if *Enable allow list filtering for web services* is selected. If *Enable allow list filtering for web services* is not selected any client IP address can access P6 Web Services.

Edit List button

Opens the Edit Allow List dialog box.

Getting Here

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, click **Integration and Allow Lists**.

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 **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, click **ID Lengths**.

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 section

  Define a header, footer, or custom text label for reports or diagrams.

Second Set section

Define a second header, footer, or custom text label for reports or diagrams.

Third Set section

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.

General section

Cache Timeout list

Determines the interval at which the cache for searching reports times out.

Enhanced Page Loading option

Determines whether to use enhanced loading in the Reports page. When this option is selected, reports are cached as you expand the report folder structure. When this option is not selected, reports are cached as soon as you open the Reports page.

Caching allows reports to be searched, so select this option if page loading performance is more important to you than searching. You can search the You can search the report name, default format, default template, available format, and available templates columns.

Getting Here

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, 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.

Project Publication section:

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.

Start Time field

Determines the start time for scheduled jobs when the *Publish projects every* field contains a value less than 1 day.

Publish a changed project when the...

Number of changes exceeds field

Determines the number of changes that must exist since a project was last published before the *Publish Projects* service is automatically initiated again.

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.

Publish resource and role data option

Determines whether to allow resource and role data in the Team Usage view to be published for reporting.

Enable Baseline Publication option

Determines whether to allow baseline data to be published for reporting.

Enable Notification Email option

Determines whether to send an email when a publication service fails.

Notification Email address field

Determines the email address which will be sent the notification email.

If this field is left blank, the notification email will be sent to the email address associated with the user who switched on the **Enable Notification Email** option.

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 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 **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, click **Services**.

Timesheets Page

Overview

Use this page to specify default timesheet options and approval levels in P6 Team Member interfaces, P6 for Android, or P6 for iOS.

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.

Allow resources to assign themselves to activities outside assigned OBS access option

Determines whether you want every newly created project to grant permission for resources to assign themselves to activities even if the resource does not have access to the relevant OBS for the activity. 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.

Assign themselves to activities with role assignments matching Team Member's role option

Determines whether team members can assign themselves to activities with unstaffed role assignments that match their role.

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.

Enable email notifications option

Determines whether you want timesheet approval managers to be notified by email when a timesheet is rejected. If this option is enabled, when a timesheet is rejected an email will be sent to all Project Managers and their delegates, Resource Managers and their delegates, users with the Admin Superuser profile, and users with the Project Superuser profile assigned for any projects included in the timesheet. This function requires that the relevant users have an email address associated with their user profile. The manager who rejected the timesheet will not receive an email notification.

Prevent users from rejecting approved timesheets option

Determines whether you want to prevent users from rejecting approved timesheets and if so within which time period.

To prevent users from rejecting any approved timesheets, select **All** in the Timeframe list.

To prevent users from rejecting timesheets approved during the previous calendar month or earlier, select **Last month or before** in the Timeframe list.

To prevent users from rejecting timesheets approved during the previous week or earlier, select **Last week or before** in the Timeframe list.

Timesheet hours display list

Select how you want approvers to see hours when approving timesheets. Select **hours (decimal)** if you want approvers to see hours as a decimal number, for example 2.33. Select **hours:minutes** if you want approvers to see hours and minutes, for example 2:20. Select **quarter-hour** if you want approvers to see hours rounded to the nearest quarter-hour, for example 2:15.

Approving Timesheets:

Auto Submission - No submission or approval 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 **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, 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.

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 abbreviations for minutes, hours, days, weeks, months, and years.

Getting Here

1) Click **Administration**.

2) On the Administration navigation bar, click **Application Settings**.

3) On the Application Settings page, 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.
❽	**Import/Export Enterprise Data link**: Click **Import/Export Enterprise Data** to import or export your enterprise data to a spreadsheet.

About Managing Enterprise Data

Over time, excess enterprise data can accumulate in P6. For example, if you import a projects using the *Insert New* import action for some data types, when data of those types in the imported file matches data already in the database P6 creates new instances of that matching data. If it is not regularly deleted, this excess data can eventually cause performance issues in the application. However, searching for and deleting excess enterprise data can be a time consuming and labor intensive task.

As an administrator user of P6 you can analyze the usage of enterprise data in the application. On the basis of this analysis, you can identify data that is underused or redundant and use that information to determine which data items are good candidates for deletion.

When you retrieve the usage statistics for enterprise data, columns are automatically added to your view to help you to identify the data you might choose to delete. These columns are:

▸ **Usage Column**: Shows usage information about the enterprise data item. This field displays *Used After* if the data has been summarized or published after the date you selected in the Display Usage Data dialog box or *Never Used*.

▶ **Active Project Count**: The number of currently in use projects and baselines in which the data item is used. On the Resources and Roles tabs of the Resource Administration page and the OBS page, any number over zero is a link that will open a dialog box listing the currently in use projects in which the data is used.

▶ **Inactive Project Count**: The number of obsolete projects and baselines in which the data item is used. On the Resources and Roles tabs of the Resource Administration page and the OBS page, any number over zero is a link that will open a dialog box listing the obsolete projects in which the data is used.

▶ **Last Assigned Date**: The date the data item was most recently assigned in any project.

Select Column: Determines whether the data item might be a good candidate for deletion, based on the options you selected in the Display Usage Data dialog box. This option is only selected by P6 if the data item matches all the conditions you set in the Display Usage Data dialog box. You can also select or clear this option manually. All data items with this option selected are deleted when you select Delete Data on the Actions menu.

You can analyze the usage of enterprise data on the following pages:

The Enterprise Data page

▶ User Defined Fields (UDFs) for all data types
▶ Global and resource calendars
▶ Activity, assignment, issue, project, resource and role codes
▶ Risk categories

The Administration Page

▶ Resources tab
▶ Roles tab

User Administration Page

▶ OBS page

Analyzing Enterprise Data Usage

The Display Usage Data dialog box allows you to specify which projects can be considered obsolete and which data items can be considered inactive. You can also specify the conditions under which P6 will select the Select Column option for data items to signify that they are candidates for deletion.

To analyze enterprise data usage:

1) Click the **Actions** menu, and select **Get Usage Data.**
2) In the **Display Usage Data** dialog box:
   a. On the **Obsolete Projects** tab
      ▪ Select the Project Statuses that signify a project is inactive.
      ▪ Select the **Last Summarized Before** option and select a date to signify that projects most recently summarized before that date can be considered inactive.
      ▪ Select the **Last Published Before** option and select a date to signify that projects most recently published before that date can be considered inactive.

- Select **Next**.

b. On the **Usage** tab:

- Select a date in the **Last Assigned Before** field to signify that date items most recently assigned before that date can be considered inactive.
- Select **Next**.

c. On the **Select Column to Check** tab:

- Select the **Never Used** option to assign the **Select Column** option to data items not used in any project in the database.
- Select the **Last Assigned Before** option to assign the **Select Column** option to data items most recently assigned before the date you selected on the Usage tab.
- Select the **Inactive Project Percentage >=** option and specify a value to assign the **Select Column** option to data items if the percentage of their assignments that are to inactive projects is equal to or higher than the value you specify.
- Select **Select**.

Deleting Obsolete Enterprise Data

On the basis of your analysis of Enterprise Data Usage, you may choose to delete data items identified as obsolete.

> **Note**: Data items with the Select Column option selected will be deleted permanently when you select Delete Data.

To delete obsolete enterprise data items:

1) Review the Select Column and select or clear the option for any data items you wish to add or remove from the list of items to delete.
2) Click the **Actions** ▼ menu, and select **Delete Data.**

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 **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Currencies**.
4) 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. Click ✗**Customize View** and display other fields, such as **Decimal Digits** and **Positive Format**, and edit as needed.
5) Click **Save.**

Adding a Currency

To add a currency:

1) Click **Administration**.

2) On the Administration navigation bar, click **Enterprise Data**.

3) On the Enterprise Data page, expand **Global** and click **Currencies**.

4) On the **Currencies** page:

   a. Click ✿**Row Actions** and select **Add**.

   b. Type an ID for the new currency.

   c. Specify the appropriate values for the currency.

   d. Click **Save**.

About Financial Periods

Financial periods are predefined time periods you can apply to financial or scheduling data throughout the application to 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 365 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 Calendar' global privilege to create, modify, or remove data on the Financial Periods page. 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. A setting in the Display Format section of the Global tab of the My Preferences page determines whether a user can add Financial Period columns to their view and the earliest and latest financial period columns they can add. If a user adds Financial Period columns to their view, they should make sure that the view is using the appropriate financial period calendar for those columns. To set the financial period calendar for a view, select ✕**Customize View**, select the Gantt tab, then choose the appropriate financial period calendar on the Financial Period list.

Creating Financial Period Calendars

Create financial period calendars to measure and compare financial data when projects have different financial periods. You can create multiple financial period calendars using different periods and different period lengths. For example, some projects might use monthly financial periods while others require weekly financial periods.

To create a financial period calendar:

1) Click **Administration**.

2) On the Administration navigation bar, click **Enterprise Data**.

3) On the Enterprise Data page, expand **Global** and click **Financial Periods**.

4) On the Financial Periods page:

   a. Click ＋**Add**▾.

      ▪ Select **Blank financial period calendar** to create a new calendar with no periods assigned.

      ▪ Select **Copy from existing financial period calendar** to select an existing calendar with periods similar to those you want to use in the new calendar.

   b. If you selected to copy an existing calendar, in the Select Financial Period Calendar
      dialog box:

   - Select a calendar to use as the basis for the new calendar.
   - Click **Show**≫ to view the financial periods which have already been created for
     the calendar.
   - Click **Select**.

   c. Type a name for the calendar and click **Save**.

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 **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Financial Periods**.
4) On the Financial Periods page:

   a. Select a calendar.

   b. On the Financial Periods tab, click ＋**Add**.

   c. To change the default name for the new financial period, click the **Name** field, and enter a
      name.

   d. To change the **Start Date** field, directly enter a new date, or select a date from the
      common calendar tool.

   e. To change the **Finish Date** field, directly enter a new date, or select a date from the
      common calendar tool.

5) Click **Save**.

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; however, if a
      financial period calendar contains financial periods with a duration of less than one week,
      that calendar is not available in timescales in P6. You can use P6 Professional if you
      need to view data by financial periods spanning increments of fewer than seven days.

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 **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Financial Periods**.
4) On the Financial Periods page, select a calendar.
5) On the Financial Periods tab, click the **Actions** ▼ menu and select **Generate Financial Periods**.
6) In the Generate Financial Periods dialog box:
   a. In the Batch Start Date field, click ▦**Select Date** and select a date from the calendar or type a start date.
   b. In the Batch Finish Date field, click ▦**Select Date** and select a date from the calendar or type a finish date.
   c. Select a Period Cycle.
   d. In the Every field, use the up and down arrows to specify a number.
   e. Click **Add**.
   f. Click ✕**Close**.
7) On the Financial Periods page:
   a. Click **Save**.

Tips

▶ 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; however, if a financial period calendar contains financial periods with a duration of less than one week, that calendar is not available in timescales in P6. You can use P6 Professional if you need to view data by financial periods spanning increments of fewer than seven days.

Deleting a Financial Period

To delete a financial period:

1) Click **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Financial Periods**.
4) On the Financial Periods page:

a. Select a calendar.
b. On the Financial Periods tab, select the financial period you want to delete.
c. Click ✿**Row Actions** and select **Delete**.
d. 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.

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.

To create a global calendar:

1) Click **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Global Calendars**.
4) On the Global Calendars page, click ＋**Add**.
5) 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 **Select**.

6) On the Global Calendars page, click the **Calendar** tab.

7) On the Calendar tab, triple-click the **Name** field and enter a name.

> **Note**: The application automatically assigns the name *New Calendar*.

8) On the Global Calendars page, click **Save**.

9) 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 **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Global Calendars**.
4) On the Global Calendars page:
    a. Click the calendar you want to modify.
    b. Click the Summary tab.
    c. In the **Time Periods** section, type an hour value in each field.
5) Click **Save**.

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 **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Global Calendars**.
4) On the Global Calendars page:
    a. Click on the calendar you want to modify.
    b. Click the **Standard Work Week** tab.
5) On the Standard Work Week tab:
    ‣ Type the number of hours for each work day in the total hours field.
    ‣ Or click and drag on the chart to create work periods for each work day.
6) Click **Save**.

Tips
‣ You can create multiple work periods for each day.
‣ You can delete a work period by moving your mouse over the work period and clicking ✕.

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 **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Global Calendars**.
4) On the Global Calendars page:
    a. Click on the calendar you want to modify.
    b. Click the **Calendar** tab.
    c. On the **Calendar** tab, click the **Date** ⩡ list for a date and select **Set to Standard** or **Nonwork**.
5) Click **Save**.

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 **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Global Calendar**.
4) On the Global Calendar page:
    a. Click on the calendar you want to designate as the default calendar.
    b. Click ✿**Row Actions** and select **Set as Default Calendar**.
    c. Click **Save**.

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 **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Overhead Codes**.
4) On the Overhead Codes page:

   a. Click ＋**Add**.

   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**.

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 **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Timesheet Periods**.
4) On the Timesheet Periods page:

   a. Click ＋**Add**.

   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**.

About Table Auditing

Table auditing helps you to determine what changes have been made at a table level in the database. You can log changes made to each table regardless of who made the change or when the change was made. You can then run reports on audited data. Two sample BI Publisher reports are available.

> **Notes**:
>
> ▪ You must configure auditing before any data will be captured against which you can run reports.
>
> ▪ Table auditing involves an increased amount of interaction between P6 and the database, which can affect performance.

Configuring Audit Settings

Configure Auditing in P6 so that you can produce reports about incremental changes to projects and project related data.

> **Note**: Table auditing involves an increased amount of interaction between P6 and the database, which can affect performance.

To configure Auditing:

1) Click **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, click **Audit**.
4) On the Audit page:
   a. In the **Interval to store user login information (in days)** field, enter a number of days.
   b. In the **Interval to store audit information (in days)** field, enter a number of days.
   c. In the Select the tables and operations to audit list, select a table or operation to audit and click **Add**.
   d. In the Audit Tables section:
      - Select **Audit Insert** to audit insertions to the table.
      - Select **Audit Update** to audit updates to data in the table.
      - Select **Audit Delete** to audit deletions of data in the table.

      > **Notes**:
      > - Select **Audit Inserts** to see when new rows have been added to that table. For example, auditing inserts on the PROJECT table will show you when someone has created a new project.
      > - Select **Audit Updates** to see when data in a table has been edited. For example, auditing updates on the PROJECT table will show you when someone has changed the name of a Project.
      > - Select **Audit Delete** to see when data in a table has been deleted. For example, auditing updates ona the PROJECT table will show you when someone has deleted a project.

   e. Select **Enable auditing for all tables**.
5) Click **Save**.

Tips

- To stop auditing on a particular table, remove it from the list by selecting ✕**Delete**.
- If you need to suspend all auditing without changing the configuration of the actions and tables which will be audited, clear the **Enable auditing for all tables** option.

About Stored Images

Store images to be used in the header or footer of printed pages. Users do not need to have access to a shared network location to use these stored images. A central repository of images makes it easier to ensure that all users have access to the correct images and logos.

You can store images in P6, P6 Professional, and Primavera Virtual Desktop and use the images to print from any of the applications connected to the database.

Creating Stored Images

Store images to use in the header and footer of printed output.

To create an overhead code:

1) Click **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Stored Images**.
4) On the Stored Images page:
   a. Click $+$**Add** and select an image file.
   b. In the **Name** field, double-click and type a unique code.
   c. In the **Description** field, double-click and type a description.
   d. Click **Save**.

Converting Classic Views

You can use the View Migration Utility (VMU) to convert classic views into standard views. You must be assigned the Admin Superuser global security profile to use the VMU.

When you use the VMU, you can choose to convert all classic views, or to convert views according to user scope (global, multiple user, or user views). After conversion, the new views will have the same user scope as the classic views had, for example, a migrated multiple user view will be assigned to the same users to which the original view was assigned.

> **Note**: Only perform this process once to avoid creating duplicate views.

To convert classic views to standard views:

1) Log in to P6.
2) In the address bar of your browser, delete any text after /p6/ and replace it with **dm/ViewMigration.jsp**.
   For example:
   ```
   http://<server>:<port>/p6/dm/ViewMigration.jsp
   ```
3) Select the group of views you want to migrate.
4) Select **Import**.

Tips:
▶ You can close the window and continue to work while the views are being migrated. When the view migration is complete, you will receive a notification in P6.

Administering P6 Professional for Cloud

Depending on your company's P6 EPPM Cloud Service, you will either use P6 Professional Cloud Connect or Primavera Virtual Desktop for P6 Professional.

For more information about P6 Professional Cloud Connect, see *Using P6 Professional with P6 Professional Cloud Connect for Cloud* (on page 124).

For more information about Primavera Virtual Desktop, see *Primavera Virtual Desktop for Cloud* (on page 127).

Installing Multiple Versions of P6 Professional

You can install multiple versions of P6 Professional on the same machine.

Tips

▶ If you change, repair, or remove a version earlier than 18.5, all other installed versions are also removed. If you uninstall version 18.5 or newer, only that version is removed.

▶ Multiple users can install P6 Professional using ClickOnce on the same machine, however each user can only install one version of P6 Professional.

ClickOnce for Cloud

ClickOnce simplifies the deployment process for your P6 Professional applications while providing you with a secure runtime environment. ClickOnce is configured and provided to you by your Oracle support representative. It contains all of the information that you need to install or upgrade your P6 Professional client application software and to enable P6 Professional Cloud Connect to communicate with your P6 EPPM Cloud database.

ClickOnce Prerequisites for Cloud

> **Note:** System administrators should update .NET and other prerequisites on all client computers before upgrading or installing P6 Professional.

Ensure that you have required prerequisites before you attempt to run ClickOnce:

▶ A compatible version of Windows operating system.

> **Note:** ClickOnce is only supported for Windows operating systems.

▶ .NET Framework

You must have administrator privileges on your machine to install some of the ClickOnce prerequisites. If you do not have the required version of .NET and do not have administrator privileges on your machine, then the ClickOnce installation will fail and you should contact your system administrator.

See https://docs.microsoft.com/en-us/dotnet/framework/deployment/guide-for-administrators for more information about .NET prerequisites. See   document for more information on supported versions of Windows and .NET.

Prerequisites for Signing and Deploying P6 Professional Using ClickOnce

The staging computer must meet the following prerequisites in order to configure ClickOnce:

▶ It must be running Windows Server 2012 R2, Windows 10, Windows Server 2016, or Windows Server 2019.
▶ The latest Java Development Kit (JDK) must be installed. See http://www.oracle.com/technetwork/indexes/downloads/index.html#java for details.
▶ The location of the Windows SDK for .NET Framework must exist in the Path environment variable.

In addition, you must obtain a digital certificate from a certificate authority (for example, VeriSign) for signing the ClickOnce files. The certificate must be in Personal Information Exchange (PFX) format and must include the private key created on your staging computer. Windows SDK is also required for signing ClickOnce files.

System administrators should also update the following prerequisites on all client computers before upgrading or installing P6 Professional:

▶ Windows Operating System
▶ .NET Framework

> **Note:** If you update your P6 Professional installation to version 17 from a previous release, you must ensure all client computers have .NET 4.6.2 installed. If .NET 4.6.2 is not installed on your client machines, the update will fail. System administrators should update .NET and other prerequisites on all client computers before upgrading or installing P6 Professional.

If you do not have the required version of .NET, the ClickOnce installation will fail and you should contact your system administrator.

Installing P6 Professional with ClickOnce for Cloud

P6 Professional ClickOnce installation performs the following:

▶ Installs a supported version of .NET onto the machines of users who either do not have .NET or have a version of .NET that is not supported for ClickOnce.
▶ Installs and upgrades the P6 Professional client application software.
▶ Configures the connectivity between the client software and the P6 Professional Cloud Connect server.

Installation Scenarios for Cloud

Installing P6 Professional for the First Time

If you have never installed P6 Professional, click **Install** to begin the P6 Professional ClickOnce installation. ClickOnce will check and install any missing prerequisites before beginning installation.

Upgrading P6 Professional with ClickOnce Installation

If you have installed P6 Professional using ClickOnce, your P6 Professional installation will be automatically updated when new versions are available, unless your administrator disabled mandatory updates. If mandatory updates are not enabled, you will be notified when a new version of P6 Professional is available. Click **Install** to proceed with the upgrade.

Upgrading and Patching P6 Professional Scenarios for Cloud

Every time a user attempts to log in to an instance of P6 Professional that has been installed using ClickOnce, P6 Professional checks the server from which it was launched for the most recent version of the application. If the version on the server is the same as the version the user is using, then nothing will happen and the user can begin to use the application. However, if a more recent version of P6 Professional becomes available as either a patch or an upgrade, the user's P6 Professional installation will be automatically updated to the latest version, unless your administrator has disabled the **mandatory update** option**.** If the mandatory update option is not enabled, then the **Update Available** dialog box will appear to users and prompt them to update or skip the P6 Professional version update.

> **Caution:** If you update your P6 Professional installation to version 17 from a previous release, you must ensure all client computers have .NET 4.6.2 installed. If .NET 4.6.2 is not installed on your client machines, the update will fail. System administrators should update .NET and other prerequisites on all client computers before upgrading or installing P6 Professional.   For more information on P6 Professional prerequisites see *Prerequisites for Signing and Deploying P6 Professional Using ClickOnce* (on page 120).

> **Note:** If your administrator disabled mandatory update, the **Update Available** dialog box appears only once for each new version of P6 Professional. If users choose to skip the version update, the **Update Available** dialog box will not display in the application until a newer version update becomes available on the server.

The following sections describe the different patching and upgrading scenarios that users might experience.

Accepting a Version Update

When a user accepts the version update, that user's P6 Professional instance will close and automatically patch or upgrade their instance. After the patching or upgrade process completes, P6 Professional launches to the application login page.

The following list represents the process a user experiences when accepting a version update:

1) A user attempts to log in to P6 Professional. P6 Professional checks the Oracle Primavera server for a new version of P6 Professional and determines that there is a new version of P6 Professional available that the user can download and install.

2) The **Update Available** dialog box appears to the user. The user clicks **OK**.

3) The user's instance of P6 Professional closes, the new version of P6 Professional downloads from the Oracle Primavera server, and P6 Professional silently updates to the most recent version. Users can check the progress of their update with the **Updating P6 Professional** dialog box.

4) After the update completes, P6 Professional opens the **Login to Primavera P6 Professional** login page.

Declining a Version Update

If a user declines the update, then that user will no longer receive a prompt to update their P6 Professional instance for that version.

The following list represents the process a user experiences when declining a version update:

1) A user attempts to log in to P6 Professional. P6 Professional checks the Oracle Primavera server for a new version of P6 Professional and determines that there is a new version of P6 Professional available that the user can download and install.

2) The **Update Available** dialog box appears to the user. The user clicks **Skip**.

3) The user logs in to P6 Professional.

4) Later, when the user logs out of P6 Professional and attempts to log back in, P6 Professional checks the Oracle Primavera server for a new version of P6 Professional and determines that the version of P6 Professional on the server is a version update that the user chose to skip. P6 Professional opens the **Login to Primavera P6 Professional** login page.

Updating a Version if Initially Declined

If a user declines to update their version of P6 Professional when the **Update Available** dialog box appears, but later decides that they want to update their version, then users will need to navigate to the Primavera Portal to update their application instance.

The following list represents the process a user experiences when updating P6 Professional if they initially chose to skip the update:

1) A user attempts to log in to P6 Professional. P6 Professional checks the Oracle Primavera server for a new version of P6 Professional and determines that there is a new version of P6 Professional available that the user can download and install.

2) The **Update Available** dialog box appears to the user. The user clicks **Skip**.

3) The user logs in to P6 Professional. Later, the user realizes that they want or need to update their instance of P6 Professional to the latest version.

After users determines that they want to update their version of P6 Professional after they have initially declined the update, they can use the following procedure to update their instance:

1) Close **P6 Professional**.

2) Log in to the **Primavera Portal** using the URL provided by their cloud administrator.

3) Click **Install P6 Professional**.

4) On the **Installing P6 Professional With ClickOnce** page, click the   **Install** button..

5) In the **Opening setup.exe** dialog box, click **Save File**.

6) Run **setup.exe**.

Reverting to a Previous Patch

As users update their P6 Professional instances to new patches, they might find that they prefer to use earlier versions of P6 Professional rather than their current version. Rather than using their current version until a newer version becomes available, these users can revert their version to a previous patch.

To revert an instance of P6 Professional to a previous patch:

1) Click **Start**.

2) Click **Control Panel**.

3) Click **Programs and Feature**.

4) Right click the **P6 Professional** item.

5) On the **Primavera** dialog box that asks "Do you wish to uninstall Primavera and all its components?", click **Yes**.

6) On the **P6 Professional Maintenance** dialog box, select **Restore the application to its previous state** and the click **OK**.

Creating a Standalone SQLite Database to Work Offline for Cloud

After you install or upgrade P6 Professional with ClickOnce, you can work offline in P6 Professional (that is, not connected to the P6 Professional Cloud Connect database) and then upload the changes to the P6 Professional Cloud Connect database. To do this, you must use dbconfig to create a P6 Professional Standalone SQLite database. dbconfig is included as part of a ClickOnce installation.

To use dbconfig to create a P6 Professional Standalone SQLite database, complete the following steps:

1) Run **dbconfig.exe** as an Administrator from the command line. On the **Select Driver Type** dialog box, in the **P6 Professional driver type** field, select **P6 Pro Standalone (SQLite)**.

2) Click **Next**.

3) Select **Add a new standalone database and connection**.

4) Click **Next.**

5) In the **Enter new password** field and the **Confirm new password** field, enter a password for the admin user.

6) Click **Next**.

7) Select **Load sample data** if you want to install sample projects.

8) Click **Next**.

9) When the **Connection Successful** message displays**,** click **Finish** to exit Database Configuration.

Using P6 Professional with P6 Professional Cloud Connect for Cloud

In high latency environments, performance can be affected by the amount of data that needs to be transferred between P6 Professional and the P6 database.

When you connect to a Cloud Connect database, P6 Professional caches some data locally to improve performance. The data in your local cache is automatically synchronized with the Cloud Connect database in the background. The first time you connect to a Cloud Connect database, or if you mark the Reinitialize local cache option when connecting, a large amount of data will be downloaded from the Cloud Connect database and stored in the local cache. This can mean that P6 Professional takes longer to open. Some changes to your security profile also trigger a refresh of the local cache which will cause P6 Professional to take longer to open. In all these cases, once P6 Professional opens, performance will be improved.

To optimize the amount of data that flows between P6 Professional on your desktop and the P6 server, ensure that you have a stable, wired connection to the P6 server and follow the guidelines described in this section.

Working With the Launcher

Once P6 Professional opens, the launcher (Primavera.CacheService.exe) minimizes to the status tray. You can right-click on the status tray icon to show the launcher, reload P6 Professional and reconnect to the same Cloud Connect database, or exit the launcher and stop synchronization with the Cloud Connect database. If you exit the launcher it will restart next time you launch P6 Professional.

Improving Login Performance

Login performance is affected by the amount of data that gets loaded during the login process. You can control this data by following the tips described below:

- Evaluate user privilege assignments to ensure that your users have access to only relevant data.
- Remove unused global objects from the system, including unused UDFs or Code assignments.
- Set the startup filters to load Current Projects Only Data and turn off loading for Resource Summary Data.

Enabling the Welcome Dialog

Enable the **Welcome dialog** from **User Preferences** dialog box to select the project at application startup. Selecting a project at startup ensures that you do not open a project that you had not intended to open or are not required to switch to the correct project after an incorrect project loads in the application.

> **Note:** You should only enable the **Welcome dialog** if you work on different projects.

To configure the **Welcome dialog**:

1) Log in to P6 Professional.
2) From the toolbar, select **Tools** and then click **User Preferences**.

3) In the **Application Startup Window** menu, under the **Application** tab, select **None**.
4) Select the **Show the Welcome dialog at startup** checkbox.
5) Exit the User Preferences dialog box.

Creating and Selecting a Portfolio with Only the Required Projects

Oracle recommends that you do not use the All Projects portfolio because it will load all the projects in the database to which the user has access. Instead, you can either create a new portfolio with your required projects or you can open the No Projects portfolio when logging in to the application.

To create a new portfolio:

1) Log in to P6 Professional.
2) From the toolbar, select **Enterprise** and then click **Project Portfolios**.
3) Click **Add** to create a new portfolio.
4) Add the required projects to the portfolio.
5) From the toolbar, select **File** and then click **Select Project Portfolio**.
6) Select the portfolio.

> **Note:** Ensure **EPS bands only for projects in current portfolio** option is selected when opening a portfolio.

Configuring Startup Options

To configure the startup options:

1) Log in to P6 Professional.
2) From the toolbar, select **Tools** and then click **User Preferences**.
3) Under the **Startup Filters** tab, deselect the **Resource Summary Data** checkbox.
4) Select the current project data; this only applies to for Resources, Roles, OBS, Activity Codes, and Cost Accounts.

Improving Functional Performance

▸ Use Exclusive mode to open projects to perform actions, such as updating the schedule. Only the user that opens a project in Exclusive mode can edit it; other users are prevented from making changes.

▸ When possible, use filters to reduce the amount of data that is loaded or displayed.

▸ P6 Professional commits data whenever a new row is added. If your network or Internet connection experiences high latency, it can take longer for data to be committed. To reduce this time, create a local Excel file and then import then data using XLS import.

Alternatively, you can use a Standalone SQLite database to enter the data and use XML export/import to move the data to main database. See the *P6 Professional Installation and Configuration Guide (Standalone)* for details.

▸ Import layouts separately from projects when doing XML import. This allows the import to run in the background.

▸ Use P6 to schedule recurring tasks like summarizer, apply actuals, scheduler, and so on, during off-peak hours.

- Avoid frequently scheduling projects.
- Use Refresh (F5) only when necessary because it forces P6 Professional to reload data from the server.

Resetting User Preferences

When a user has become locked out of P6 Professional Cloud Connect, the cause is sometimes that the record in the database which stores their user preferences has become corrupt. Administrators can delete user preferences on the User Administration page for those users to allow them back into P6 Professional Cloud Connect. When you delete a user's preferences, that user's preferences will be reset to the defaults so they might choose to re-configure their preferences when they are able to log back into P6 Professional Cloud Connect. If the user has access to P6, they can delete their preferences themselves on the My Preferences page.

To reset users' preferences:

1) Log into P6 as a user with administrative privileges.
2) Click **Administration**.
3) On the Administration navigation bar, click **User Administration**.
4) On the User Administration page, click **Users**.
5) On the **Users** page:
   a. Select the users whose preferences you want to reset.
   b. Click **✿Row Actions** and click **Reset User Preferences**.
6) On the **Users** page, click **Save**.

> **Note**: Users must be logged out of P6 Professional Cloud Connect before you reset their preferences. When they log back into P6 Professional Cloud Connect they must select the **Reinitialize local cache** option for the database.

Removing a P6 Professional Instance Installed with ClickOnce

To remove a P6 Professional instance installed with ClickOnce:

1) Open **Control Panel** and click **Programs and Features**.
2) In the list of installed applications, click the P6 Professional item and click **Uninstall**.
   - At the prompt "Do you wish to uninstall Primavera and all its components?" click Yes.

When the process has completed, Oracle recommends you open Programs and Features, click F5 to refresh the view, and check that Primavera P6 Professional is no longer listed. If Primavera P6 Professional is still listed, or you were unable to remove the P6 Professional instance using the instructions above, you must remove the P6 Professional manually.

To remove a P6 Professional instance manually:

1) In Registry Editor:
   a. Navigate to the following path:
   ```
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninst
   all
   ```

b. Look for a folder which contains both of the following keys:

Name: **DisplayName**. Type: **REG_SZ**. Data: **P6 Professional (x64)**

Name: **Publisher**. Type: **REG_SZ**. Data: **Oracle - Primavera P6**

c. Right click on the folder which contains the two keys listed above and select **Delete**.

2) In File Explorer:

a. Navigate to the following path:

`%USERPROFILE%\AppData\Local\Apps\2.0\.`

  ▪ In the Search field, enter p6pr and allow the search to complete.

  ▪ Delete all files and folders found by the search.

b. Navigate to the following path:

`%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\.`

c. Delete the **Oracle - Primavera P6** folder.

Primavera Virtual Desktop for Cloud

Prerequisites for Cloud

You must do the following before using Primavera Virtual Desktop:

1) Check the version of browser installed on your computer and upgrade if necessary. See *Client System Requirements*.

2) Add https://*.oraclecloud.com as a trusted site in your internet options. See ***Adding the Oracle Cloud URL to Trusted Sites*** (on page 128).

3) Install Adobe Acrobat Reader on your local computer. Adobe Acrobat Reader can be downloaded from https://get.adobe.com/reader.

4) Install the Secure Global Desktop (SGD) client. See ***Accessing P6 Professional with Primavera Virtual Desktop for Cloud*** (on page 129)

5) Optionally configure access to your local drives from Primavera Virtual Desktop. See ***Accessing Local Drives*** (on page 129).

In addition, some further prerequisites for use of Primavera Virtual Desktop must be carried out by a P6 administrator and system administrator. For further information see: ***Administering Primavera Virtual Desktop for Cloud*** (on page 129).

Prerequisites for Accessing P6 Professional with Primavera Virtual Desktop for Cloud

The first time you access P6 Professional with Primavera Virtual Desktop version 18.8 or later, you must install the Oracle Secure Global Desktop client.

To install the Oracle Secure Global Desktop client:

1) Uninstall any existing versions of the Secure Global Desktop client from your system.

2) Browse to the Primavera Portal page.

3) Click the **Primavera Virtual Desktop** link.

> **Note**: If you receive a prompt to launch the application, click **Cancel**.

4) On the Secure Global Desktop loading page, click the **Client Options** link.
5) On the Secure Global Desktop welcome page, click **Install the Oracle Secure Global Desktop Client**.
6) In the installation wizard:
   a. Select the **Install Only For Me** option.

   > **Note**: You can select the Install For Everyone option if you have administrative privileges.

   b. Accept the default options on all further installation screens.
7) Log in to the Primavera Portal.
   a. Click the **Primavera Virtual Desktop** link.
   b. Select the option to launch the application with Oracle Secure Global Desktop Client.
   c. Select **Remember my choice for sgd** links.
   d. Click **Open Link**.

   > **Note**: Launching Primavera Virtual Desktop in HTML5 mode is not supported for cloud.

Tip

▶ For information about Secure Global Desktop product and patch announcements, and up-to-date details on the latest recommended version, see the following knowledge management document:

   Oracle Secure Global Desktop, Release Announcement Reference (Doc ID 2093579.2) (***https://mosemp.us.oracle.com/epmos/faces/DocumentDisplay?id=2093579.2***)

▶ Ten minutes after closing the browser or logging out of Primavera Virtual Desktop, the P6 Professional session times out. If you log back in within ten minutes, the session remains active.

Adding the Oracle Cloud URL to Trusted Sites

To add the Oracle Industry URL to the trusted sites list:

1) In Internet Explorer, click the Tools menu and select Internet Options.
2) In the Internet Options dialog box:
   a. Select the **Security** tab.
   b. Select **Trusted sites**.
   c. Select the **Sites** button.
3) In the Trusted sites dialog box:
   a. In the **Add this website to the zone:** field, type `https://*.oraclecloud.com`.
   b. Select **Add**.
   c. Select **Close**.

4) In the Internet Options dialog box, select **OK**.

Accessing Local Drives

Primavera Virtual Desktop automatically maps to all the local drives you have configured on your computer. This allows you to save documents to locations which you can access when you are not logged in to Primavera Virtual Desktop.

Accessing P6 Professional with Primavera Virtual Desktop for Cloud

Primavera Virtual Desktop enables you to access P6 Professional using your browser via the Primavera Portal. After you enter your username and password and P6 Professional has authenticated your credentials, a virtual desktop for P6 Professional launches.

> **Note**: P6 Professional requires the Oracle Secure Global Desktop Client. See *Prerequisites for Accessing P6 Professional with Primavera Virtual Desktop for Cloud* (on page 127)

To access P6 Professional with Primavera Virtual Desktop:

1) Log in to the Primavera Portal.
2) Click **Primavera Virtual Desktop for P6 Professional**.
3) In the login dialog box:
   a. Enter your username in the **Login Name** field.
   b. Enter your password in the **Password** field.
   c. Click **OK**.

Administering Primavera Virtual Desktop for Cloud

This section contains information about configuring P6 Professional users and Windows users for using Primavera Virtual Desktop.

Administration Prerequisites

Before users can log into P6 Professional using Primavera Virtual Desktop, you must:

1) Assign users P6 Professional module access rights and project privilege rights in P6.
2) Assign users the Primavera Virtual Desktop role in Primavera Administration. See the *Primavera Administration Identity Management Guide* for details.

> **Note**: After you assign the role assignment, users must wait approximately 10 minutes for the assignment to take effect.

3) Ensure that all usernames in Primavera Administration meet the following requirements.
   ‣ User names must be unique on the computer that is being administered. User names must not be the same as any group names on the computer that is being administered.
   ‣ The user name can be up to 20 alphanumeric characters and symbols and is not case sensitive.

‣ The user name cannot contain the following characters: " / \ [ ] : ; | = , + * ? < > @
‣ The user name cannot consist solely of periods (.) or spaces.

> **Note**: Password can contain up to 127 characters.

Printing Using Primavera Virtual Desktop for Cloud

Primavera Virtual Desktop offers several ways to print from P6 Professional:

‣ **Universal PDF Viewer** enables you to open a PDF of your schedule in a PDF viewer. This option requires that Adobe Acrobat Reader is installed on your computer.
‣ **Universal PDF Printer** enables you to print a hard copy of your schedule. This option automatically selects the printer you have selected as the default. When you print to your default printer, you can change the page orientation in Primavera Virtual Desktop. All other printer settings must be configured for the printer before launching Primavera Virtual Desktop.
‣ **Print to PDF** enables you to create a PDF of your schedule in a location you specify. You must specify a destination for the file each time you print.

> **Notes**:
> ▪ Oracle recommends using the Print to PDF option unless you are printing a hard copy to your default printer.
> ▪ If Universal PDF Printer is not enabled, submit a Service Request in My Oracle Support. The necessary configuration change applies to all users.

Viewing the Primavera Virtual Desktop Print Queue

To view the print queue for Primavera Virtual Desktop:

1) Browse to the Primavera Portal page.
2) Click the **Primavera Virtual Desktop** link.
3) In the Navigation pane, select the **List All Jobs** button.

Changing The Default Overwrite Setting For Print To PDF

When you use the Print to PDF option, by default any existing file will be overwritten with the new file.

To change the default overwrite setting:

1) From the File menu, select **Print Setup**.
2) In the Print Setup dialog box:
   a. On the Name list, select **Print to PDF**.
   b. Click **Properties**.
   c. Select **Destination>**.

d. In the Print to PDF Properties screen, select **File system** and click **Options**.

e. Click **Overwrite without asking** and select a different action from the list.

f. Click **OK**.

Troubleshooting

Java Version and Browser Mismatch

It is important for Internet Explorer and the Java Runtime Environment (JRE) to be compatible.

To check whether Internet Explorer is using 64 or 32 bit tabs:

1) Open Internet Explorer and open several tabs.
2) Right click on the Windows start bar and select Task Manager.
3) In the Image Name column, look for iexplore.exe
   ‣ If you see multiple entries of iexploere.exe *32, Internet Explorer is using 32-bit tabs.
   ‣ If you see only entries of iexplore.exe, Internet Explorer is using 64-bit tabs.

If Internet Explorer is using 64 bit tabs, download and install 64-bit JRE.

If Internet Explorer is using 32-bit tabs, you can either switch on Enhanced Protection Mode in Internet Explorer, or download and install 32-bit JRE.

To switch on Enhanced Protection Mode:

1) Open Windows Control Panel and select **Internet Options**.
2) In the Internet Properties dialog box:
   a. Click the **Advanced** tab.
   b. Scroll to the Security section and select **Enable Enhanced Protection Mode***.
   c. Click **OK**.
3) Restart your computer.

Secure Global Desktop Is Blocked By Virus Scanning Software

If the virus protection software installed on your computer incorrectly identifies components of Cloud Services as suspicious, contact your IT team.

Network Level Authentication Failure

If you receive an message about network level authentication having failed, see: *Secure Global Desktop Error "Session Failed: Network Level Authentication Failed" When Attempting to Launch P6 Professional via Primavera Virtual Desktop (Doc ID 2200935.1)* at https://support.oracle.com/epmos/faces/DocumentDisplay?id=2200935.1

P6 Professional Does Not Allow You to Select a File Destination

When you are printing in Primavera Virtual Desktop, if you receive a message that a report has been printed, but you are not able to select a destination for the report output:

1) In the Print dialog box, select **Properties**.
2) In the Print to PDF Properties dialog box, select a file location for the report.

Network Connectivity Loss

If Primavera Virtual Desktop crashes because of a loss of network connectivity, ensure that you have a reliable internet connection with your provider before logging back into Primavera Virtual Desktop.

Local Drives Are Not Available

If the local drives configured for your computer are not available inside Primavera Virtual Desktop, log out of P6 Professional and then log out of Primavera Virtual Desktop. Log in to Primavera Virtual Desktop.

Primavera Cache Service for Cloud

Primavera Cache Service dramatically improves the performance of P6 Professional in a cloud environment. The service synchronizes data in a local cache database with a Cloud Connect database while you work in P6 Professional and even after the application is closed. Primavera Cache Service greatly enhances user experience by improving the speed of the most frequent operations: adding, deleting, and updating activities.

While you work in P6 Professional you are working in the local cache database which provides increased performance over connecting to the Cloud Connect database directly. In the background, the Primavera Cache Service continues to synchronize global data and data for the projects you are working in between the local cache database and the Cloud Connect database.

Architecture for Cloud

An embedded SQLite database is at the core of Primavera Cache Service. The SQLite database has a schema similar to a P6 EPPM database and caches data for projects you open, as well as global data that is related to those projects. By default, data is synchronized every 30 seconds between the local cache database and the Cloud Connect database.

The following diagram shows the software components and their interactions:
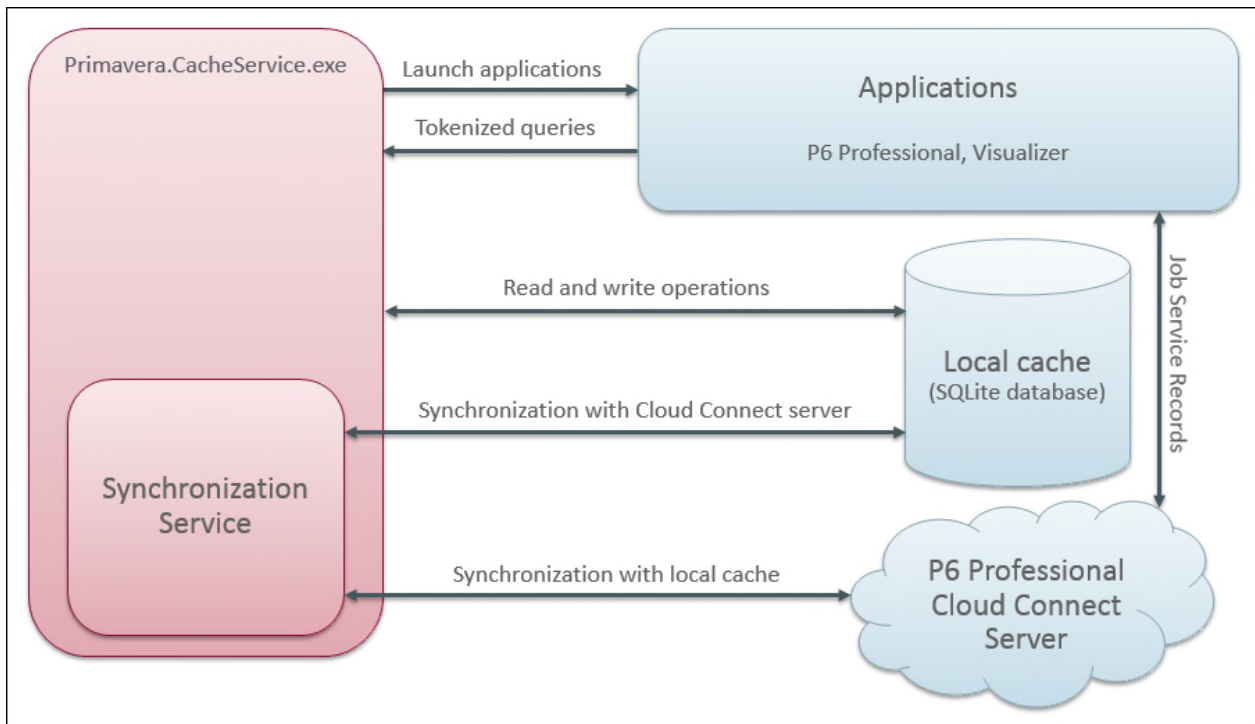
When a user logs in to a Cloud Connect database using Primavera Cache Service, the service checks for a local cache database for the selected Cloud Connect database in the appdata folder for that user. If a local cache database already exists, the service synchronizes global data between the local cache database and the Cloud Connect database before opening P6 Professional. If there is not already a local cache database for the selected Cloud Connect database in the appdata folder for the user, the service creates an embedded SQLite database with a name in the format `sync_<cloud connect alias name>_<user name>.db` and then and loads global data into the newly created local cache database from the Cloud Connect database.

Connecting without Cache

If your the security policy for your organization forbids the downloading of server data to a local machine, you can prevent a user from using the Primavera Cache Service altogether. To prevent the downloading of data to a local machine, clear the **Enable Client-side Cache** option when setting up the P6 Professional Cloud Connect database connection in the database configuration tool. If the client-side cache is not enabled, Primavera.CacheService.exe does not continue to run when you exit P6 Professional.

Primavera.CacheService.exe for Cloud

Primavera.CacheService.exe manages local cache databases for each P6 Professional Cloud Connect database you log in to and ensures that each local cache database is synchronized with the relevant Cloud Connect database.

When you open P6 Professional from the shortcut, Primavera.CacheService.exe runs and allows you to log in to and manage Cloud Connect database connections. When you log in to a Cloud Connect database, Primavera.CacheService.exe starts P6 Professional and then minimizes, but continues to run in the status tray. When you connect to a P6 Professional Cloud Connect database, Primavera.CacheService.exe continues to run even after you close P6 Professional so that the service can continue to synchronize the local cache databases with the relevant Cloud Connect databases.

If you most recently logged into a Cloud Connect alias, Primavera.CacheService.exe continues to run as a status tray application after P6 Professional exits. This allows the cache service to continue synchronizing the local cache databases with Cloud Connect databases, so that P6 Professional starts more quickly the next time you connect. If the Primavera.CacheService.exe is running in the status tray, you can right click on it and select **Start P6 Professional** to restart P6 Professional. You can maximize Primavera.CacheService.exe at any time by right-clicking on the icon in the status tray and selecting **Show**.

Logging On and Creating a Local Cache for Cloud

When you first log on to a Cloud Connect database, the Primavera Cache Service initializes the relevant local cache database and copies all global data from the cloud database to the newly created local cache database, including the EPS structure as well as project IDs and Names. The first time you open a project, all data in that project and any related global data is copied to the local cache database. From that point onwards, regular synchronizations will transfer all changed data for open projects and all global data between the cloud and local cache databases. If no projects are open only global data is synchronized.

There can be a delay during startup under certain circumstances. The first time you connect to a specific Cloud Connect database, the service builds and then loads data into a local cache database from the Cloud Connect database. If you select the **Reinitialize local cache** option when you log on to a Cloud Connect database, the service rebuilds the local cache database. Performance is significantly improved when connecting to an existing local cache or when Primavera.CacheService.exe is already running.

If you want to connect to a different Cloud Connect alias, click **Disconnect** for the alias you most recently used. After the service has disconnected from the previous database, you can select a different Cloud Connect alias.

Reinitializing Primavera Cache

Primavera Cache Service synchronizes data between the local cache and Cloud Connect database for the projects you are currently working in and any global data used by those projects. Data will be added to the cache as necessary. If there are projects stored in your local cache which you no longer need to work on, you can clear this data from the local cache by selecting the **Reinitialize local cache** option when you log into a Cloud Connect alias. The local database will be reinitialized and repopulated with the projects you had open last time you worked in that Cloud Connect database and the global data used by those projects. Restarting P6 Professional after reinitializing the local cache will take longer than restarting without reinitializing the local cache because the fresh data must be downloaded before P6 Professional can open.

> **Note**: If data is present in the local cache database but has not yet been synchronized to the Cloud Connect database, reinitializing the local cache will result in that local data being lost.

Synchronizing Data Between the Local Cache and the Cloud Connect Database for Cloud

Primavera Cache Service performs two-way synchronization, that is the service synchronizes data from the local cache to the Cloud Connect database and from the Cloud Connect database to the local cache. The date and time of the last successful synchronization for each project is shown in the Last Sync Date column in P6 Professional.

By default, the synchronization will run at 20 second intervals, which is optimum for most systems. If you need to adjust the frequency at which synchronizations are initiated, change the value for the SyncInterval key in the Primavera.CacheService.Exe.Config file. The value represents the number of seconds between synchronizations. Values lower than 1 are ignored.

To determine which data needs to be synchronized, the last update date or insert date for each data item is compared between the cloud database and the local cache. If your data connection is interrupted, your changes are stored in your local cache database and will be synchronized with the cloud database when connectivity is restored.

During the synchronization process, there is potential for conflicting changes if multiple users are modifying the same data. The synchronization service applies the following rules to resolve conflicts:

1) A delete operation will always take precedence over other operations.
2) If the same data is modified both on the server and on the client, client-side changes takes precedence over server-side changes.

> **Note**: Primavera Cache Service does not check for the chronological order of updates to resolve conflicts.

For example, consider a situation where Client A and Client B are both connecting to the same cloud database and working in the same project. Client A applies an actual start to activity A1000. The next time Client A synchronizes with the cloud database, the last updated date for activity A1000 will be compared between the local cache database and the cloud database. Since the data is newer on the client than on the server, Primavera Cache Service running on Client A will copy the data for Activity A1000, including the status and actual start date, from the cache database on Client A to the cloud database. The next time Client B synchronizes with the cloud database, the Primavera Cache Service running on Client B compares the last updated date for activity A1000 between the client cache database and the cloud database. Because the cloud database has a later last updated date for activity A1000, the Primavera Cache Service running on Client B will copy the data for activity A1000, including the status and actual start date, from the server to the cache database on Client B.

Offline Mode

It is not always possible to have a steady connection to the internet. Offline mode uses the Primavera Cache Service to allow users to continue working in P6 Professional while their internet connection is unavailable. When internet connectivity is restored, users can reconnect to the cloud database and synchronize the data in the local cache database with the Cloud Connect database.

Before users can work in offline mode, you must complete the following steps:

▶ *Enabling Offline Mode* (on page 136)
▶ *Assigning the Global Security Privilege* (on page 136)
▶ *Configuring the Local Cache* (on page 137)

Considerations For Working In Offline Mode

There are several factors which can influence the decision about whether to allow users to work offline.

How many people are working on a schedule at any one time? If there is typically only one planner or scheduler making updates to a project or set of projects, or if multiple planners or schedulers are working on a project but they are working with unrelated data working offline might be a good fit for your organization. However if multiple planners or schedulers regularly update the same data in the same projects, working offline will not be good fit.

Enabling Offline Mode

An application setting in P6 controls the availability of the global security privilege which allows users to work in offline mode.

To enable offline mode:

1) Login to P6 as a user with the *Edit Application Settings* global security privilege.
2) Click **Administration**.
3) On the Administration navigation bar, click **Application Settings**.
4) On the Application Settings page, click **General**.
5) In the General pane, select **Enable offline mode**.
6) Click **Save**.

> **Note**: If you clear the Enable offline mode option, users will no longer be able to go offline. Users who are already working offline at the time that the option is cleared will be able to continue working offline until the next time they connect to the cloud connect database, after which they will not be able to go offline again.

Assigning the Global Security Privilege

To allow users to work in offline mode, you must assign them to a global security profile which includes the correct privileges.

To assign the global security privilege to a profile:

1) Login to P6 as a user with the *Add/Edit/Delete Users* global security privilege.
2) Click **Administration**.
3) On the Administration navigation bar, click **User Administration**.
4) On the User Administration page, click **Global Security Profiles**.
5) On the Global Security Profiles page:
   a. Select a profile to which you want to add the offline mode privilege.
   b. Click the **Tools** detail window.
   c. Enable the **Enable Work Offline** option.

   > **Note**: To see this privilege, select the Enable offline mode option in the General pane of Application Settings.

   d. Click **Save**.

Configuring the Local Cache

Offline mode is available with the P6 Pro Cloud Connect database alias and requires the Primavera Cache Service to be configured in the database alias.

To configure the database alias to use Client-side Cache:

1) Start P6 Professional.
2) In the login dialog box:
   a. Click **Edit database configuration**.
3) In the Database Configuration dialog box:
   a. Select a database using the P6 Pro Cloud Connect driver type.
   b. Select **Enable local cache**.

Operations that are Not Cached for Cloud

Some data and operations are only available when you are connected directly to the Cloud Connect database. These include:

▸ Projects which were not open when you were connected to the Cloud Connect database are not cached and are not available in the cache database.
▸ Almost all operations which use job services require an active connection to the Cloud Connect database. This includes: creating and updating baselines, copying baselines with a project, creating reflection projects, applying actuals, and summarizing projects. The only job service operation which can be completed in the cache database is copying a project without copying baselines.
▸ Checking projects in or out and restoring baselines can only be done when connected directly to the Cloud Connect database.
▸ Summary data for projects is retrieved directly from the Cloud Connect database and is not available when working in the cache database.

▶ Modifying global objects that have project-level dependencies, including resource assignments and shared calendars, can be done both in the cache database and when connected to the Cloud Connect database. However you can only delete those objects when you are connected to the Cloud Connect database.

> **Note**: If the permissions assigned to a user profile change after loading the project, the new permissions will take effect the next time Primavera.CacheService.exe is started.

P6 Team Member Setup Tasks

This chapter covers the tasks for P6 Team Member, P6 mobile, Email Statusing Service, and Timesheets.

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 Email Statusing Service and P6 mobile to status their activities. P6 mobile allows access to P6 Team Member Web functionality. P6 Team Member Web, Email Statusing Service and the P6 mobile apps provide quick, convenient, and easy access to assigned activities using the platform or device that accommodates your line of work.

Your project manager uses P6 to create and update the project schedule and activity 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, Email 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 activities.
▶ Provide status on your activities. 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:

▶ View only your assigned activities.

▶ Provide status updates on your activities. The project manager customizes the status fields in your view. These fields may include time spent, time left, % complete, remaining duration, start date, and finish date.

▶ Provide status updates for other resources assigned to activities.

▶ Modify your view to display your activity list by project and by current status, including Active, Due, Overdue, Starred, or Completed. You can refine your activity 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 an activity with a star to signify its importance to you. You can view all your starred activities in one list when you select the Starred activity list view in the app menu.

▶ View a list of all your steps for an activity. 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 an activity for additional information about the activity. Update codes and UDFs if your project manager requires you to update activity status using these fields.

▶ View the baseline dates for an activity.

▶ View predecessor and successor activity related to an activity and contact resources associated with related activities.

▶ Communicate with the project manager or other team members through email.

▶ Communicate with the project manager about an activity by viewing and posting messages in the Discussion dialog box. All messages are saved with the selected activity.

▶ View and edit notebook topics associated with an activity to see or provide more information about the activity.

▶ View documents associated with an activity 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.

Email Statusing Service

You can use Email Statusing Service to:

▶ Request a list of your current activities through email using the email account associated with your P6 user account. You can request a filtered list of activities by project; time frame; current status, including Active, Due, Overdue, Completed, or Starting; or by all the activities that you starred.

▶ Reply to the email you receive with your activity list, record your progress, and send your updates.

Project managers can use Email Statusing Service to:

▶ Send a Welcome email to new Email Statusing Service users, which includes the email address to the email Statusing Service, and instructions for requesting an activity list and updating the list through email.

▶ Send team members an email request for status updates. Project managers can customize the activity list sent to team members using the available filter options. Team members can provide status by replying to the email with their updates.

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 Apple App Store to download the mobile application.

▶ If you are using an Android device, go to the Google Play Store to download the mobile application.

> **Note**: If you are in a region without access to the Google Play Store, or your organization is using a Content Security Service or Mobile Device Management solution and requires that users do not download P6 mobile from the Apple App Store or Google Play Store, submit a Service Request in My Oracle Support to request versions of the P6 mobile apps for those scenarios.

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, https://*server*.*port*/p6tmws).

b. Enter your P6 username.

c. Enter your P6 password.

d. Tap **Sign In**.

> **Notes**:
>
> - You will need to configure Email Statusing Service separately. See the *P6 EPPM System Administration Guide*.
>
> - P6 for iOS supports SSL (https) or HTTP only when it has a certificate signed by a trusted authority.
>
> - P6 for Android requires SSL (https) when you are not using SSO authentication. If you are using SSO authentication, you can use HTTP or HTTPs protocols. HTTPS requires a valid certificate from an Android trusted certifying authority.

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 System Administration 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.
>
> P6 for Android only accepts SSL certificates from a certifying authority and must use an HTTPS connection.

To start the app:

1) On your device's **Home** screen, tap P6 **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, https://*server*.*port*/p6tmws).

   b. Enter your P6 username.

   c. Enter your P6 password.

   d. Tap **Sign In**.

> **Notes**:
>
> - You will need to configure Email Statusing Service separately. See the *P6 EPPM System Administration Guide*.
> - P6 for iOS supports SSL (https) or HTTP only when it has a certificate signed by a trusted authority.
> - P6 for Android requires SSL (https) when you are not using SSO authentication. If you are using SSO authentication, you can use HTTP or HTTPs protocols. HTTPS requires a valid certificate from an Android trusted certifying authority.

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 System Administration 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.

Setting P6 to Support P6 mobile Users

For users to perform activities 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 for at least one active project. P6 mobile apps will show activities that have not yet started, active activities, and activities 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, Email Statusing Service, or P6 mobile to view and update their assigned activities. 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

If your company is running an older version of P6 EPPM, users can install and use the latest version of P6 for iOS; however, they may not be able to use all the features of P6 for iOS.

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 activities may be incorrect by one hour.
▶ If users do not have any activities 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 the Default Language of the P6 Team Member Web User Interface

The default language of the user interface is English.

To change the default language of your application's user interface:

1) Enter the URL for the application in your browser.

2) At the end of the URL, enter: `?locale=`*<locale_code>*

The locale codes are as follows:

- Arabic = ar

- Brazilian Portuguese = pt_BR
- Dutch = nl
- French = fr
- German = de
- Italian = it
- Japanese = ja
- Korean = ko
- Russian = ru
- Spanish = es
- Simplified Chinese = zh_CN
- Traditional Chinese = zh_TW

For example, to change the language to German, the URL would be http://yourserver/p6tmweb/?locale=de.

> **Note**: The users will need to know their SSO username and password.

Tips:

Bookmark this URL for future access.

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 Settings 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

Name and Description	Default	Valid Ranges/Values
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

Setting Name and Description	Default	Valid Ranges/Values
Allow users to enter negative hours Select to permit users to enter a negative number of hours against an activity.	no	yes/no

Email Service

Setting Name and Description	Default	Valid Ranges/Values
When sending email Select 'Use a separate email client' to allow email from P6 Team Member to be sent using your preferred email client. If this option is selected, users must have an email client installed to send email from P6 Team Member. Select 'Use P6 Team Member email client' to allow users to send email using the email client built into P6 Team Member.	Use P6 Team Member email client	Use a separate email client, Use P6 Team Member email client

Settings for Status Updates

Setting Name and Description	Default	Valid Ranges/Values
Start time to use for not-started activities and assignments Select 'Current time' to specify when a team member clicks or taps Start on a not-started activity or assignment with a start date earlier than the current date, the actual start of the activity or assignment should be set to the date and time the team member clicked or tapped Start. Select 'Start of day' to specify when a team member clicks or taps Start on a not-started activity or assignment with a start date earlier than the current date, the actual start of the activity or assignment should be set to 00:00 (midnight) on the date the team member clicked or tapped Start. Select 'Calendar work period start' to specify when a team member clicks or taps Start on a not-started activity or assignment with a start date earlier than the current date, the actual start of the activity or	Calendar work period start	Current time, Start of day, Calendar work period start

Setting Name and Description	Default	Valid Ranges/Values
assignment should be set to the beginning of the work period according to the relevant calendar.		

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
Time entry Select 'hours (decimal)' to require all resources report their hours as a decimal value. For example 2 hours and 20 minutes would be reported as 2.33. Select 'hours:minutes' to require all resources report their hours as the number of hours and the number of minutes. For example 2 hours and 20 minutes would be reported as 2:20. Select 'quarter-hour' to require all resources report their hours as the number of hours and either 00, 15, 30, or 45 minutes. Minutes values other than 00, 15, 30, or 45 will automatically be rounded to the nearest quarter-hour value. For example, 2 hours and 20 minutes could be reported as 2:20 but would be stored as 2:15.	hours (decimal)	hours (decimal), hours:minutes, quarter-hour

Setting Name and Description	Default	Valid Ranges/Values
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

Notes:

- 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.

- When the Allow resources to enter negative hours option is not selected, it is still possible for users to enter a negative value of hours in a timesheet, for example if it is necessary to correct a previous entry. However, if the number of hours entered would result in a negative number of hours being calculated for the activity, the user will see a message requesting that they enter a larger number.

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 in P6 Team Member interfaces, P6 for Android, or P6 for iOS.

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.

Allow resources to assign themselves to activities outside assigned OBS access option

Determines whether you want every newly created project to grant permission for resources to assign themselves to activities even if the resource does not have access to the relevant OBS for the activity. 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.

Assign themselves to activities with role assignments matching Team Member's role option

Determines whether team members can assign themselves to activities with unstaffed role assignments that match their role.

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.

Enable email notifications option

Determines whether you want timesheet approval managers to be notified by email when a timesheet is rejected. If this option is enabled, when a timesheet is rejected an email will be sent to all Project Managers and their delegates, Resource Managers and their delegates, users with the Admin Superuser profile, and users with the Project Superuser profile assigned for any projects included in the timesheet. This function requires that the relevant users have an email address associated with their user profile. The manager who rejected the timesheet will not receive an email notification.

Prevent users from rejecting approved timesheets option

Determines whether you want to prevent users from rejecting approved timesheets and if so within which time period.

To prevent users from rejecting any approved timesheets, select **All** in the Timeframe list.

To prevent users from rejecting timesheets approved during the previous calendar month or earlier, select **Last month or before** in the Timeframe list.

To prevent users from rejecting timesheets approved during the previous week or earlier, select **Last week or before** in the Timeframe list.

Timesheet hours display list

Select how you want approvers to see hours when approving timesheets. Select **hours (decimal)** if you want approvers to see hours as a decimal number, for example 2.33. Select **hours:minutes** if you want approvers to see hours and minutes, for example 2:20. Select **quarter-hour** if you want approvers to see hours rounded to the nearest quarter-hour, for example 2:15.

Approving Timesheets:

Auto Submission - No submission or approval 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 **Administration**.
2) On the Administration navigation bar, click **Application Settings**.
3) On the Application Settings page, 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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.
4) On the **Users** page:
   a. Select a user.
   b. In the **Associated Resource** field, double-click and click **···Select**.
5) In the **Select Resource** dialog box, select a resource and click **Select**.

> **Note**: In Native Authentication mode, the user's Personal Name will be updated to match the Resource Name. Otherwise, the Resource Name will be updated to match the user's Personal Name.

6) 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 ⚙**Row Actions** and then click **Create Resource**.

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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.
4) In the **Users** pane, select the user and click the **Module Access** detail window.
5) In the **Module Access** detail window, select **Timesheet**.
6) Click **Resources**.
7) On the Resources navigation bar, click **Administration**.
8) On the Administration page, click the **Resources** tab.
9) On the **Resources** tab, select the resource and click the **Settings** detail window.
10) In the **Settings** detail window:
   a. Click •••**Select** in the **User Login** field.
   b. 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 •••**Select**.
12) In the **Select User** dialog box, choose a manager to assign to the resource and click **OK**.
13) Click **Save**.

> **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	**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.
❷	**Generate Timesheet Periods**: To add a batch of timesheet periods, you will click **Actions and then click Generate Timesheet Periods**.

Item	Description
❸	**Timesheet Periods**: You can use the **Timesheet Periods** page to view the timesheet periods already created or to add new timesheet periods.
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 **Administration**.
2) On the Administration navigation bar, click **Enterprise Data**.
3) On the Enterprise Data page, expand **Global** and click **Overhead Codes**.
4) On the Overhead Codes page:
   a. Click $+$**Add**.
   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**.

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: 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 EPPM Application Administration 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 101).

Tips

▶ A setting in Primavera P6 Administrator enables daily emails to be sent to timesheet reviewers listing all the updates pending their review. There is also a setting to allow all users to receive a daily email listing all their timesheets which have been approved or rejected in the past 24 hours.

▶ 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 101), 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 152).

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.

▸ 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 for On-Premises

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 **Administration**.
2) On the Administration navigation bar, click **User Administration**.
3) On the User Administration page, click **Users**.
4) On the **Users** page, click the **Module Access** detail window.
5) Assign users the **Team Member** module access option.

Setting P6 to Support Email 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 activities using P6, and others using Email.

> **Note**: Timesheet users can request a list of their activities using Email Statusing Service; however, timesheet users can only update their activities using P6 Team Member Web.

To support updating assignment status by Email, you will need to:

1) Ensure the users you want to use Email 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 Email address.

4) Assign users to one or more activity assignments for at least one active project. Email Statusing Service will show activities that have not yet started, active activities, and activities 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, Email Statusing Service, or P6 mobile to view and update their assigned activities. OBS access is required for each user with a Team Member work distribution filter assigned.

5) Ensure your users download and install an Email client application or browser to access web mail.

6) Have your teams and managers plan their Email process. For example, consider details such as the timing of updates by Email 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 Email address is assigned to one of these accounts, have them access their account within an SMTP Email client.

Error Messages

Users may receive error messages when updating activities if their Email application is set to return Email messages in HTML format.

One of the following situations will occur:

▸ An Email 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 Email will be returned with a message that the updated value is incorrect because only part of the updated value was parsed by the Email Statusing Service.

The following methods can be used to avoid this issue:

▸ When entering activity updates, delete the original value in its entirety before entering an updated value.

▸ Set the Email application to reply to messages in text format.

▸ Click the **Update this activity** link to update activities individually.

P6 Integration API Setup Tasks for On-Premises

Complete the following task to finish enabling P6 Integration API.

In This Section

Enabling Access to P6 Integration API from P6 for On-Premises

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 54).

To enable access to the P6 Integration API:

1) Log in 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.

P6 EPPM Web Services Setup Tasks

Complete the following tasks to finish enabling P6 EPPM Web Services.

In This Section

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* (on page 54).

To enable access to P6 EPPM Web Services:

1) Log in 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**.

Adding Web Services to the Allow List

P6 can restrict access to web services only to those client IPs provided in the Web Services Allow List.

To add a client IP address to the allow list:

1) Log in to P6 as a user with administrative privileges.
2) On the Administer menu, choose **Application Settings**.
3) On the Application Settings page, click **Integration and Allow Lists**.
4) On the Integration and Allow Lists page, in the Web Services Allow List section, click **Edit List**.
5) In the Edit Allow List dialog box, click ╋**Add**.
6) Type the client IP address to allow access to P6 EPPM Web Services.

> **Note**: Client addresses must be entered using CIDR (Classless Inter-Domain Routing) notation.

7) Click **Save**.

Primavera Risk Analysis Setup Tasks

Primavera Risk Analysis can read project data from a P6 EPPM database in the cloud. By integrating Primavera Risk Analysis with P6 EPPM you can enable P6 users to analyze risks in their projects.

Primavera Risk Analysis and User Access Privileges

Primavera Risk Analysis uses P6 EPPM security when it connects to a P6 EPPM database. Users that have been provisioned to use P6 EPPM applications can only use Primavera Risk Analysis for the projects to which they have access.

Connecting Primavera Risk Analysis to a P6 EPPM Cloud Database for Cloud

To connect Primavera Risk Analysis to a P6 EPPM cloud database:

1) Open **Primavera Risk Analysis**.

> **Note:** If you have Primavera Risk Analysis open, you must close any open plans before you can connect to a P6 EPPM Cloud Database.

2) Click **File**.
3) On the **File** menu, select **Primavera** and then click **Connection Wizard**.
4) In the **Primavera P6 Connection Wizard** dialog box, complete the following:
   a. Select **P6 Cloud** and then click **Next**.
   b. Enter the required information in the following fields:

   - **Apache CFX Location**: The path to the Apache CXF application.

   > **Note:** You must install the services framework Apache CXF version 2.2.7 in order to connect to P6 EPPM Web Services. You can download Apache CXF from http://archive.apache.org/dist/cxf/2.2.7. After launching the site, you must select the download files that correspond to the windows operating system (for example, `apache-cxf-2.2.7.zip`). Extract the file to a folder on your local machine.

   - **Java JRE Location**: The file path to a version of JRE that is supported byP6 EPPM. For more information about supported versions of JRE, see *Tested Configurations*.
   - **Web Services URL**: The Web Services URL that can be found on the Cloud Welcome page.
   - **Proxy Host**: Enter the proxy host address if your company uses a proxy to connect to the internet. If you do not use a proxy, leave this field empty.
   - **Proxy Port**: Enter the proxy port number if your company uses a proxy to connect to the internet. If you do not use a proxy, leave this field empty.

- **Authentication Method**: Select either **Username Token Profile** or **HTTP Cookie**. You can determine which authentication method that you need to select based on the P6 EPPM Web Services URL from **Web Services Instructions...** on the Primavera Portal.

  If the URL is *https://pgbu-vbe2-p6.oraclecloud.com/p6ws-token*, select **Username Token Profile**.

  If the URL is *https://pgbu-vbe2-p6.oraclecloud.com/p6ws*, select **HTTP Cookie**.

c. Click **Next**.

d. If necessary, complete the following:

- Set the **Java Heap Size.** Java Heap Size is an optional setting to define the Java Heap Size when importing large projects. By default this is set to 512Mb and should remain on this setting unless errors occur importing large projects.
- Select **Always display import log.**
- Select **Use these connection setting for all Primavera Risk Analysis users**.

e. Click **Next**.

f. Click **Finish**.

Overview of Eventing (On Premises Only)

Depending on administrative settings, events can be triggered by changes that take place in the P6 database. These events can be classified into two types of events:

- **Business object events**: Triggered when the P6, the P6 Integration API (on-premises only), or P6 EPPM Web Services is used to update or create objects in the P6 database.
- **Special operation events**: Triggered when a supported operation or job service is invoked.

When a change triggers an event, the P6 Event Notification system sends the event message to a user configured message queue. You can use the events in a client application to trigger subsequent actions. You could, for example, launch an external workflow based on the existence of a specific event.

> **Note:** The content in this section details optional configuration for P6. You do not need to configure eventing for P6 in order to enable P6 for users to work in the application.

Event Triggers

An event may be one of two types, a business object event or a special operation event.

- See Business Object Events for a list of business object events.
- See Special Operation Events for a list of special operation events.

Changes that trigger events

With the exception of the Timesheet object, create and update changes made to supported objects using P6, the P6 Integration API (on-premises only), or P6 EPPM Web Services will trigger an event. When a status change is made to a Timesheet object using P6, a TimesheetUpdated event will be triggered.

Changes that do not trigger events

The following create and update changes do not trigger events:

▶ Create and update changes made to objects that do not support events
▶ Create and update changes made to objects that support events but are not configured to send events
▶ Changes made in P6 Professional

> **Note**: Additionally, an event is triggered when you run either the Apply Actuals or Summarize Job service from P6 Professional.   Receiving either of these events depends on administrative settings and requires that P6, the P6 Integration API (on-premises only), or P6 EPPM Web Services is running on the same database as P6 Professional.

About the Event Messages

The system sends the event messages in an XML format. You can configure the system to send these to a message queue or to an Enterprise Service Bus (ESB).

Cost Information

Using the administrator setting *Show costs*, you can determine whether cost information is included in events.

Event Schema File

The p6events.xsd file is installed in the <installation directory>/schema directory for P6 Integration API (on-premises only) and P6 EPPM Web Services. You can use this file to determine the format of the event messages.

Sample Business Object Event Message

Sample ActivityCreated Message: When an activity is created, the system sends an ActivityCreated message similar to the following message:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<MessagingObjects
xmlns="http://xmlns.oracle.com/Primavera/P6/V8.2/Common/Event"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ActivityCreated>
    <Id>Auto-1</Id>
    <ObjectId>125500</ObjectId>
    <ProjectObjectId>11840</ProjectObjectId>
    <WBSObjectId>36320</WBSObjectId>
  </ActivityCreated>
</MessagingObjects>
```

Sample ActivityUpdated Message: When an activity is updated, the system sends an ActivityUpdated message similar to the following message:

```
<?xml version="1.0" encoding="UTF-8"?>
<MessagingObjects
xmlns="http://xmlns.oracle.com/Primavera/P6/V8.2/Common/Event"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ActivityUpdated>
    <Id>Auto-1</Id>
    <Name>t2</Name>
    <ObjectId>125500</ObjectId>
    <ProjectObjectId>11840</ProjectObjectId>
    <WBSObjectId>36320</WBSObjectId>
    <NewValues>
      <Name>t2</Name>
    </NewValues>
    <OldValues>
      <Name>Auto-1</Name>
    </OldValues>
  </ActivityUpdated>
</MessagingObjects>
```

Testing Event Notification

Test event notification to ensure event messages are sent when an event occurs.

To test event notification:

1) If it is not already installed, install P6. See the *P6 EPPM Installation and Configuration Guide*.

> **Note**: If you are using more than one server, install P6 on the local server.

2) Configure WebLogic for eventing:
   ‣ See ***Configuring the WebLogic Message Queue*** (on page 170) if the queue and the application are on the same domain.
   ‣ See ***Sending Events to a Remote WebLogic JMS Server*** (on page 171) if the queue and the application are on different servers.

3) Open P6 and create a project.

4) In P6:
   a. Add one or more activities to the project.
   b. Summarize the project to test if an event is generated.

5) Launch the WebLogic **Administration Console** to verify that the event is generated and sent to the queue.

6) In the WebLogic **Administration Console**, expand **Services/Messaging** and click **JMS Modules** in the **Domain Structure** pane.

7) On the **JMS Modules** page, click the module you created for the remote server.

8) On the **Settings** page for the module, click the queue you created for the remote server.

9) On the **Settings** page for the queue, click the **Monitoring** tab.

10) On the **Monitoring** tab, select the option for the remote server destination you created and click **Show Messages**. The event message should be visible in the **JMS Messages** list.

Configuring Your Environment to Support Event Notification

Prerequisites to Receive P6 Events

Configuring WebLogic JMS Servers to Receive P6 Events

You will need to install and configure WebLogic to receive P6 events as JMS messages from your cloud deployment. For supported versions, see *Tested Configurations*. For more information about how to install WebLogic, see http://www.oracle.com/technetwork/middleware/weblogic/documentation/index.html.

After you have installed WebLogic, you must configure your administration server, managed servers, and clusters.

Configuring P6 Application Settings

You must center you eventing and directory services information on the Eventing tab of the P6 Applications Settings page.

Submit a Service Request

After you have completed the configuration of your JMS servers and the Eventing page of the Application Settings, you must submit a Service Request in My Oracle Support to enable events.

Configuring your Environment

If you would like to receive notification when events occur, you must configure the JMS message queue and P6 to send the events in which you are interested.

To configure your environment to support notification:

1) Configure the WebLogic message queue:

   a. (Optional) Target the JMS server to a migratable target. See *Targeting the JMS Server to a Migratable Target* (on page 167)

   b. Determine if the WebLogic message queue will be on the same domain as P6.

      - See *Configuring the WebLogic Message Queue* (on page 170) if the queue and the application are on the same domain.

      - See *Sending Events to a Remote WebLogic JMS Server* (on page 171) if the queue and the application are on different domains.

   c. (Optional) Configure the message queue security policy. See *Configuring the Security Policy for the WebLogic Message Queue* (on page 173).

2) Configure the application settings in P6 to send event notification. See *Configuring Eventing in P6* (on page 168).

An event may be one of two types, a business object event or a special operation event.

Configuring Cross-Domain WebLogic Credentials

1) Log in to the WebLogic Administration Console with the following URL:
   ```
   http://<host_name>:<port>/console
   ```
2) In the **Change Center** pane, click **Lock & Edit**.
3) In the **Domain Structures** pane, click the name of the domain.
4) Open the **Security** tab and then open the **General** tab.
5) Expand **Advanced**.
6) In the **Credential** field, enter a password for the domain.

> **Notes:** By default, when a domain is created, a unique credential is generated for the domain. Creating a unique credential and sharing it with other domains establishes trust between those domains.

7) In the **Confirm Credential** field, enter the password that you entered in the **Credential** field.
8) Click **Save**.
9) Click **Activate Changes**.
10) Restart the WebLogic administration server and all managed servers.

Targeting the JMS Server to a Migratable Target

JMS-related services are hosted on individual server instances within a cluster and for these services, the WebLogic Server migration framework supports failure recovery with service migration, as opposed to failover. In a clustered server environment, a recommended best practice is to target the JMS server to a migratable target, so that a member server will not be a single point of failure. Therefore, the following prerequisite instruction is required if configuring The WebLogic Message Queue In A Cluster.

> **Note**: The instruction below assumes the WebLogic domain being configured has managed servers already created and assigned to a cluster parameter.

1) Configure the cluster migration Basis to Consensus:
   a. Log in into the WebLogic Administration console.
   b. In the Change Center of the Administration Console, click **Lock & Edit**.
   c. Navigate to the following location under the Domain Structure:
      Environment -> **Clusters** -> **ClusterName** -> **Migration**
   d. Locate the **Migration Basis** drop-down list and change its value to **Consensus**.
   e. Select **Save**.
   f. Select **Active Changes**.
2) Configure a migratable target for one of the managed servers in the cluster:
   a. In the Change Center of the Administration Console, click **Lock & Edit**.

b. In the **Domain Structure** tree, expand **Environment**, then select **Migratable Targets**.

c. On the Summary of Migratable Targets page, select the link for one of the managed servers in the list.

d. Select the migration tab:

e. In Service Migration Policy, select the **Auto-Migrate Exactly-Once Services** migration policy.

f. In **Constrained Candidate Servers**, move the user-preferred server and the additional managed servers in the cluster you want to support failure recovery from the **Available** column to the **Chosen** column.

g. Select **Save**.

h. In the Change Center of the Administration Console, click **Active Changes**.

i. Restart the Admin server and the managed servers in the cluster for changes to take effect.

Configuring Eventing in the Primavera P6 Administrator

Depending on administrative settings, events can be triggered when P6, P6 EPPM Web Services, or the P6 Integration API is used to update or create objects in the P6 database or when one of the special operations completes. When a business object change or special operation triggers an event, the P6 Event Notification system sends an event message to a user-configured message queue. If you are planning to use P6 Event Notification with P6 EPPM products, follow the steps below to configure the notification to work with your Java Messaging Service (JMS), the application server, and P6. Refer to the message queue vendor documentation.

Configuring Eventing in P6

If you want events to occur when business objects are created or updated, or when an operation is performed, you must configure Eventing page in the Application Settings of P6.

To configure the Eventing page:

1) Launch P6.

2) Click **Administration**.

3) On the Administration navigation bar, click **Application Settings**.

4) On the Application Settings page, click **Eventing**.

5) Click the **General** tab.

6) In the Eventing section:

a. Select **Eventing**.

b. Set additional settings as appropriate for your implementation. See *Eventing Settings* (on page 169) for details on available settings.

7) In the Directory Services section:

a. In the **Provider URL** field, enter the URL of the JNDI provider for the Connection Factory. For example:
   - If you are using a standalone server: t3://<Host_Name>:<Port>

- If you are using a cluster:
  t3://<Host_Name_1>:<Port_1>,<Host_Name_2>:<Port_2>

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

c. In the **Lookup Name** field, enter the lookup used to test the directory connection. This can be the JNDI name of the JMS connection factory created earlier or the JMS destination.

d. In the **Security Principal** field, enter the principal to connect to the JNDI provider. If you are using WebLogic, this is the name of a WebLogic user.

e. In the **Security Credentials** field, enter the credentials to connect to the JNDI provider. If you are using WebLogic, this is the password for the WebLogic user you entered in the **Security Principal** field.

f. In the **Security Level** field, enter the security level to use when authenticating to the directory service.

8) Click the **Configuration** tab.

9) In the Business Objects section:

a. Expand a business object type and configure the options to determine the type of notifications you will receive.

- Select or clear the **Create** option for an object to determine whether you will receive a notification when that object is created.
- Select or clear the **Update** option for an object to determine whether you will receive a notification when that object is updated.

10) In the Special Operations section:

a. Expand an operation type and select or clear the **Enabled** option for each operation to determine if it is enabled or disabled.

11) Click **Save and Close**.

Eventing Settings

Setting Name and Description	Default	Valid Ranges/Values
Eventing Select to enable the sending of events for P6, P6 EPPM Web Services, and P6 Integration API.	selected	—
Interval The length of time that the Event Notification System uses to determine how often it sends events to the message queue. Specifying a smaller time increases the frequency with which the Event Notification System reports event occurrences to the message queue.	5m	1s-10m

Setting Name and Description	Default	Valid Ranges/Values
Max Queue Size The amount of memory allocated to the queue for events. Once exceeded, events will be published immediately.	1000	10-5000
Show Costs Select to enable the display of cost fields in event notifications.	selected	—
JMS Connection Factory Specify the JNDI name of the JMS Connection Factory.	—	—
JMS Connection Name Specify the JNDI name of the queue or topic where events are published.	—	—
JMS Destination Security Select to use the user name and password specified when sending messages to JMS queue.	not selected	—
JMS Connection Username Specify the user name to use when sending events to the specified JMS destination specified.	—	—
JMS Connection Password Specify the password to use when sending events to the JMS Destination specified.	—	—

Configuring the WebLogic Message Queue

When an event is triggered, the P6 Event Notification system sends the event message to a message queue. To receive these notifications, you must first configure the message queue.

The following procedure indicates how to set up a WebLogic Java Messaging Service (JMS) message queue when the queue and P6 are on the same domain. See *Sending Events to a Remote WebLogic JMS Server* (on page 171) if the application and the queue are on different domains. For information about setting up other JMS-based message queues, see the vendor documentation.

To set up the WebLogic JMS message queue:

1) In either a new or existing WebLogic domain, launch the WebLogic **Administration Console** if it is not already open.

2) In the WebLogic **Administration Console**:

   a. Create a new JMS server and persistence store. See ***Creating a JMS Server and Persistence Store*** (on page 175).

   b. Create a JMS module. See ***Creating a JMS Module*** (on page 176).

   c. Create a new connection factory. See ***Creating a JMS Connection Factory*** (on page 176).

   d. Create a new queue or topic. See ***Creating a JMS Message Queue and Subdeployment*** (on page 178) to see how to create a new queue.

   > **Note**: Create a queue to deliver a message to a specific group of users. Create a topic to distribute a message amongst several users.

Sending Events to a Remote WebLogic JMS Server

When an event is triggered, the P6 Event Notification system sends the event message to a message queue. If you are using a remote JMS server, then you must configure the local and remote servers to receive these notifications.

The following procedure should be used when the queue is on a different domain than P6. For information about setting up other JMS-based servers, see the vendor documentation.

> **Note**: If you are configuring the WebLogic messaging queue in a cluster, ensure that you have targetted the JMS server to a migratable target.
> See: ***Targeting the JMS Server to a Migratable Target*** (on page 167)

To send events to a remote WebLogic JMS server:

1) Start the WebLogic **Configuration Wizard**.

2) In the wizard, create a WebLogic domain on the remote server to which you will be sending the events. See ***Creating a WebLogic Domain on a Remote or Local Server*** (on page 174).

   > ▪ **Note**: Rename the WebLogic administration server to a name that is different from the name you used to deploy the P6 application. For example, RemoteAdminServer.

3) Start the new server and launch the WebLogic **Administration Console**. The new server will act as the remote server.

4) In the WebLogic **Administration Console**:

   a. Create a WebLogic message queue.

      1. Create a new JMS server. See ***Creating a JMS Server and Persistence Store*** (on page 175).

      2. Create a JMS module. See ***Creating a JMS Module*** (on page 176).

3. Create a connection factory. See **Creating a JMS Connection Factory** (on page 176).
4. Create a new queue or topic. See **Creating a JMS Message Queue and Subdeployment** (on page 178) to see how to create a queue.

> **Note**: Create a queue to deliver a message to a specific group of users. Create a topic to distribute a message amongst several users.

   b. Configure the trust relationship on the remote server. See **Configuring a Trust Relationship** (on page 172).
5) Create a WebLogic domain on the local server from which the events will be sent. See **Creating a WebLogic Domain on a Remote or Local Server** (on page 174).
6) Start the local server and launch the WebLogic **Administration Console**.
7) In the WebLogic **Administration Console**:
   a. Target the JMS Server to a migratable target. See **Targeting the JMS Server to a Migratable Target** (on page 167)
   b. Create a new JMS server. See **Creating a JMS Server and Persistence Store** (on page 175).
   c. Create a JMS module. See **Creating a JMS Module** (on page 176).
   d. Create a foreign server. See **Creating a Foreign JMS Server** (on page 177).
   e. Configure the trust relationship on the local server. You must use the same credentials that were used on the remote server. See **Configuring a Trust Relationship** (on page 172).
8) Restart both Weblogic **Administration Console** servers (restart the domains, not the machines).
9) If it is not already installed, install P6 EPPM Web Services or P6 on the local server.
10) Launch P6 to configure message queue settings and event notification options. See **Configuring Eventing in the Primavera P6 Administrator** (on page 168). The values you enter in the **Directory Service** and **Eventing** sections of the P6 Application Settings Eventing page should be the the Local JNDI names of the Destination and the Connection Factory in the Foreign JMS Server.

Configuring a Trust Relationship

If you are sending events between different servers, you must establish a trust relationship between the local server, on which P6 is installed, and the remote server, on which you have setup the JMS message queue.

To configure a trust relationship:

1) If it is not already open, launch the WebLogic **Administration Console** on the server where you need to configure the trust relationship.
2) In the WebLogic **Administration Console**, click the name of your domain which is the top element in the **Domain Structure** pane.
3) On the **Settings** page, click the **Security** tab and then the **General** tab.
4) On the **General** tab, expand the **Advanced** section.

5) In the **Advanced** section:

   a. Enter and confirm credentials in the **Credential** and **Confirm Credential** fields.

   > **Note**: Make a note of the credentials you enter for the remote server; you must enter the same credentials for both servers.

   b. Click **Save**.

Configuring and Testing the WebLogic Message Queue Security

After you create a new user on the Users and Groups tab in Security Realms, you must change the Security Principal and the Security credentials listed under Directory Services in P6.

To configure and test the WebLogic message queue security:

1) Log in to P6 as an administrator.
2) From the **Administer** menu, select **Applications Settings**.
3) On the **Application Settings** page, click **Eventing**.
4) Under **Directory Services**, complete the following:

   a. Enter the new username in the **Security Principal** field.
   b. Enter the new password in the **Security Credentials** field.
   c. Enter the provider URL in the **Provider URL** field.
   d. Enter the initial context factory name in the **Initial Context Factory** field.
   e. Enter the lookup name in the **Lookup Name** field.

   > **Note**: The user name and password were set in the ***Configuring the Security Policy for the WebLogic Message Queue*** (on page 173) topic.

   f. Click Test Connection.
   g. Repeat the steps above with the original username and password to ensure that they no longer work.
5) Under Eventing,enter your eventing settings and test the connection. See ***Configuring Eventing in P6*** (on page 168).

Configuring the Security Policy for the WebLogic Message Queue

You can configure the WebLogic security policy to allow only specific users, roles, or groups to access the queue. The following is an example a security policy configured for one user. If you need more information, refer to the WebLogic documentation.

To configure the WebLogic message queue security policy for one user:

1) Launch the WebLogic **Administration console**.
2) In the WebLogic **Administration console**, click **Security Realms** in the **Domain Structure** pane.
3) On the **Summary of Security Realms** page, click the security realm you are using in the **Name** column under **Realms**.

4) On the **Settings** page for the realm, click the **Users and Groups** tab and then click the **Users** tab.

5) On the **Users** tab, under **Users** click **New**.

6) On the **Create a New User** page, enter a name and password in the appropriate fields and click **OK**.

> **Note**: Make a note of the name and password as they will be needed in the ***Configuring and Testing the WebLogic Message Queue Security*** (on page 173) topic.

7) On the **Settings** page for the user, click the **Roles and Policies** tab and then click the **Realm Policies** tab.

8) On the **Realm Policies** tab, under **Policies** expand **JMS** then expand the module you created for the remote server and click the queue you created for the remote server.

9) On the **Settings** page for the queue, click the **Security** tab and then click the **Policies** tab.

10) On the **Policies** tab:

   a. In the **Policy Conditions** section, click **Add Conditions**.

   b. Under **Choose a Predicate**, select **User** from the **Predicate** list and click **Next**.

   c. Under **Edit Arguments**:

     1. Enter the user name for the user you just created in the **User Argument Name** field and click **Add**. You can now use this user in P6.

     2. Click **Finish**.

11) On the **Settings** page for the queue, click **Save**.

12) Log in to P6 as an administrator.

13) From the **Administer** menu, select **Applications Settings**.

14) On the **Application Settings** page, click **Eventing**.

15) Enter information in the required fields. For more information about information that is required for each field, refer to ***Configuring Eventing in P6*** (on page 168).

16) Change and test the **Directory Services** user name and password. See ***Configuring and Testing the WebLogic Message Queue Security*** (on page 173).

Creating a WebLogic Domain on a Remote or Local Server

Create a WebLogic domain on a remote or local server to define how the server and domain interact.

To create a WebLogic domain:

1) Start the Weblogic **Configuration Wizard** on the local or remote server.

2) In the **Welcome** window, select **Create a new WebLogic domain** and click **Next**.

3) In the **Select Domain Source** window, click **Next** to accept the default selections.

4) In the **Specify Domain Name and Location** window:

   a. Enter the domain name. If you are creating a domain on both a local and remote server, give the domains a different name.

   b. Select the domain location.

c. Click **Next**.

5) In the **Configure Administrator User name and Password** window, enter the user name and password information and click **Next**.

> **Note**: Make a note of the name and password, you will need this information for the **JNDI Properties Credential** fields and the **JNDI Properties** box in the *Creating a Foreign JMS Server* (on page 177) topic.

6) In the **Configure Server Start Mode and JDK** window:
   a. Select **Production Mode** in the left pane.
   b. Select an appropriate JDK in the right pane.
   c. Click **Next**.

7) In the **Select Optional Configuration** window, click **Next**.

8) In the **Configuration Summary** window, click **Create**.

9) In the **Creating Domain** window, select **Start Admin Server** and click **Done**.

Creating a JMS Server and Persistence Store

Create a JMS server to hold queues and topics.

To create a JMS server and persistence store:

1) If it is not already open, launch the WebLogic **Administration Console** on the remote or local server.

2) In the WebLogic **Administration Console**, expand **Services**/**Messaging** and click **JMS Servers** in the **Domain Structure** pane.

3) On the **Summary of JMS Servers** page, click **New**.

4) On the **Create a New JMS Server** page:
   a. Under **JMS Server Properties**:
      1. Enter a name in the **Name** field.
      2. Click **Create a New Store**.
   b. Under **Select a store type**, select **File Store** from the **Type** list and click **Next**.
   c. Under **File Store Properties**:
      1. Enter a name in the **Name** field.
      2. Select a server instance from the **Target** list.

      > **Note**:   If you are configuring the WebLogic Message Queue in a cluster, select the migratable target you configured earlier.

      3. Specify a location for the file store in the **Directory** field.

         ▪ This location must already exist on your machine and you must have read/write rights to this folder. No error messages appear on the WebLogic console if the filestore is not configured correctly.

      4. Click **OK**.

    d. Under **JMS Server Properties**, select the new store from the **Persistent Store** list and click **Next**.

    e. Under **Select Targets**:

- If you are deploying to a standalone server, select the administration server (for example, AdminServer) as the target from the **Target** list and click **Finish**.
- If you are deploying to a cluster, select the migratable target configured earlier.

Creating a JMS Module

Create a JMS module to manage and configure resources.

To create a JMS module:

1) If it is not already open, launch the WebLogic **Administration Console** on the remote or local server.
2) In the WebLogic **Administration Console**, expand **Services**/**Messaging** and click **JMS Modules** in the **Domain Structure** pane.
3) On the **JMS Modules** page, click **New**.
4) On the **Create JMS System Module** page:

    a. Under **The following properties will be used to identify your new module**, enter a name in the **Name** field and click **Next**.

> **Note**: Make a note of this name, you will need to know which module to expand in the *Configuring the Security Policy for the WebLogic Message Queue* (on page 173) topic.

    b. Under **The following properties will be used to target your new JMS system module**, select a target server in the **Servers** box and click **Next**.

> **Note**: If you are deploying to a cluster, select the cluster from the targets list.

    c. Under **Add resources to this JMS system module**, select the **Would you like to add resources to this JMS system module** option and click **Finish**.

Creating a JMS Connection Factory

Create a connection factory to enable connections between your JMS elements.

To create a JMS connection factory:

1) Log in to the WebLogic **Administration Console**.
2) In the WebLogic **Administration Console**, expand **Services**/**Messaging** and click **JMS Modules** in the **Domain Structure** pane.
3) On the **JMS Modules** page, select the module to which you want to add the connection factory.
4) On the **Settings** page, click the **Configuration** tab and under **Summary of Resources** click **New**.

5) On the **Create a New JMS System Module Resource** page:

    a. Under **Choose the type of resource you want to create**, select the **Connection Factory** option and click **Next**.

    b. Under **Connection Factory Properties**:

        1. Enter a name for the connection factory in the **Name** field.

        2. Enter a name in the **JNDI** field.

> **Note**: Make note of the JNDI name. You will need to enter this name in the **JMS Connection Factory** field of P6 Application Settings Eventing page. If you are using a remote server, you will need to enter this name in the **Remote JNDI Name** field on the **Connection Factories** tab in the *Creating a Foreign JMS Server* (on page 177) topic.

        3. Click **Next**.

    c. Under **The following properties will be used to target your new JMS system module resource**, ensure the correct server is targeted and click **Finish**.

> **Note**: If you are deploying to a cluster, the cluster should be selected as the target.

Creating a Foreign JMS Server

Create a foreign JMS server to establish a link between the WebLogic domains.

To create a foreign JMS server:

1) If it is not already open, launch the WebLogic **Administration Console**.

2) In the WebLogic **Administration Console**, expand **Services**/**Messaging** and click **JMS Modules** in the **Domain Structure** pane.

3) On the **JMS Modules** page, select the module you created for the remote server.

4) On the **Settings** page, click the **Configuration** tab and under **Summary of Resources** click **New**.

5) On the **Create a New JMS System Module Resource** page:

    a. Under **Choose the type of resource you want to create**, select the **Foreign Server** option and click **Next**.

    b. Under **Foreign Server Properties**, enter a name in the **Name** field and click **Next**.

    c. Under **The following properties will be used to target your new JMS system module resource**, ensure the correct server is targeted and click **Finish**.

> **Note**: If you are deploying to a cluster, the cluster should be selected as the target.

6) On the **Configuration** tab of the **Settings** page, click the name of the new foreign server.

7) On the **Settings** page, click the **Configuration** tab and then click the **General** tab.

8) On the **General** tab:

a. Enter the URL of the remote server created from step 4 of section **Sending Events to a Remote WebLogic JMS Server** in the **JNDI Connection URL** field.

For example:

- If you are using a standalone server: t3://<hostname>:7001.
- If you are using a cluster: t3://<hostname>:7003,<hostname>:7004.

b. Enter the password that you used to log on to the remote WebLogic server in the **JNDI Properties Credential** field.

c. Reenter this password in the **Confirm JNDI Properties Credential** field.

d. Enter *java.naming.security.principal*=<name> in the **JNDI Properties** box, where *name* is the user name you used to log on to the remote WebLogic server.

e. Click **Save**.

9) On the **Configurations** tab, click the **Destinations** tab and click **New** under **Foreign Destinations**.

10) On the **Create a New Foreign JMS Destination** page:

a. Enter a name in the **Name** field.

b. Enter a JNDI name in the Local JNDI Name field. Ensure that the Local JNDI name is different from the JNDI name that you had previously assigned to the message queue for the remote server.

c. Enter the JNDI name that you assigned to the message queue for the remote server in the **Remote JNDI Name** field.

d. Click **OK**.

11) On the **Configurations** tab, click the **Connection Factories** tab and click **New** under **Foreign Connection Factories**.

12) On the **Create a New Foreign JMS Connection Factory** page:

a. Enter a name in the **Name** field.

b. Enter a JNDI name in the **Local JNDI Name** field. Ensure that the Local JNDI name is different from the JNDI name that you had previously assigned to the connection factory for the remote server.

c. Enter the JNDI name that you assigned to the connection factory for the remote server in the **Remote JNDI Name** field.

d. Click **OK**.

Creating a JMS Message Queue and Subdeployment

Create a message queue to act as a receptacle for event messages sent from P6.

To create a JMS message queue and subdeployment:

1) Log in to the WebLogic **Administration Console**.

2) In the WebLogic **Administration Console**, expand **Services**/**Messaging** and click **JMS Modules** in the **Domain Structure** pane.

3) On the **JMS Modules** page, select the module to which you want to add the queue.

4) On the **Settings** page, click the **Configuration** tab.

5) On the **Configuration** tab under **Summary of Resources**, click **New**.

6) On the **Create a New JMS System Module Resource** page:

   a. Under **Choose the type of resource you want to create**, select the **Queue** option and click **Next**.

   b. Under **JMS Destination Properties**:

      1. Enter a name for the queue in the **Name** field.

      2. Enter a name in the **JNDI** field.

         Note: Make note of the JNDI name. You will need to enter this name in the **JMS Destination Name** field of the P6 Application Settings Eventing page. If you are using a remote server, you will need to enter this name in the **Remote JNDI Name** field on the **Destinations** tab in the Creating a Foreign JMS Server topic.

      3. Click **Next**.

   c. Under **The following properties will be used to target your new JMS system module resource**, click **Create a New Subdeployment**.

7) On the **Create a New Subdeployment** page, enter a name in the **Subdeployment Name** field and click **OK**.

8) On the **Create a New JMS System Module Resource** page:

   a. Select the new subdeployment from the **Subdeployments** list.

   b. Select the JMS server you created when creating the Persistence Store as the target from the **JMS Servers** box.

   c. Click **Finish**.

Testing Event Notification

Test event notification to ensure event messages are sent when an event occurs.

To test event notification:

1) If it is not already installed, install P6. See the *P6 EPPM Installation and Configuration Guide*.

      Note: If you are using more than one server, install P6 on the local server.

2) Configure WebLogic for eventing:

   ▸ See *Configuring the WebLogic Message Queue* (on page 170) if the queue and the application are on the same domain.

   ▸ See *Sending Events to a Remote WebLogic JMS Server* (on page 171) if the queue and the application are on different servers.

3) Open P6 and create a project.

4) In P6:

   a. Add one or more activities to the project.

   b. Summarize the project to test if an event is generated.

5) Launch the WebLogic **Administration Console** to verify that the event is generated and sent to the queue.

6) In the WebLogic **Administration Console**, expand **Services/Messaging** and click **JMS Modules** in the **Domain Structure** pane.

7) On the **JMS Modules** page, click the module you created for the remote server.

8) On the **Settings** page for the module, click the queue you created for the remote server.

9) On the **Settings** page for the queue, click the **Monitoring** tab.

10) On the **Monitoring** tab, select the option for the remote server destination you created and click **Show Messages**. The event message should be visible in the **JMS Messages** list.

Oracle BPM Setup Tasks

The Oracle Business Process Management (BPM) Suite provides an integrated environment for developing, administering, and using business applications centered around business processes. BPM supports BPM and Business Process Execution Language (BPEL) standards from modeling and implementation to run-time and monitoring.

P6 integrates with BPM which lets you initiate and manage workflows. You can use a sample project initiation workflow for P6 sample database.

You can expand your investment in BPM to include workflows representing more stages of your application, program, project, or product development life cycle from design-time and implementation to run-time and application management.

The Oracle BPM Suite enables you to:

▸ Create and customize business processes, models, and standards using pre-defined components for web-based applications.
▸ Collaborate between process developers and process analysts.
▸ Expand business process management to include flexible, unstructured processes.
▸ Integrate your applications with Web Services.
▸ Add dynamic tasks and support approval routing using declarative patterns and rules-driven flow determination.

> Unify different stages of your development life cycle by addressing end-to-end requirements for developing process-based applications. Oracle BPM unifies the design, implementation, run time, and monitoring stages based on a Service-Oriented Architecture (SOA) infrastructure. This allows different personas to participate through all stages of the workflow life-cycle.

Assigning the TestConfig Role to Users

To use this workflow, you need to assign a BPM role for the user to initiate the test and receive the confirmation the test was successful.

To assign the role:

1) Login to the BPM Workspace as a user with administrative rights.
2) Click **Administration** on the top right toolbar.
3) On the **Organization Roles** list, select **P6ConfigValidator.TestConfig**.
4) On the **Details** pane, make one or more BPM users or user groups a member of the **TestConfig** role. The BPM users or user groups assigned to the TestConfig role must match a P6 username for the workflow to be visible from P6.
5) Click **Apply** to save these changes.

BPM Workflows in P6

The following sections detail information about workflows and how to work with them.

About Workflows

A workflow is an automated business process that routes information and tasks between participants according to a defined set of procedures or rules designed to coordinate a specific business goal. Workflows are primarily characterized by their level of procedural automation involving one or more dynamic related series of processes, and their combination of human and machine-based tasks involving interaction with software and systems.

The following industry segments, marked by relatively high office labor costs and transaction volume, have demonstrated successful workflow implementations:

- Insurance
- Banking
- Legal
- General & Administrative
- Design
- Engineering
- Manufacturing

Business process modeling and workflow automation allow transactions to be conducted electronically without the need for manual intervention such as conducting certain validations or re-keying data. When workflow IT systems are processing repetitive, mundane, and often error-prone work, talented staff resources become available to handle activities that add real value to the enterprise.

Working with Workflows in P6 (On Premises only)

You can use workflows to route business processes such as project initiation requests through your organization to gather information and visibility before a go/no go decision is made. Template data, routing designators, and approval rules can be set for each stage of a workflow. To illustrate these options, suppose we have a workflow involving five key approval managers. You can define the workflow such that all five must approve and even specify a particular sequence, if any. A much more relaxed approval rule would require only one out of the five to approve. The following are just some example of how you can use workflows.

Workflows are defined, deployed, and configured in BPM where your workflow designer defines the workflow tasks involved and assigns them to specific users, roles, or groups. Then, in P6, a business need kicks off an instance of the workflow and its required tasks are automatically routed to their users, roles, or groups.

When a specific user or any user assigned to a role or group logs into P6, the Workflows portlet on their dashboard will display their relevant tasks at this stage of the workflow, as authenticated by BPM. As a workflow participant, you can select a task in the workflow instance and claim ownership for it. This means you will be responsible for performing the task. The application refreshes itself to show only the actions permitted for this stage of the workflow for you (the currently logged in user).

After your administrator sets up BPM for P6, they can configure a dashboard to display the Workflows portlet. The following list represents a list of the key Workflow elements that you can observe in the portlet depending on your configuration.

- ▸ **Action Required Tab**: This tab shows the tasks that are important to you (the currently logged in user).
- ▸ **My Workflows Tab**: This tab enables you to view all workflows according to role and status filters you can set.
- ▸ **Initiate a Workflow**: Click Initiate a Workflow to start a new instance of a workflow based on a predesigned template.
- ▸ **BPM Workspace**: Use the BPM Workspace to update the progress of tasks, initiate a change, request a project, and retrieve project information. You are also able to apply a bulk action to multiple work items.

> **Note**: If SSO authentication is not configured with BPM, you must log into BPM in the resulting window, close that window, and then return to P6 and click _ View Form again. This procedure is required whenever your BPM session expires.

- ▸ **Sample Workflow**: A basic workflow image with tasks for a business user, two project offices, and a project manager.
- ▸ **Workflow History**: View a chronological sequence of all the previous actions, users, and stages in the current workflow.

Copyright

Oracle Primavera P6 EPPM Application Administration Guide