HP Project and Portfolio Management Center

Software Version: 7.1

Security Model Guide and Reference

Document Release Date: March 2007
Software Release Date: March 2007

Legal Notices

Documentation Updates

This manual's title page contains the following identifying information:

- Software version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates, or to verify that you are using the most recent edition of a document, go to: http://ovweb.external.hp.com/lpe/doc_serv/.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Mercury Product Support

You can obtain support information for products formerly produced by Mercury as follows:

- If you work with an HP Software Services Integrator (SVI) partner (www.hp.com/managementsoftware/svi_partner_list), contact your SVI agent.
- If you have an active HP Software support contract, visit the HP Software Support site and use the Self-Solve Knowledge Search to find answers to technical questions.
- For the latest information about support processes and tools available for products formerly produced by Mercury, we encourage you to visit the HP-Mercury Software Support web site at: support.mercury.com.
- Contact your HP Sales Representative if you have additional questions.

HP Software Support

You can visit the HP Software Support web site at www.hp.com/managementsoftware/services.

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To find more information about access levels, go to: www.hp.com/managementsoftware/access_level.

To register for an HP Passport ID, go to: www.managementsoftware.hp.com/passport-registration.html.

Table of Contents

List of Figures

List of Tables

1 Getting Started with the PPM Center Security Model

In This Chapter:

Introduction to the HP Project and Portfolio Management Center Security Model

Businesses must often control access to information and business processes. This is done to protect sensitive data, such as employee salaries, or to simplify business processes by hiding data that is irrelevant to the user. HP Project and Portfolio Management Center (PPM Center) includes a set of features to help control data and limit the following:

- Who can access specific windows and pages
- Who can view or edit specific data
- Data displayed in restricted fields and on pages
- Who can view, create, edit, or process PPM Center entities (requests, packages, projects, portfolios, and so on)
- Who can view, create, or edit configuration entities (workflow, request types, object types, security groups, and so on)
- Who can change security settings

This document presents an overview of the PPM Center data security model and provides instructions on how you can control access to PPM Center entities using a combination of licenses, access grants, and other security-related features.

Security-Related Features in PPM Center

To control data and process security and secure the PPM Center system, you use a combination of the following features:

- **Licenses**

  After you assign a license to a user, you can grant that user access to a set of PPM Center user interface and functionality. Licenses determine available behavior but must be used in conjunction with access grants to enable specific fields and functions. For example, a user with a Demand Management license, but with no access grants, can log on to the system, but cannot create requests.

  Chapter 3, *Managing HP Project and Portfolio Management Center Licenses,* on page 39 provides instructions on how to assign licenses to individual users or to groups of users. Appendix B, *License Types,* on page 153 provides information about the specific access that each

license provides. Appendix C, *Licenses and User Roles,* on page 157 contains detailed information about product licenses.

- **Access grants**

  Access grants are linked to users through security groups. They determine the windows and functions in which users can view information or perform actions. Access grants also provide levels of control over specific entities and fields. Chapter 2, *Users and Security Groups,* on page 19 contains information on how to create users and give them access to information and functionality in PPM Center. The tables in Appendix A, *Access Grants,* on page 137 provide information about all of the access grants used to control user access to specific features and parts of the PPM Center user interface.

- **Entity-level restrictions**

  Settings on the entity that specify who can create, edit, process, and delete PPM Center entities (such as requests, packages, or projects). Entity-level restrictions also let you determine which request types and object types can be used with certain workflows. These restrictions are often set in the configuration entities (workflows, request types, object types, and so on).

- **Field-level restrictions**

  For each custom field that you define in the PPM Center, you can configure when it is visible or editable. For some fields, you can also specify who can view or edit the field.

- **Configuration-level restrictions**

  To specify who can modify configuration entities in the system, you can use ownership group settings. For example, you can control who can edit existing workflows. This ensures that only qualified users can modify your PPM Center–controlled processes. For information about the security settings and permissions required to configure PPM Center, see Chapter 10, *Configuration Security,* on page 125.

  HP recommends that you maintain two levels of system administrators for your organization. Chapter 11, *Service Provider Functionality,* on page 131 contains information about how to create administrator-level users whose records cannot be modified by other users.

Providing Access to the PPM Center Applications

The process for configuring security for individual PPM Center applications can vary:

- For information about the security settings required to create, process, and manage requests in HP Demand Management, see Chapter 4, *Request Security,* on page 47.
- For information about the security settings required to create, process, and manage packages in HP Deployment Management, see Chapter 5, *Package Security,* on page 75.
- For information about the security settings required to create, process, and manage projects in HP Project Management, see Chapter 6, *Project and Task Security,* on page 83.
- For details on the security settings related to HP Resource Management, see Chapter 7, *Resource Management Security,* on page 95.
- For details on the security settings related to HP Financial Management, see Chapter 8, *Cost and Budget Data Security,* on page 109.
- All PPM Center user and configuration guides contain some security-related information about the product that the document describes.
- For information about the security settings that users must have to access and use the PPM Dashboard, see Chapter 9, *PPM Dashboard Security,* on page 119.

Related Documents

For more information related to this document, see the following user and configuration guides:

- *HP Demand Management User's Guide*
- *HP Demand Management Configuration Guide*
- *HP Deployment Management User's Guide*
- *HP Deployment Management Configuration Guide*
- *HP Project Management User's Guide*
- *HP Project Management Configuration Guide*
- *HP Program Management User's Guide*
- *HP Program Management Configuration Guide*
- *HP Portfolio Management User's Guide*
- *HP Portfolio Management Configuration Guide*
- *HP Resource Management User's Guide*
- *HP Time Management User's Guide*
- *HP Time Management Configuration Guide*
- *Commands, Tokens, and Validations Guide and Reference*
- *HP-Supplied Entities Guide* (includes descriptions of all PPM Center portlets, request types, and workflows)

2 Users and Security Groups

In This Chapter:

Defining PPM Center Users

To create and define PPM Center users, you use the PPM Workbench. This section provides the detailed steps to create users.

Creating Users

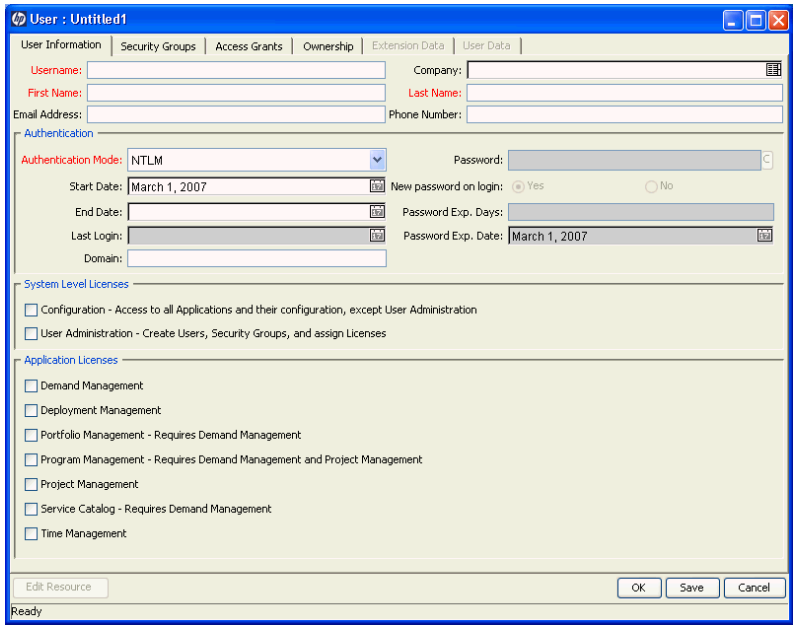
To create a PPM Center user:

1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Sys Admin > Users.**

   The User Workbench window opens.
4. Click **New.**

   The User window opens.



5. In the **Username, First Name,** and **Last Name** fields, type the required names.

You must specify a user name that is unique in PPM Center.

6. You can enter information in the optional **Email Address, Company,** and **Phone Number** fields.

   For a description of a control on the **User Information** tab, see *Table 2-1* on page 22.

7. In the **Authentication** section, do the following:

   a. In the **Authentication Mode** list, select a user authentication method for the new user.

      If you select **PPM,** then PPM Center authenticates the user based on its internal user database. If you select a different mode, PPM Center authenticates the user based on the enterprise directory database server. To change the behavior of the **Authentication Mode** list, specify a different value for the `AUTHENTICATION_MODE` server configuration parameter.

      For information about the `AUTHENTICATION_MODE` server configuration parameter, see the *System Administration Guide and Reference.*

   b. In the **Password** field, enter a PPM Center password for the user.

      This password is encrypted in the user interface and in the database.

   c. If you want the user to create a password the first time he or she logs on to PPM Center, next to **New password on login,** leave **Yes** selected. Otherwise, select **No.**

   d. To specify the number of days the password is to remain valid, in the **Password Exp. Days** field, type the number of days that the user has to change the password.

      After you type a value, the **Password Exp. Date** field displays the password expiration date.

8. To assign the user a system-level license, under **System Level Licenses,** do one or both of the following:

   - To give the user access to all product functionality available through the PPM Workbench and standard interfaces in PPM Center (except for user and security group administration), select the **Configuration - Access to all Applications and their configuration, except User Administration** option.

- To give the user permission to administer the users and security groups for all HP products licensed at your site, select the **User Administration - Create Users, Security Groups, and assign Licenses** option.

To assign licenses to multiple users at one time, use the License Workbench. For details on how to do this, see *Assigning Licenses to Multiple Users in the License Workbench* on page 42.

9. If, under **System Level Licenses,** you did not select the **Configuration - Access to all applications and their configuration, except User Administration** option, then under **Application Licenses,** select the checkboxes for the products to which you want to give the user access.

You can only assign licenses that your company has purchased. If you do not have licenses for a given PPM Center product, then that license field is unavailable.

HP Deployment Management Extension licenses are issued on a site-wide basis and are, therefore, not included as an option in the User window.

10. Click the **Security Groups** tab, and then link the user to the security groups that provide functional roles and access grants required.

    For information about how to link the user to security groups, see *Linking Users to Security Groups* on page 25.

11. Click the **Ownership** tab, and then select the users or groups that can edit, copy, or remove this user.

    For information about how to select the users or security groups that can configure a user, see *Setting Ownership for Configuration Entities* on page 126.

12. Click **OK.**

    The new user can now log on to PPM Center.

Table 2-1. User window: Fields on the User Information tab (page 1 of 3)

Field Name	Description
Username	Unique user account name to be used to log on to PPM Center.
Company	The company for which the user works. The values in this list are set by the following validation: CRT - Company.
First Name	The user's first name.
Last Name	The user's last name.
Email Address	The user's email address in the format `name@domain.com`. This address is referenced elsewhere in the application.

Table 2-1. User window: Fields on the User Information tab (page 2 of 3)

Field Name	Description
Phone Number	The user's phone number.
Authentication Mode	A list of the available authentication methods. Possible values are **PPM, LDAP, NTLM,** and **SITEMINDER.** If you select **PPM,** then authentication is performed using the internal user database of PPM Center. If you select another authentication mode, authentication is performed using the enterprise directory database server. For details, see the *Open Interface Guide and Reference.*
Start Date	The date on which a user account is to be activated.
End Date	The date on which a user account expires. You can leave this field empty.
Last Login	The date of a user's last system logon. This date is deleted based on the `DAYS_TO_KEEP_LOGON_ATTEMPT_ROWS` parameter in the `server.conf` file. The default value for this parameter is 14 days. If there is no value in the **Last Login** field, the user has not logged in for at least 14 days (assuming the parameter default value has not changed). For detailed information about server configuration parameters, see the *System Administration Guide and Reference.*
Domain	Used only if you use NTLM authentication. Set the value for this in the `<PPM_Home>/integration/ntlm/ntlm.conf` file.
Password	The user password. Administrators can set restrictions on the password format: minimum length, required special characters, and so on. These restrictions are specified in the `server.conf` file on the PPM Server. For detailed information about server configuration parameters, see the *System Administration Guide and Reference.*
New password on login	Setting to determine whether to ask a user to enter a new password the next time they log on.
Password Exp. Days	The number of days before a user password expires. The first time a user logs on after the password expiration date, he is prompted to create a new password.
Password Exp. Date	The date on which a password expires. The value in this field is calculated based on the Password Expiration Days value or the Ask New Password On Logon attribute.
Configuration	Select this option to give the user access to all functionality for the products licensed at the site, including configuration interfaces for all PPM Center entities (such as object types and request types) except users and security groups.

Table 2-1. User window: Fields on the User Information tab (page 3 of 3)

Field Name	Description
User Administration	The User Administrator license is required to configure user accounts and security groups.
Deployment Management	The Deployment Management license provides access to all product functionality available through the PPM Workbench interface and additional access to advanced standard interface functions. If this checkbox is not selected, the user cannot see the Deployment Management screen group or menus.
Demand Management	The Demand Management license provides access to all product functionality. If this checkbox is not selected, the user cannot see the Demand Management screen group or menus.
Portfolio Management	The Portfolio Management license provides access to Portfolio Management functionality, and must be used in conjunction with a Demand Management license. Users who do not have this selected cannot see the related menus and can not access the functionality.
Program Management	The Program Management license gives a user access to Program Management functions. This license must be used in conjunction with Demand Management and Project Management licenses. Users who do not have this license cannot see the related menus or access the functionality.
Project Management	The Project Management license provides users with access to work planning functions such as work plans, baselines, and earned value, as well as functions like project types and work plan templates. Although high-level project information is accessible with either a Project Management or Demand Management license, core project management functions such as project type management and work plan management are only available to users with a Project Management license.
Time Management	The Time Management license gives users access to Time Management functions in PPM Center. If this is not selected, the user cannot see the Time Management menus or access the functionality. Users for whom timesheets are to be submitted must also have this license.
Edit Resource	Each user has associated resource settings such as Title, Direct Manager, and Capacity. Click this button to view or edit these resource settings.

If your organization has many users, you can import user information from other databases into interface tables, and then directly into the PPM Center database. You can also import users from an LDAP server through the interface tables. For information on how to import users from an LDAP server, see the *Open Interface Guide and Reference.*

Linking Users to Security Groups

To link users to security groups, you can use the **Security Groups** tab in the User window or use an organization model defined in PPM Center. This section provides the steps you perform from the **Security Groups** tab.

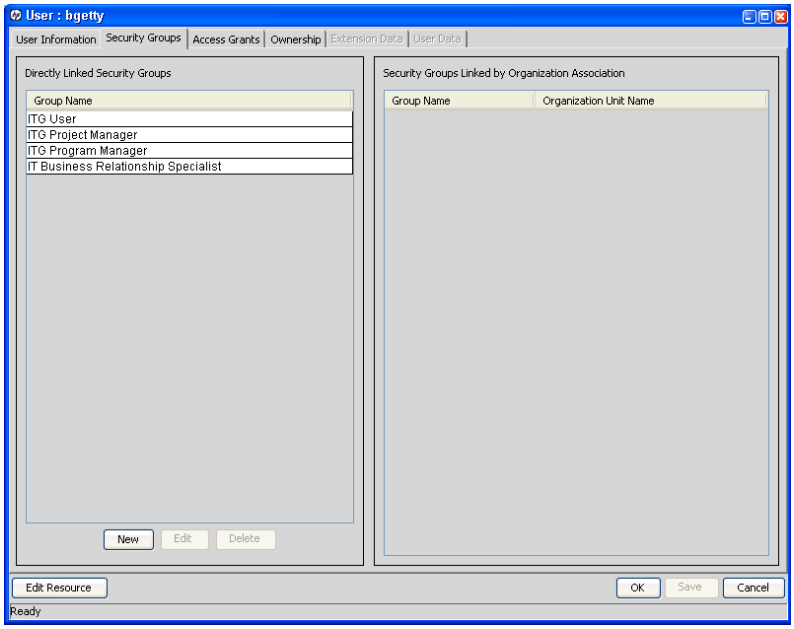
To link a user to a security group:

1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Sys Admin > Users.**

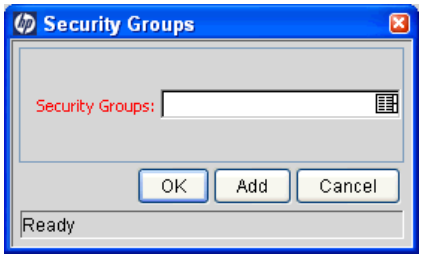
   The User Workbench opens.
4. Use the **Query** tab to locate the user you want to add to security groups.
5. On the **Results** tab, double-click the row that displays the user name.

   The User window opens to the record for the user.
6. Click the **Security Groups** tab.



7. Click **New.**

   The Security Groups window opens.



8. In the **Security Groups** field, click the auto-complete button.

   The Validate window opens.

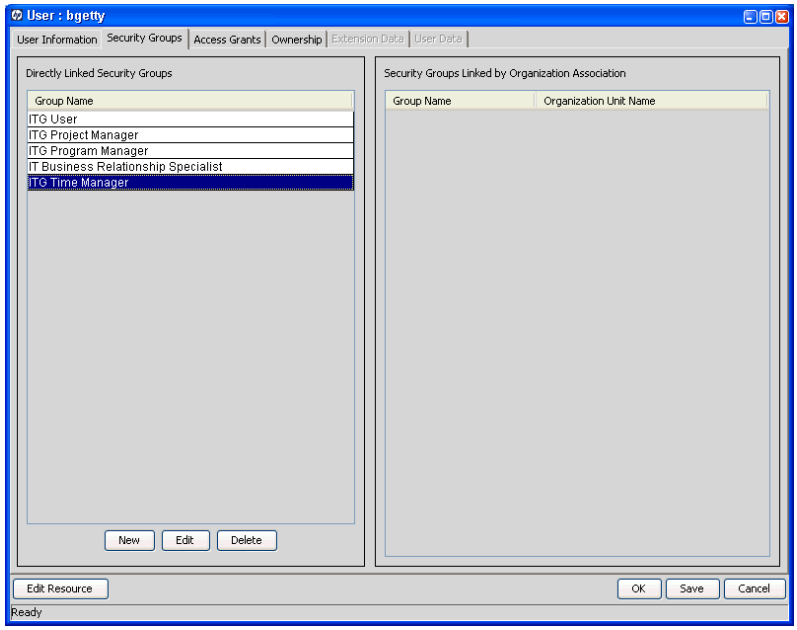
9. Under **Available,** in the **Security Group** column, select one or more security groups to link to the user.

   You can use the **`Ctrl`** or **`Shift`** key to select multiple groups.

10. To add these groups to the **Selected** list, click the right-pointing arrow.

11. Click **OK.**

12. In the Security Groups window, click **OK.**



In the User window, the **Directly Linked Security Groups** field lists the selected security groups, which are now linked to the user.

A user associated with an organization unit (defined in the HP Resource Management functionality) may inherit security group associations. The **Security Groups Linked by Organization Association** field lists these security groups, if any are linked (indirectly) to the selected user.

For more information, see the *HP Resource Management User's Guide.*

13. Click **OK.**

Configuring Resource Information

A resource is something or someone assigned to work. Resources can include employees, contractors, managers, consulting groups, supplies, or any other category your organization requires. A user is considered a resource in PPM Center. You can capture user information specific to the user's roles and skills as a resource, such as "database administrator" or "programmer."

Entering resource information such as this for each user is optional. For information about how to configure resource information, see the *HP Resource Management User's Guide.*

The hourly rate (chargeback or billed labor cost) associated with the resource or skill is defined on the Cost Rate page.

Workload capacity, represented as the percentage of the working day that a resource is available for planned work items, is defined through the resources's association with different resource pools.

Importing Users from a Database or LDAP Server

If your organization has many users, you can use the PPM Center open interface to create user accounts. This API uses interface tables within the PPM Center database instance. Data added to these interface tables is validated and eventually imported into standard database tables to generate users who you can then process normally within PPM Center. You can also import user information from LDAP servers.

For detailed information, see the *Open Interface Guide and Reference,* which provides an overview of relevant database tables and complete instructions on how to import users.

Creating Security Groups

To control access to specific sections of the PPM Center user interface and its functionality, you create security groups, specify their members, and then configure their access grants.

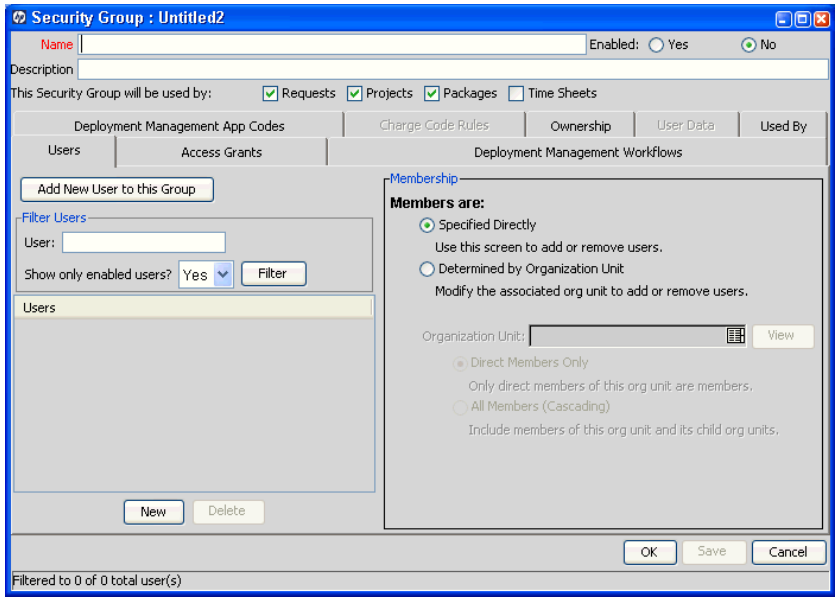
To create a security group:

1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Sys Admin > Security Groups.**

   The Security Group Workbench window opens.
4. Click **New Security Group.**

   The Security Group window opens.



5. In the **Name** field, type a name for the group.
6. To enable the new group, next to **Enabled,** click **Yes.**
7. In the **Description** field, you can type a description of the group.

   To add members to the security group, you can either select a list of users or associate the group with an organization unit that has been defined in PPM Center.

8. To make this group selectable, do one of the following:
   - To select group members directly:
     i. On the **Users** tab, click **Add New User to this Group.**
     ii. The Users dialog box opens.
     iii. In the **Users** field, click the selector button.
     iv. The Validate window opens.
     v. In the **Available** section, select the users to add to the security group.
     vi. Click **OK.**
     vii. In the Users dialog box, click **OK.**
   - Alternatively, to add users based on their organization unit associations:
     i. In the **Membership** section of the **Users** tab, under **Members are,** select **Determined by Organization Unit.**
     ii. In the **Organization Unit** field, enter the name of an organizational unit.
     iii. If you want to associate just the members of this organization unit with the new security group, leave **Direct Members Only** selected. If you also want to include members of the child organization units of the selected unit, click **All Members (Cascading).**
9. To specify user interface and feature access, click the **Access Grants** tab, and then select the access grants to assign to the security group.

For a complete list of access grants, see Appendix A, *Access Grants,* on page 137.

10. If the security group is to be used in deployment, do the following:
    a. Click the **Deployment Management Workflows** tab, and then specify the workflows that members of this security group can use to deploy changes.

b. On the **Deployment Management App Codes** tab, restrict the security group from using specific application codes in creating package lines.

   This restricts the applications through which each user can process objects.

To simplify the maintenance of a security model around processes, consider creating and maintaining the following two types of security groups. (As new users are added to the system, you can grant them the required screen and function access and associated with specific workflows.)

- Security groups to control who can act on specific workflow steps (a list of users with no special access grants)
- Security groups to control who can access a particular screen or function (a list of users and required access grants)

Creating a Security Group by Specifying a List of Users

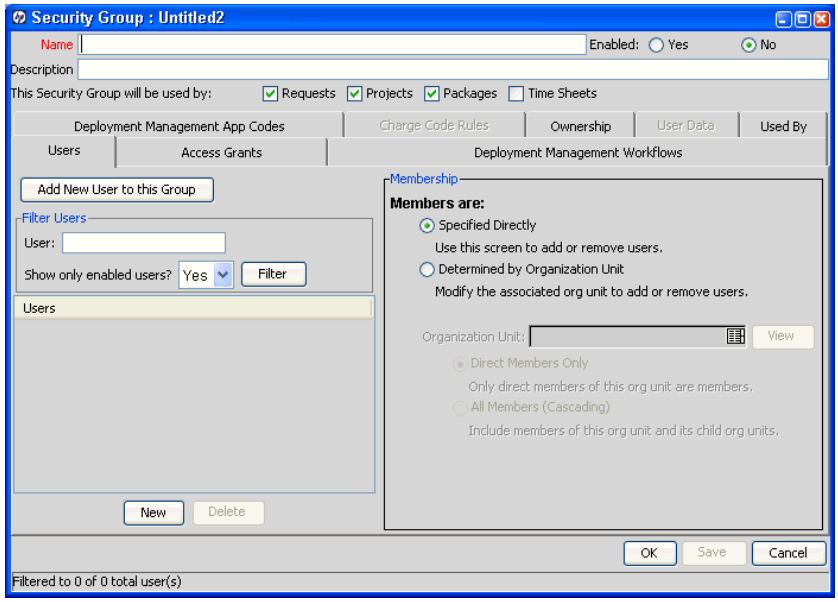
To create a security group:

1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Sys Admin > Security Groups.**

   The Security Group Workbench opens.
4. Click **New Security Group.**

   The Security Group window opens.



5. In the **Name** field, type a name for the group.
6. In the **Description** field, you can type text that describes the group and its purpose.
7. To enable this security group, next to **Enabled,** select **Yes.**

   Only the names of enabled security groups are available when generating or updating users or workflows.
8. For **This Security Group will be used by,** select the checkboxes for the PPM Center entities that you want to be able to use the security group.

   Table 2-2 lists the available checkboxes.

Table 2-2. Options used to associate security groups and entities (page 1 of 2)

Field Name	Description
Requests	Determines whether this security group can be used in request processing. If this checkbox is not selected, the security group is not displayed in: ■ **Assigned Group** field on the request ■ **User Access** tab in the Request Type window—this restricts users in the security group from selecting a request type when creating a request. **Note:** If a user has the System: Override Key Fields Segmentation access grant, then the security group is displayed in the **Assigned Group** field.

Table 2-2. Options used to associate security groups and entities (page 2 of 2)

Field Name	Description
Projects	Determines whether this security group participates in project management activities.
Packages	Determines whether this security group can be used in package processing. If the checkbox is cleared, the security group is not displayed in the **Assigned Group** field in the Package window. **Note:** If a user has the System: Override Key Fields Segmentation access grant, then the security group is displayed in the **Assigned Group** field.
Timesheets	Selecting this checkbox enables the **Charge Code Rules** tab. You can use this tab to specify who has access to certain charge codes in HP Time Management.

9. To link selected users to the security group:
   a. On the **Users** tab, click **New.**

      The Users window opens.

   b. In the **Users** field, select one or more users.
   c. Click **OK.**
10. Link the access grants, as follows:

Each access grant enables certain functions performed on a screen. For a description of each access grant, see Appendix A, *Access Grants,* on page 137.

   a. In the **Available Access Grants** list, select one or more access grants.
   b. Click the right-pointing arrow.
   c. Click **OK.**
11. Restrict the security group from using certain workflows when processing packages, as follows:
   a. Click the **Deployment Management Workflows** tab.
   b. Select the workflows in the **Allowed Deployment Management Workflows** list.

c. Click the left-pointing arrow.

   The **Restricted Deployment Management Workflows** lists the selected workflows.

d. To exclude all future workflows, select the **Always restrict new Workflows** checkbox.

12. Restrict the security group from using certain application codes when creating a package line.

    This restricts the applications through which each user can process objects.

    a. Click the **Deployment Management App Codes** tab.

    b. Select the app codes in the **Allowed Deployment Management App Codes** list.

    c. Click the left-pointing arrow.

       The selected items move to the **Restricted Deployment Management App Codes** list.

    d. To exclude all future app codes, select the **Always restrict new App Codes** checkbox.

13. Click the **Ownership** tab, and then select the ownership groups that you want to be able to edit, copy, or delete the current security group.

    For more information about how to set ownership for a security group, see Chapter 10, *Configuration Security,* on page 125.

14. On the **User Data** tab, enter any necessary information.

15. To save your changes, do one of the following:

    - To register the current security group and close the Security Group window, click **OK.**
    - To save the information and leave the Security Group window open, click **Save.**

Using Resource Management to Control User Security

You can associate users with security groups by including them in an organization model definition. Use the PPM Center resource management capabilities to place a user into a model that includes security and access information. For information on how to do this, see the *HP Resource Management User's Guide.*

To define a security group to use the members of an organization unit:

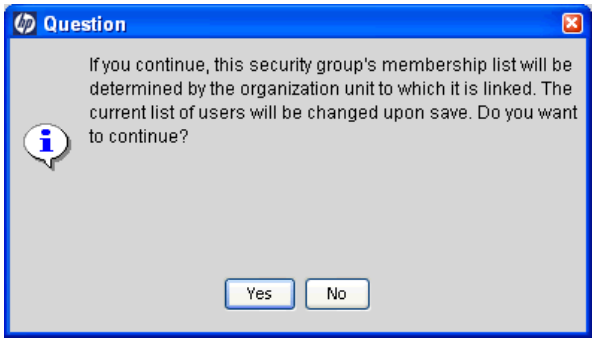
1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Sys Admin > Security Groups.**

   The Security Group Workbench opens.
4. Click **New Security Group.**

   The Security Group window opens.
5. On the **Users** tab, in the **Membership** section, select **Determined by Organization Unit.**

   A dialog box opens and displays a message that explains that the group membership is to be determined by the organization unit to which the group is linked (and not users that you added to this tab), and prompts you to indicate whether you want to continue.



6. Click **Yes.**

   If you select an organization unit to control user access to the security group, any users in the **Users** list are replaced by the members of the organization unit.

7. Select the organization unit.

8. Select one of the following:

   - To include only direct members of the specified organization unit, and exclude its child organization units, select **Direct Members Only.**
   - To include members of this organization unit and its child unit, select **All Members (Cascading).**

     For example, suppose your Quality Assurance organization unit consists of the Testers and Bug Fixers sub-units. If you elect to include members of child organization units for the Quality Assurance unit, then the list of users contains all of the resources defined in each of the units (Quality Assurance, Testers, and Bug Fixers).

9. Click **OK.**

For information about how to associate users with an organization model, see the *HP Resource Management User's Guide.*

Using the Deployment Management App Codes Tab

Application codes (or *app codes*) are part of each HP Deployment Management environment definition. If a site is not licensed for Deployment Management, the **App Codes** tab is unavailable in Deployment Management.

If a security group contains Deployment Management users, you can limit the application codes available to its members when new package lines are generated. This way, you restrict the applications through which each user can process objects. For example, you could assign software changes for an ERP system to one set of users, and assign access to Front Office application changes to a different set of users.

By default, a new security group gives its members access to all Deployment Management app codes. Use the left and right arrows between the two lists on this tab to move app codes to and from the **Restricted** list. Any app code in the **Restricted Deployment Management App Codes** list is unavailable for use by the security group members. To completely restrict a user from using a specific app code, exclude that app code from all security groups to which the user belongs.

As you add lines to a package, Deployment Management normally has an app code default of **NONE.** You can exclude this **NONE** selection out of the **App Code** field. The workflow definition includes a checkbox labeled **Force App Code Selection.**

Using the Charge Code Rules Tab

The **Charge Code Rules** tab lets you control charge code access for security groups used with HP Time Management. Specify the charge codes that are to be visible to members of the security group member here. You can restrict charge codes based on category, client, or department.

A charge code that satisfies a value set by a charge code rule is visible to a members of the security group. For example, a charge code rule of the Category type with the value Billable makes charge codes in the Billable category visible security group members. No other categories are displayed.

If a user belongs to a security group that has no restrictions imposed on it, that user has access to all charge codes. HP recommends that you enable charge code rules for all security groups.

Table 2-3. Security Group window - Charge Code Rules tab fields

Field Name	Description
Restrict Charge Codes to the following rules	Determines whether to restrict charge codes for this security group. If this is not selected, the security group has access to all charge codes.
Type	The type of charge code rule. You can restrict charge codes based on charge code category, client, or department.
Value	The value of the category, client, or department for the allowed charge code.

3 Managing HP Project and Portfolio Management Center Licenses

In This Chapter:

Overview of License Management

Each user who is to view data or perform work in a PPM Center product must have the required product license. Different licenses provide access to, and allow user to perform different actions in different parts of the application. For example, a Project Management license grants a user access to the project planning interface, whereas a Deployment Management license grants access to the interface for creating and processing packages.

The following sections contain the procedures you use to assign PPM Center product licenses from the User Workbench and using the Assign Licenses wizard. For a detailed description of each license, see Appendix B, *License Types,* on page 153.

Assigning Licenses from the User Workbench

To assign a license to a user from the User Workbench:

1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

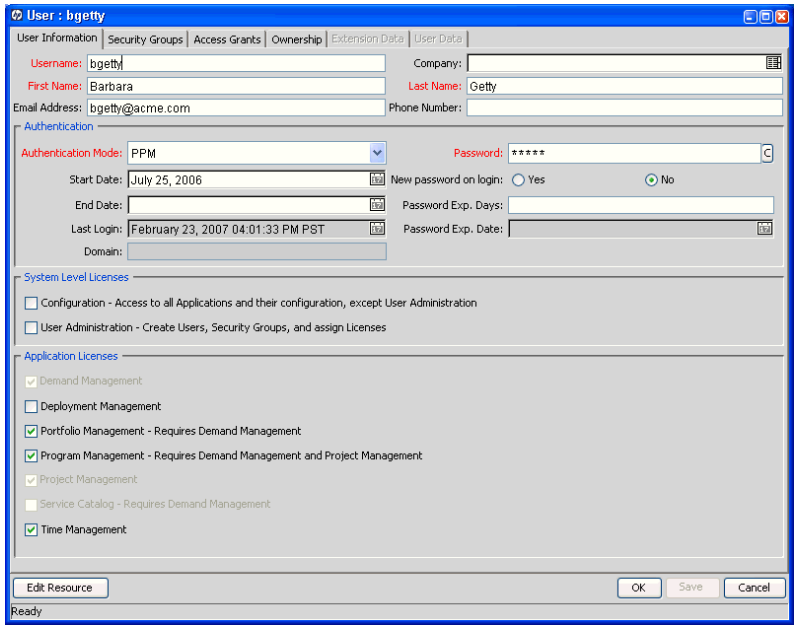
   The PPM Workbench opens.
3. From the shortcut bar, select **Sys Admin > Users.**

   The User Workbench opens.
4. Click **List.**

   The **Results** tab lists all user records.

5. Double-click the record for the user to whom you want to assign a license.

   The User window opens and displays the record for the user you selected.



6. To assign the user a system-level license, under **System Level Licenses,** do one or both of the following:

   - To give the user access to all product functionality available through the PPM Workbench and standard interfaces in PPM Center (except for user and security group administration), select the **Configuration - Access to all Applications and their configuration, except User Administration** checkbox.
   - To give the user permission to administer the users and security groups for all HP products licensed at your site, select the **User Administration - Create Users, Security Groups, and assign Licenses** checkbox.

7. Under **Application Licenses,** select all of the checkboxes that correspond to the application licenses you want to assign to the user.

   You can only assign licenses that your company has purchased. If you do not have licenses for a given PPM Center product, then that license field is unavailable.

   HP Deployment Management Extension licenses are issued on a site-wide basis and are, therefore, not included as an option in the User window.

8. Click **Save.**

To assign a license to a user, you must have the license in the system. If you do not have enough licenses available, after you click **Save,** the PPM Workbench displays an error.

Assigning Licenses to Multiple Users in the License Workbench

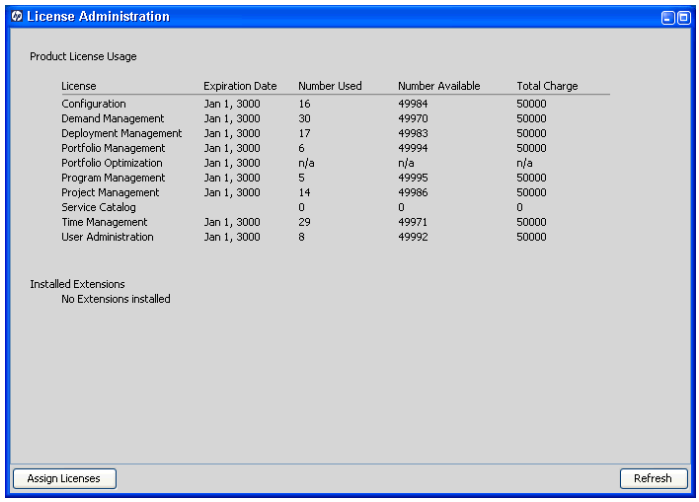
You can use the License Administration window to assign licenses to a group of users. This window provides a single access point from which to view current license usage and availability in the system. You can then use the Assign Licenses wizard to step through the process.

To assign licenses using the Assign Licenses wizard:

1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

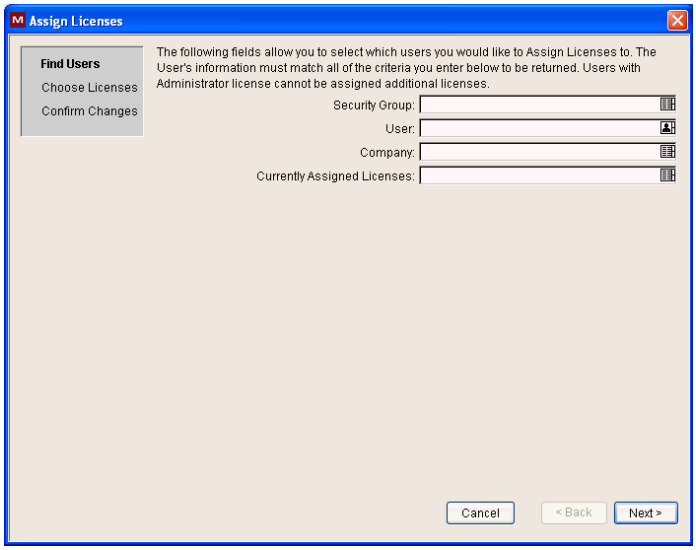
   The PPM Workbench opens.
3. From the shortcut bar, select **System Admin > License.**

   The License Administration window opens. This window lists the licenses available to assign and shows how many of each have been used and how many are available. It also lists the Deployment Management Extensions, if any, installed at your site.



4. Click **Assign Licenses.**

   The Assign Licenses wizard opens to the **Find Users** step.



5. In one or more of the fields listed in *Table 3-1*, enter search criteria to locate the users to whom you want to assign licenses:

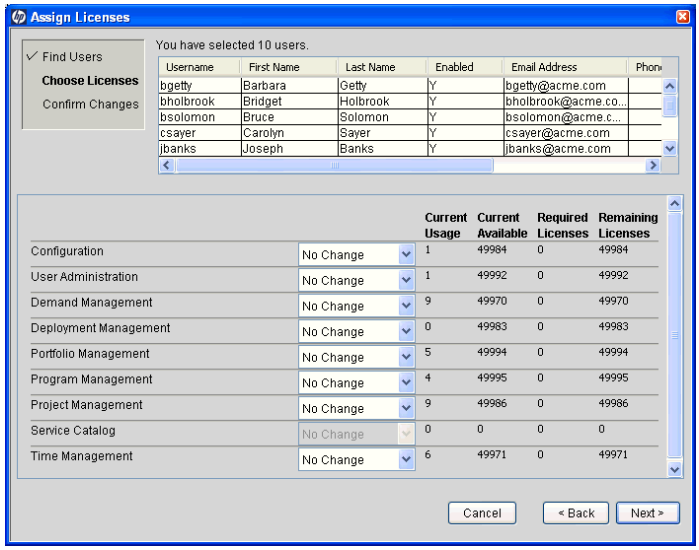
Table 3-1. License Administration wizard - Find Users step

Field Name	Description
Security Group	Locates users who belong to a specific security group. You can select multiple security groups in this field. The search returns a list of all users who belong to any of the selected security groups.
User	Locates users specified in this field.
Company	Locates users associated with a specific company. Companies are associated with users in the Contact window in the Contact Workbench.
Currently Assigned Licenses	Locates all users who have a license specified in this field.
User Data Fields (if any are defined)	Search for users based on the custom user data fields defined at your site.

   If you do not select one or more users, all users are selected by default.

6. Click **Next.**

   The wizard advances to the **Choose Licenses** step.

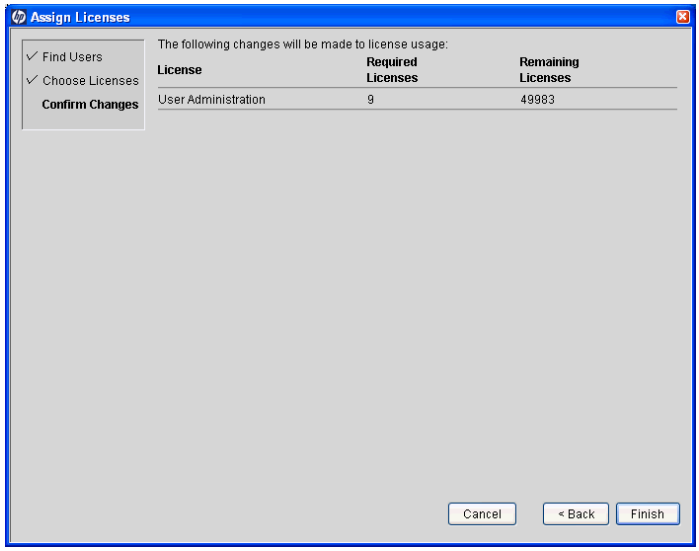


7. On the **Choose Licenses** step, review the listed users, and then select the licenses that you want to assign to them from the license fields.

   Although you can select only a subset of users in the users list, the licenses specified are applied to all users who meet the requirements you specified on the **Find Users** step.

8. Click **Next.**

   The wizard advances to the **Confirm Changes** step.



9. Review the license assignments and ensure that the number in the **Remaining Licenses** column is greater than or equal to zero.

   A negative number indicates that you do not have enough licenses to apply to the users, and cannot complete the license assignment.

10. Click **Finish.**

The Assign Licenses wizard only assigns an available license if the selected user does not already have the license. Licenses append, but do not overwrite, the license specifications for a user (unless you select **Remove License**).

For example, John Smith meets the search requirements you specify for the Find User step. For the Choose License step, you specify that every user is to be granted a Demand Management license. Because John Smith already has a Configuration license, he is not assigned a Demand Management license.

Removing Licenses Using the Assign Licenses Wizard

You can use the Assign Licenses wizard to remove licenses from a set of users.

To remove licenses:

1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.

3. From the shortcut bar, select **Sys Admin > License.**

   The License Administration window opens.

4. Click **Assign Licenses.**

   The Assign Licenses wizard opens.

5. On the **Find Users** step, enter the search criteria to locate the users from which you want to remove licenses, and then click **Next.**
6. On the **Choose Licenses** step, from the list to the right of the license name you want to remove, select **Remove License,** and then click **Next.**
7. On the **Confirm Changes** step, review the license changes, and then click **Finish.**

Assigning Licenses Using the Open Interface

You can also use the PPM Center open interface to assign licenses to users. This API uses interface tables within the PPM Center database instance. Data added to these interface tables is validated and eventually imported into standard database tables, generating or updating user account information.

For detailed information about this feature, see the *Open Interface Guide and Reference*.

4 Request Security

In This Chapter:

Overview of Request Security

This chapter addresses the data and process security related to creating and processing requests in HP Demand Management. Demand Management lets you control who can participate in request resolution.You can restrict user participation based on the following:

- **Request creation**
  - Who can create requests
  - Who can use a specific workflow
  - Who can use specific request types
- **Request processing**
  - Who can act on each step in the workflow

    For this restriction, enable access by specifying users or security groups. Access can also be provided dynamically by having a token resolve to provide access.
  - Who can view or edit certain fields in a request

    For this restriction, enable view or edit access to request fields by specifying users or security groups. You can also have a token resolve to provide access dynamically.
- **Managing request resolution**
  - Who can change the workflow
  - Who can change each request type

Configuring this data and process security often involves setting the following:

- Licenses
- Access grants
- Request type settings on the **User Access** tab
- Field-level settings set in the Field definition window

Prerequisite Settings for Users and Security Groups

General access to request types and certain functions related to processing requests are controlled by access grants associated with security groups. Users in those security groups have access to all of the functionality enabled by those access grants. You can impose restrictions on request viewing or processing at the request type level.

This section addresses the license and access grants settings required to enable general access to request processing.

Only users with the Administrator license can create or modify user and security group accounts. Work with your administrator to provide users with the basic settings required to process requests. Process and data restrictions can later be implemented using settings in the workflow and request type definitions.

Licenses

To create and process requests, users must have either the Demand Management license or the Configuration license.

For details on the functionality associated with each license, see *Licenses and User Roles* on page 157. The following sections address how the functionality provided with each access grant depends on the license type the user has.

Access Grants

Table 4-1 lists the access grants that provide general access to request processing functionality.

Table 4-1. Access grants related to request creation and processing

Access Grant	Description
Demand Mgmt: Edit Requests	Perform basic request processing actions: create requests, edit certain requests, and delete requests that you have not submitted. ■ Lets the user generate requests. ■ Prevents the user from changing the workflow when creating or editing a request. ■ Lets the user edit the request as specified on the **User Access** tab in the Request Type window. ■ Lets the user delete the request as specified on the **User Access** tab in the Request Type window. ■ Lets the user cancel the request as specified on the **User Access** tab in the Request Type window.
Demand Mgmt: Edit All Requests	Perform advanced request processing actions: creating, editing, deleting, changing the request's workflow, and overriding references. ■ User can always edit the request. ■ Override and/or remove any references on any request. ■ User can always delete or cancel a request. ■ User can change the workflow when creating and editing a request.
Demand Mgmt: Change Request Type	Change the request type for existing requests.
Demand Mgmt: Edit Request Header Types	Create, update, and delete request header types in the Request Header Types Workbench.
Demand Mgmt: Edit Request Types	Create, update, and delete request types in the Request Types Workbench.
Demand Mgmt: Override Demand Mgmt Participant Restriction	This access grant lets the user review a request, regardless of whether that user has viewing permission as defined on the **User Access** tab for the request type.

Screen and function access provided through access grants is cumulative. A user who belongs to three different security groups has the access to all of the user interface and functionality granted to all of the groups combined. To

restrict certain screen and feature access, remove the user from any security group that has access to those areas.

Use the **Access Grants** tabs in the User window to see all security groups that have been given specific access grants, and then:

- Remove the user from the security group (using the **Security Group** tab in the User window).
- Remove the access grants from the security group (in the Security Group window). Do this only if no one in that security group requires the access that the access grant provides.

The PPM Center includes additional access grants that you can use to control access to other functions in Demand Management. For more information, see Appendix A, *Access Grants,* on page 137.

Viewing a Request

You can control which users can view requests of a specific type.

To enable all users to view a specific type of request:

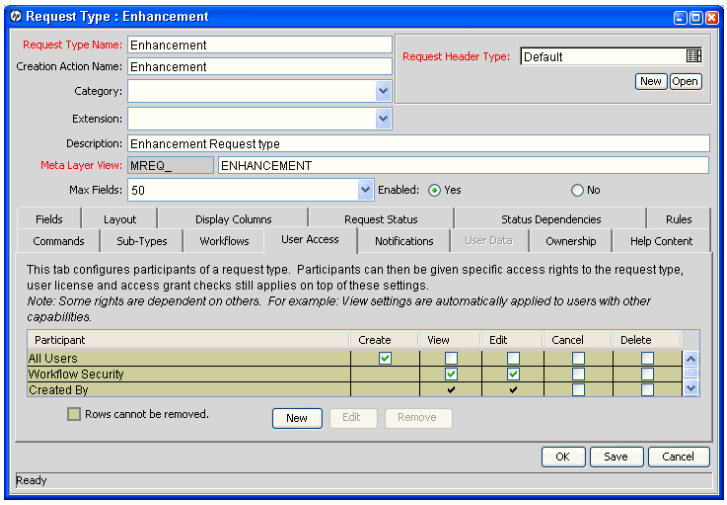
1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Demand Mgmt > Request Types.**

   The Request Type Workbench opens.
4. Click **List.**
5. On the **Results** tab, locate, and then double-click the row that displays the request type that you want all users to be able to view.

   The Request Type window opens to the **Fields** tab.

6. Click the **User Access** tab.



7. In the **All Users** row, if the **View** checkbox is cleared, select it.

8. Click **Save.**

To allow only members of a specific security group to view requests of a specific type:

1. On the **User Access** tab, in the **All Users** row, clear the **View** checkbox.

   By default, the **View** checkbox in the **Workflow Security** row is selected. This indicates that any user included in security for the associated workflow (defined in any workflow step in the Workflow window) can view the request.

2. Click **New.**

   The Participant Security window opens.

3. In the list at the top of the window, leave **Enter a Security Group Name** selected.

4. In the **Security Group** field, enter the name(s) of the security group(s) that can view requests of this type.

5. Click **OK.**

   The **User Access** tab now lists the selected security group(s).

6. In the Request Type window, click **Save.**

To enable specific users to view a request:

1. On the **User Access** tab, in the **All Users** row, clear the **View** checkbox.
2. Click **New.**

   The Participant Security dialog box opens.

3. In the list at the top of the dialog box, select one of the following items:

   - **Enter a Username.** Restricts request access to the user(s) you specify.
   - **Enter a Standard Token.** Control request security dynamically, depending on the value in a standard field. Select from a list of system tokens that correspond to a user or security group.
   - **Enter a User Defined Token.** Control request security dynamically, depending on the value in a custom field. Select any field token that corresponds to a user or security group.

   The field labels under the list change dynamically, depending on which item you select from the list.

4. In the field under the list, which is now labeled **Username, Standard Token,** or **User Defined Token,** enter one or more values (usernames or tokens).
5. Click **OK.**

   The **User Access** tab now lists the items you specified.

6. In the Request Type window, click **Save.**

Creating a Request

You can determine who can create certain requests or use specific request types and workflows.

The following sections assume that your users have the required license and access grants to create and process requests.

Enabling Users to Create Requests

You can use the **User Access** tab in the Request Type window to determine which users can create requests of a specific request type. You can enable all users with required access grants to create a specific request type, or enable only certain users to create requests of a specific type.

The **User Access** tab can include multiple lines that grant access to create or process the requests. A user who meets any of the requirements listed on the tab can perform that action in the request.

To enable all users to create and submit a specific request type:

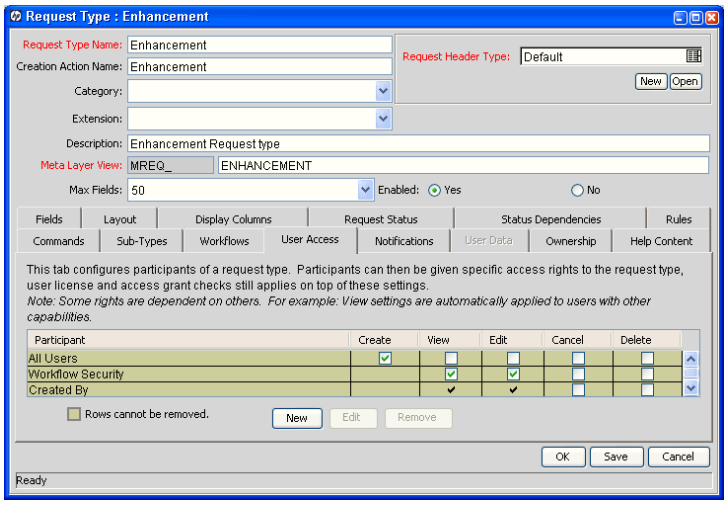
1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Demand Mgmt > Request Types.**

   The Request Type Workbench opens.
4. Click **List.**

   The **Results** tab lists all existing request types.
5. Double-click the row that displays the request type that you want all users to be able to create.

6. Click the **User Access** tab.



7. In the **All Users** row, select the **Create** checkbox.
8. Click **Save.**

To enable only members of a specific security group to create requests of a specific type:

1. On the **User Access** tab, in the **All Users** row, clear the **Create** checkbox.
2. Click **New.**

   The Participant Security window opens.

3. In the list at the top of the window, leave **Enter a Security Group Name** selected.
4. In the **Security Group** field, enter the name of the security group that you want to enable to create requests of the selected type.
5. Click **OK.**

   The **User Access** tab now lists the selected security group.

6. Click **Save.**

To enable specific users to create a request:

1. On the **User Access** tab, in the **All Users** row, clear the **Create** checkbox.
2. Click **New.**

   The Participant Security window opens.

3. In the list at the top of the dialog box, select one of the following items:
   - **Enter a Username.** Restricts request access to the user(s) you specify.
   - **Enter a Standard Token.** Control request security dynamically, depending on the value in a standard field. Select from a list of system tokens that correspond to a user or security group.
   - **Enter a User Defined Token.** Control request security dynamically, depending on the value in a custom field. Select any field token that corresponds to a user or security group.
4. In the field, which is labeled **Username, Standard Token,** or **User Defined Token,** enter one or more values (usernames or tokens).
5. Click **OK.**

   The **User Access** tab now lists the items you specified.
6. Click **Save.**

Restricting Users from Selecting a Specific Workflow

When a user creates a request, he must select a workflow for the request to follow to its resolution. You can control which workflows users can apply to which request types.

To restrict users from selecting a specific workflow to apply to a new request of a specific type:

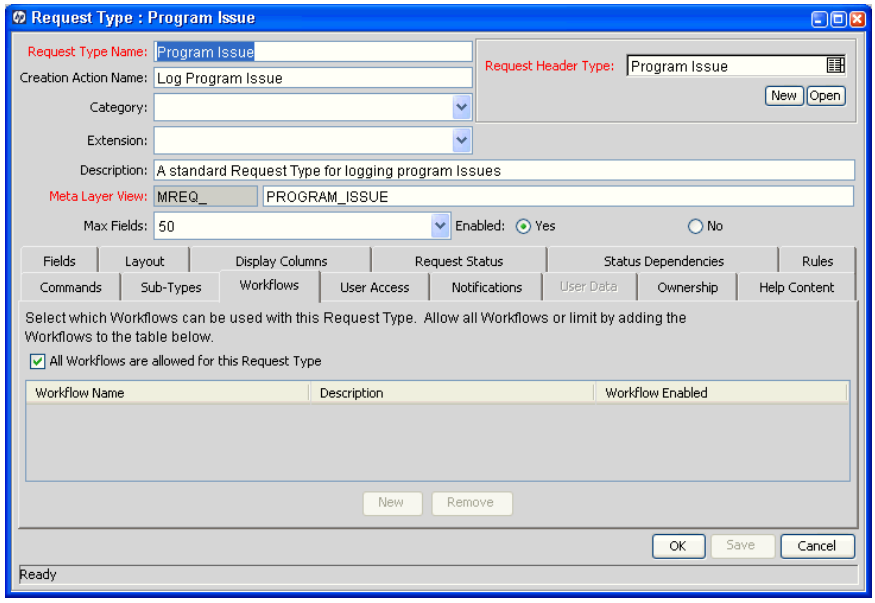
1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Demand Mgmt > Request Types.**

   The Request Type Workbench opens.
4. Click **List.**

   The **Results** tab lists all existing request types.
5. Double-click the row that displays the request type for which you want to restrict applied workflows.

   The Request Type window opens.
6. In the Request Type window, click the **Workflows** tab.



7. Clear the **All Workflows are allowed for this Request Type** checkbox.
8. Click **New.**

   The Workflow: New window opens.

9. In the **Workflow** field, enter the names of the workflows that users can apply to this request type.
10. Click **OK.**

    The **Workflow** tab lists the selected workflows.
11. Click **Save.**

Only workflows specified on the **Workflow** tab can be applied to requests of this selected type.

Request types can be associated with workflows such that only certain request types can be processed through the workflow. The selected request type must be enabled so that the user can create a request when using that workflow.

You can opt to restrict all new request types. You can also specify the default request type to be used with this workflow. (This is set on the Workflow window **Request Types** tab.)

Processing a Request

You can control who can process requests following a request submission. This includes specifying who can edit fields on request, cancel a request, and delete a request. You can also control who can act on certain steps (decisions and executions) in a process.

The following sections assume that your users have the required license and access grants to perform basic request creation and processing.

Enabling Users to Edit Fields on a Request

You can determine who can edit fields on requests of a specific type.

To enable all users to edit fields on a specific request type:

1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

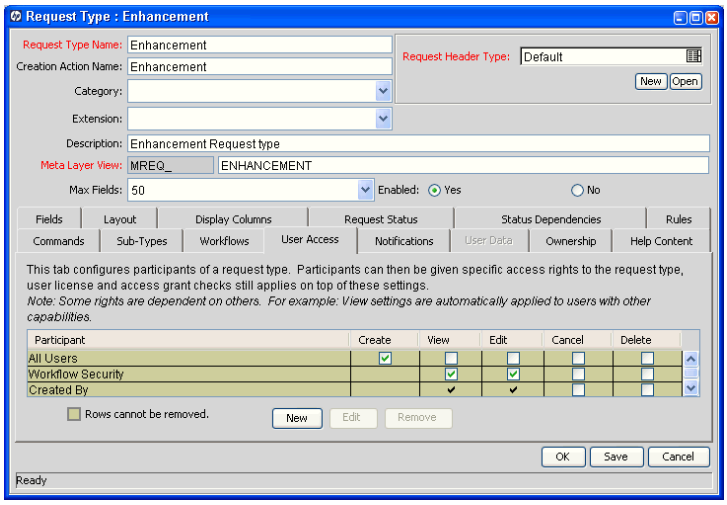
   The PPM Workbench opens.
3. From the shortcut bar, select **Demand Mgmt > Request Types.**

   The Request Type Workbench opens.
4. Click **List.**

   The **Results** tab lists all existing request types.
5. Double-click the row that displays the request type for which you want to configure field editability.

   The Request Type window opens to the **Fields** tab for the request type.

6. Click the **User Access** tab.



7. In the **All Users** row, select the **Edit** checkbox.
8. Click **Save.**

To enable only members of a specific security group to edit a request:

1. On the **User Access** tab, in the **All Users** row, clear the **Edit** checkbox.

   By default, the **Edit** checkbox in the **Workflow Security** row is selected. This indicates that any user included in the security for the associated workflow (defined in any workflow step in the Workflow window) can edit request fields.

2. Click **New.**

   The Participant Security dialog box opens.

3. In the list at the top of the window, leave **Enter a Security Group Name** selected.
4. In the **Security Group** field, select the security group(s) whose members can edit requests of the selected type.
5. Click **OK.**

   The **User Access** tab now lists the selected security group(s). The **Edit** checkbox is selected by default.

6. Click **Save.**

To enable only specific users to edit requests of a given type:

1. On the **User Access** tab, in the **All Users** row, clear the **Edit** checkbox.
2. Click **New.**

   The Participant Security dialog box opens.

3. In the list, select one of the following items:

   - **Enter a Username.** Specify individual user names.
   - **Enter a Standard Token.** Control request security dynamically, depending on the value in a standard field. Select from a list of system tokens that corresponds to a user or security group.
   - **Enter a User Defined Token.** Control request security dynamically, depending on the value in a custom field. Select from any field token that corresponds to a user or security group.

     The field labels under the list change dynamically, depending on which item you select from the list.

4. In the field now labeled **Username, Standard Token,** or **User Defined Token,** enter one or more values (usernames or tokens).
5. Click **OK.**

   The **User Access** tab displays a new line that shows the selected user or token. By default, the **Edit** field is selected.

6. In the Request Type window, click **Save.**

Enabling Users to Cancel or Delete a Request

You can determine who has permission to cancel or delete requests of a specific type.

To enable all users to cancel or delete requests of a given type:

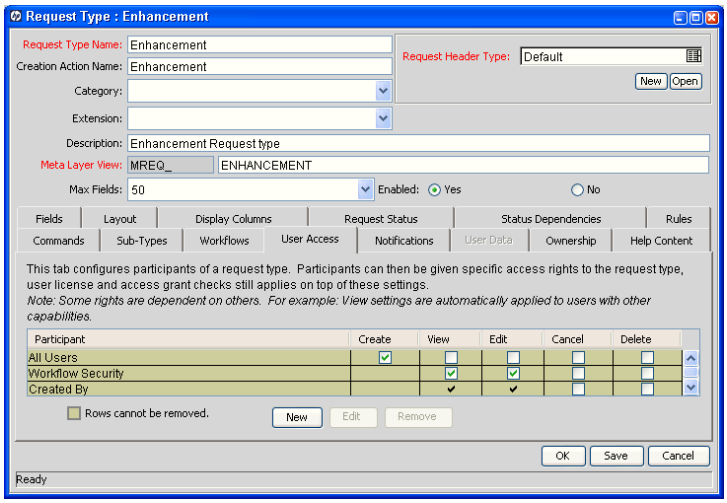
1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Demand Mgmt > Request Types.**

   The Request Type Workbench opens.
4. Click **List.**

   The **Results** tab lists all existing request types.
5. Double-click the row that displays the request type you want to configure.

   The Request Type window opens.
6. Click the **User Access** tab.



7. In the **All Users** row, select the **Cancel** and **Delete** checkboxes.
8. Click **Save.**

To allow only specific users or members of a specific security group to cancel or delete a request:

1. On the **User Access** tab, click **New.**

   The Participant Security dialog box opens.

2. In the list, select one of the following items:

   - **Enter a Security Group.** Specify all users in a security group.
   - **Enter a Username**
   - **Enter a Standard Token.** Control request security dynamically, depending on the value in a standard field. Select from a list of system tokens that corresponds to a user or security group.
   - **Enter a User Defined Token.** Control request security dynamically, depending on the value in a custom field. Select from any field token that corresponds to a user or security group.

   The field labels under the list change dynamically, depending on which item you select from the list. For example, selecting **Enter a Username** changes the field label below the list to **Username.**

3. Enter the specific value that corresponds to the recipient type you selected.
4. Click **OK.**

   The **User Access** tab displays a new line that shows the selected user or token.

5. In the new row, select the **Cancel** and **Delete** checkboxes.
6. In the Request Type window, click **Save.**

To enable the user who logged the request to cancel or delete that request:

1. Open the Request Type window.
2. Click the **User Access** tab.
3. In the **Created By** row, select the **Cancel** and **Delete** checkboxes.
4. Click **Save.**

Enabling Users to Act on a Specific Workflow Step

You must specify who can act on each step in the request resolution workflow. Only users who are specified on the **Security** tab in the Workflow Step window can process a request at that step.

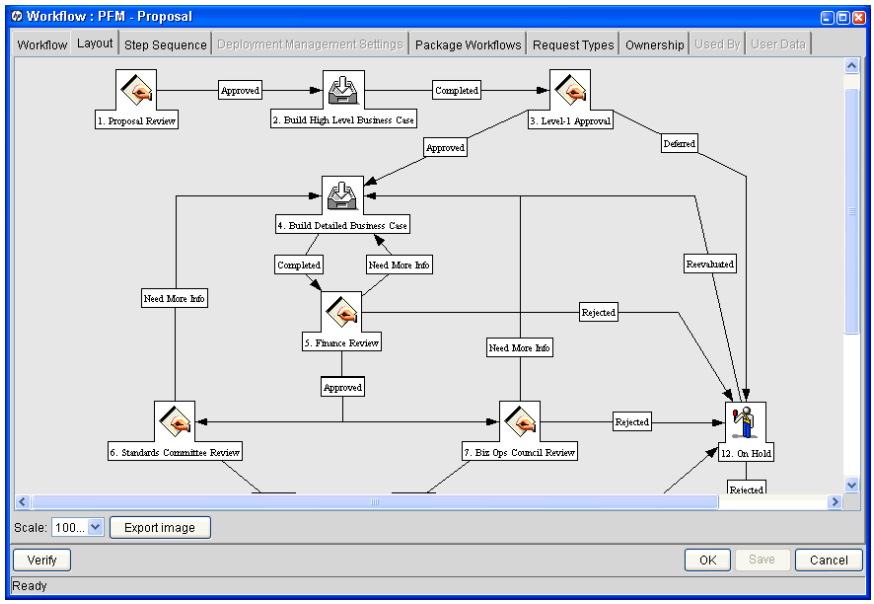
To specify who can act on a specific workflow step:

1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Configuration > Workflows.**

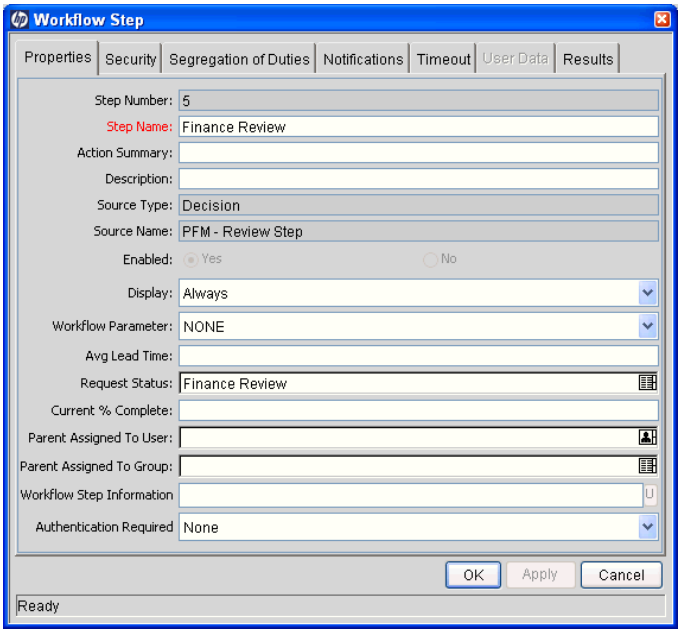
   The Workflow Workbench opens.
4. Click **List.**
5. On the **Results** tab, locate and open the workflow.

The Workflow window opens to the **Layout** tab.



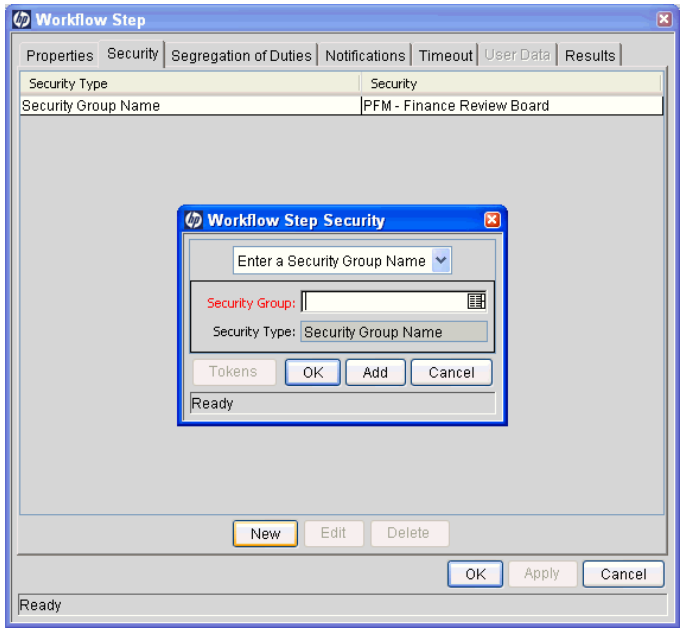
6. Double-click the step you want to configure.

   The Workflow Step window opens.



7. Click the **Security** tab, and then click **New.**

   The Workflow Step Security dialog box opens.



8. In the list at the top of the window, select one of the following methods for specifying the step security:

   - **Security Group Name**
   - **Username**
   - **Standard Token**
   - **User Defined Token**

   Selecting a value from this list automatically updates the other fields in the window. For example, selecting **Enter a Username** changes the **Security Group** field label to **Username.**

9. Specify the security groups, usernames, or tokens to control the access to this step.

10. Click **OK.**

    The security specification is added to the **Security** tab. You can add more specifications to the step by clicking **New** and repeating these steps. You can, therefore, control step security using a combination of security groups, usernames, and tokens.

11. Click **OK.**

Consider assigning a security group to each decision, execution and condition step, even if many of the steps proceed automatically. If a command fails, or a condition is not met, it may be necessary to manually override the step.

Also consider assigning a “Request Manager” security group to each step. You can provide that group with global access to act on every step in the process. This helps avoid bottlenecks by giving a small group permission to process stalled requests.

Avoid allowing just one person to act on a workflow step. If that user changes roles or leaves the company, a process update (reconfiguration) would be required. Instead, use a token or security group to configure access dynamically.

Viewing and Editing Fields on a Request

You can use several features to prevent users from viewing or editing specific fields on a request. You configure this field-level data security using the Request Type and Request Header Type windows in the PPM Workbench.

Information presented in the following sections is based on the assumption that the user has been granted standard access to view and edit the request, but does not have the Demand Mgmt: Edit All Requests access grant.

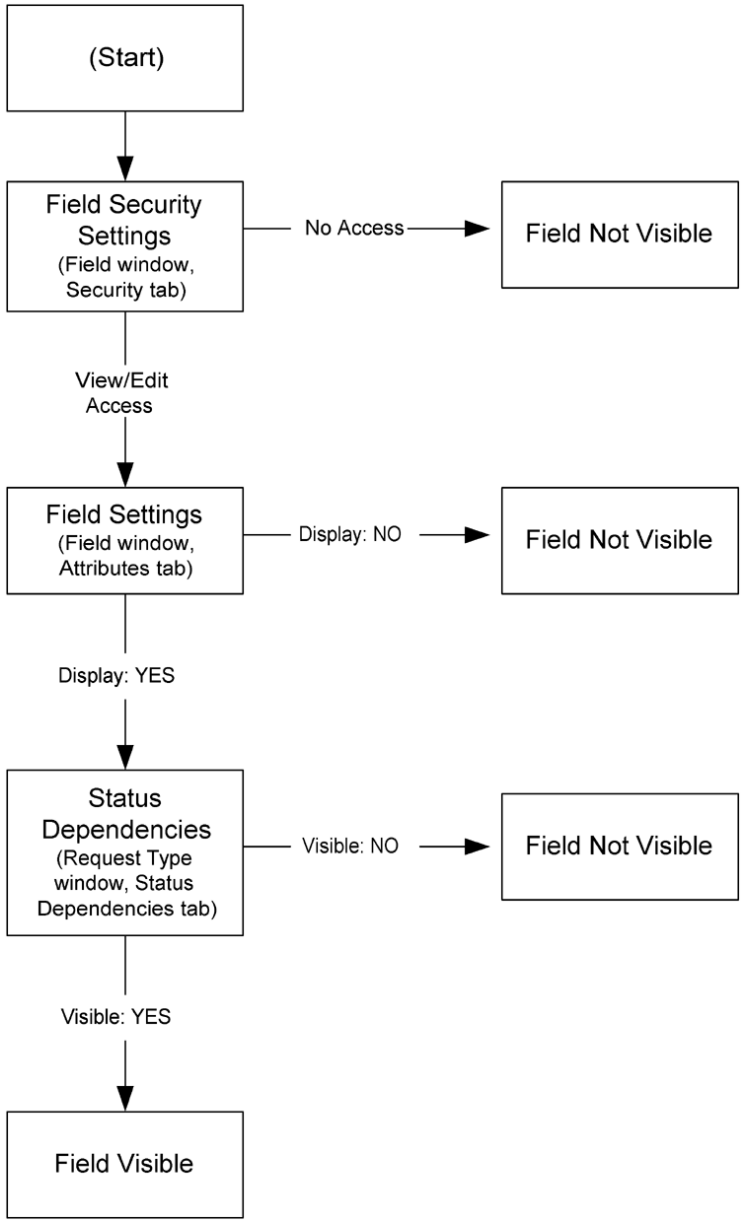
Field-Level Data Security Overview

You can configure field editability and visibility in the following areas of the PPM Workbench:

- Field window: Use the **Attributes** tab to set general view and edit access for all users.
- Field window: Use the **Security** tab to set view and edit access for a specific user list.
- Request Type window: Use the **Status Dependencies** tab to set view and edit access for a field based on request status.

  Figure 4-1 on page 68 illustrates the settings that determine whether a field is visible to a given user.

Figure 4-1. Field visibility interactions



Field Window: Attributes Tab

You can use the **Attributes** tab in the Fields window to set general field view and edit access.

To open the **Attributes** tab in the Fields window and set field visibility and editability:

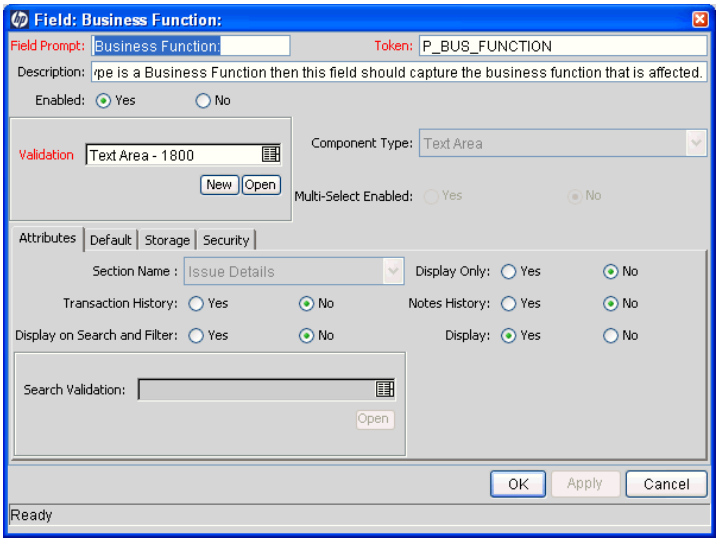
1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Demand Mgmt > Request Types.**

   The Request Type Workbench opens.
4. Click **List.**
5. Open the request type with fields that you want to configure.

   The Request Type window opens to the **Fields** tab.
6. To view the fields associated with the request type, in the **Prompt** column, expand the listed nodes.
7. Double-click the row that displays information about the field you want to configure.

   The Field window opens to the **Attributes** tab.



8. To make the selected field editable on a request, next to **Display Only,** leave **No** selected. To make it a read-only field, select **Yes.**
9. To make the selected field visible on a request of the selected type, next to **Display,** leave **Yes** selected. To hide the field, select **No.**

Field Window: Security Tab

Use the **Security** tab to set view and edit access for a specific user list.

To limit field visibility and editability to a specific group of users:

1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

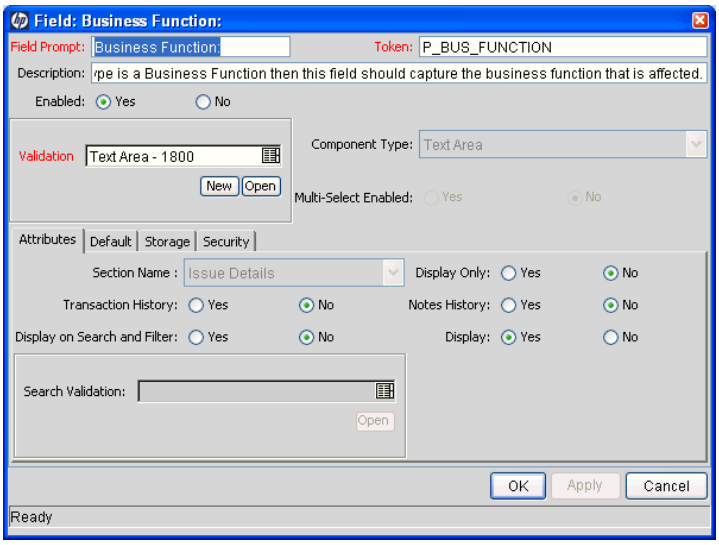
   The PPM Workbench opens.
3. From the shortcut bar, select **Demand Mgmt > Request Types.**

   The Request Type Workbench opens.
4. Click **List.**
5. Open the request type with fields that you want to configure.

   The Request Type window opens.
6. Click the **Fields** tab.
7. To view the fields associated with the request type, in the **Prompt** column, expand the listed nodes.

8. Double-click the row that displays information about the field you want to configure.

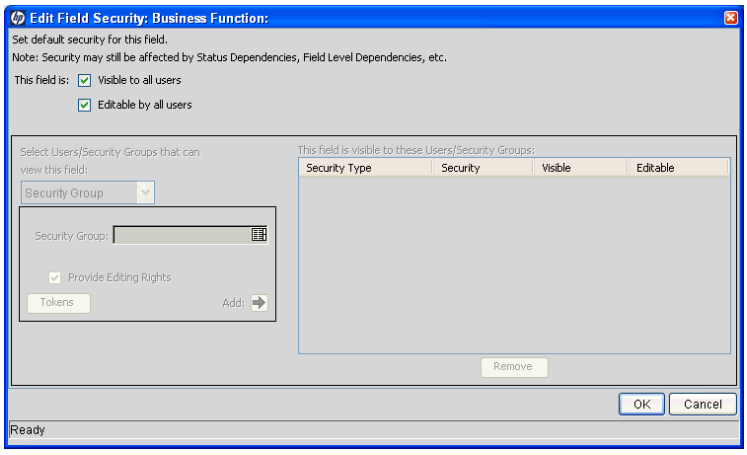
   The Field window opens.



9. Click the **Security** tab.

10. Click **Edit.**

    The Edit Field Security window opens.



11. Clear the **Visible to all users** checkbox.

This also clears the **Editable by all users** checkbox.

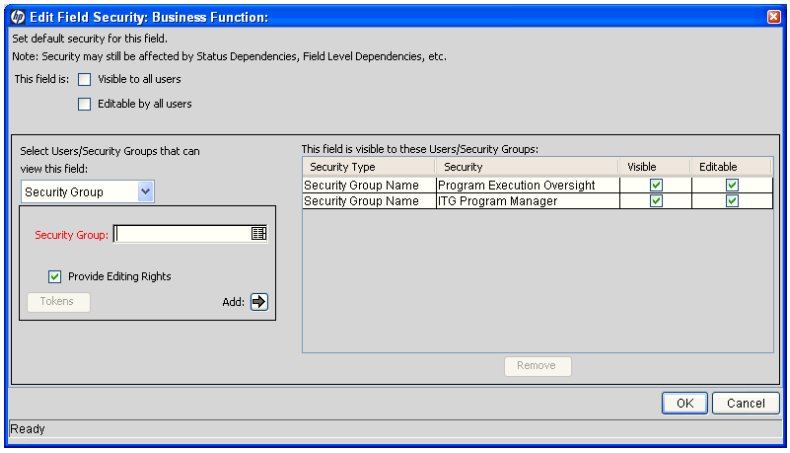
12. In the list under **Select Users/Security Groups that can view this field,** select one of the following:

    - **Security Group**
    - **Username**
    - **Standard Token**
    - **User Defined Token**

    The value you select from this list updates the other fields in the window. For example, selecting **Enter a Username** changes the **Security Group** field label to **Username.**

13. Select the security groups, usernames, or tokens to control access to the step.

14. Click the **Add** arrow to add the selection to the table on the right.



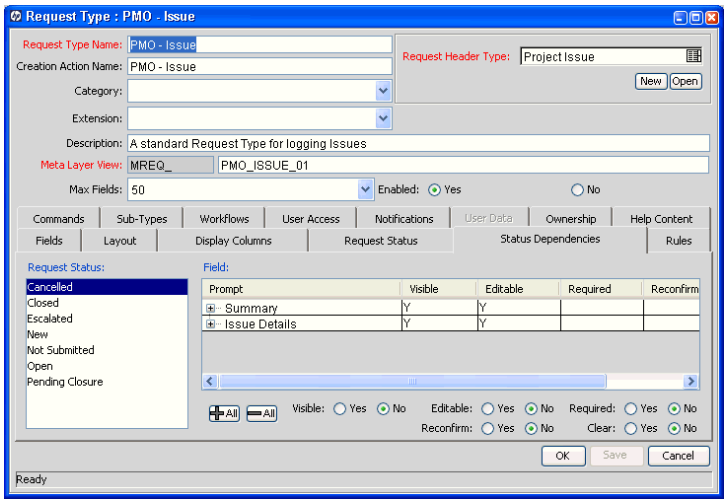
15. Click **OK.**

Request Type Window: Status Dependencies Tab

You can directly link request field behavior to the status values for the request. Select a field and a request status and assign that field's attributes under the given request status. This is done by selecting among the options at the bottom of the screen.

You can set view and edit access for a field depending on request status using the following controls on the **Status Dependencies** tab:

- **Visible.** This option determines whether or not a field is visible at a specific request status. To hide the field at the request status, select **No.**
- **Editable.** This option determine whether the field can be edited at a specific request status. To make the field read-only at this request status, select **No.** To make the field modifiable at the request status, select **Yes.** If the **Required, Reconfirm,** or **Clear** option is set to **Yes,** then **Editable** must be set to **Yes.**



Overriding Request Security

Users with the following settings can view, edit, and delete any request.

Table 4-2. Settings required to override request security

Setting	Value	Description
Access Grants linked to the Security Group	Demand Mgmt: Edit All Requests	Perform advanced request processing actions: creating, editing, deleting, changing the request's workflow, and overriding references.
	Demand Mgmt: Override Demand Mgmt Participant Restriction	View the detailed information on a restricted request for which the user is not an active participant.

Users who have the System: Ownership Override access grant can edit request types, regardless of ownership restrictions.

5 Package Security

In This Chapter:

Overview of Package Security

This chapter addresses the data and process security related to creating and processing packages in HP Deployment Management. Deployment Management lets you determine who can participate in package deployment. You can restrict user actions based on the following:

- **Package creation**
  - Who can create packages
  - Who can use a specific workflow
  - Who can use specific object types
- **Package processing**
  - Who can approve or process each step in the workflow
  - Whether you only want participants to process the packages. Participants are defined as the assigned user, the creator of the package, members of the assigned group, or any users who have access to the workflow step(s).
- **Managing deployment**
  - Who can change the workflow
  - Who can change each object type
  - Who can change the environment and environment group definitions
  - Who can change the security group definitions

Configuring this data and process security often involves a setting a number parameters, such as:

- Licenses
- Access grants
- Object type, workflow, and security group settings
- Field-level settings

This lets you control which processes are used for deployments and which environments are affected.

The screen and function access that access grants provide is cumulative. A user who belongs to three different security groups has access to all of the user interface and functionality available to the three groups combined. To restrict certain screen and feature access, remove the user from any security group that grants that access.

You can use the **Access Grants** tabs in the User window to see all security groups where specific access grants are included. You can then:

- Remove the user from the security group (on the **Security Group** tab in the User window).
- Remove the access grants from the security group (in the Security Group window). Do this only if no one in that security group needs the access that the access grant provides.

This chapter provides information about how to allow a user to view or edit items in Deployment Management. To restrict access, you can change settings or remove the access grants or licenses.

Viewing a Package

You can control which users can view a package. To enable a user to view packages, modify the settings listed in *Table 5-1*:

Table 5-1. Settings to view packages

Setting	Value	Description
License (only one is required)	Deployment Management or Configuration	The Deployment Management license provides a user with access to the PPM Workbench or standard interface where they can view the package approval page.
Access Grants linked to the Security Group	Deployment Management: View Packages	This access grant allows the user to view packages. **Note:** The Deployment Management: Edit Packages and Deployment Management: Edit All Packages access grants also provide viewing privileges, but enable more advanced editing and processing functions. You configure access grants in the Security Group window.

Restricting Package Viewing to Participants

To determine who can have access to packages that use the current workflow, you use the **Package Security** option on the **Deployment Management Settings** tab in the Workflow window. Restricting access to participants means that a nonparticipant user who searches for packages cannot see packages that use the current workflow. In this instance, participants are defined as one of the following:

- Assigned user
- Package creator
- Members of the assigned security group
- Any user who has access to the workflow step(s)

To give all Deployment Management users access to packages that use the applied workflow, select **All Users.**

To restrict the users who can access packages associated with this workflow to participants, select **Participants Only.**

Creating a Package

You can control who can create packages or use specific object types and workflows. This provides a great deal of control over who can process changes of a certain type to specific environments.

Enabling Users to Create Packages

To enable a user to create and submit packages, configure the settings listed in *Table 5-2* on page 79.

Table 5-2. Settings to enable package creation

Setting	Value	Description
License	Deployment Management or Configuration	The Deployment Management license gives a user access to the PPM Workbench, where the package is defined.
Access Grants linked to the Security Group (only one is required.)	Deployment Management: Edit Packages	This access grant allows the user to generate, edit and delete certain packages. The user cannot delete a package if it has been released or if the user is not the owner. To edit the package, the user must be its creator, the assigned user, a member of the assigned security group, or a member of the workflow step security.
	Deployment Management: Edit All Packages	This access grant lets the user create, edit, and delete packages at any time.
Allowed Deployment Management Workflows in the Security Group window	You must allow at least one workflow.	A package must have an applied workflow to follow. To create and submit a package, you must select the workflow to process the deploying objects. This is set on the **Deployment Management Workflows** tab in the Security Group window.
Allowed Deployment Management Object Types in the Workflow window.	You must allow at least one object type in each workflow used to deploy changes.	You can associate object types with workflows so that only certain object types can be processed through the workflow. You must enable at least one object type so that the user can create a package line using that workflow. Set this in the Workflow window, on the **Deployment Management Settings** tab, with the **Package Line** option selected.

Preventing Users from Selecting a Specific Workflow

You can restrict users from selecting specific workflows when creating a new package. To do this, ensure that the following conditions are met.

Table 5-3. Settings to restrict workflow selection

Setting	Value	Description
Restricted Deployment Management Workflows in the Security Group window	Include the workflows that you want to restrict.	To create a package, a user must select a workflow for the package to follow. Users (in the security group) cannot select a workflow included in the **Restricted Deployment Management Workflows** list. **Note:** If a user belongs to another security group that is allowed to use that workflow, the user can select it. (This is set on the **Deployment Management Workflows** tab in the Security Group window.

Because the source and destination environments are defined in the workflow step, restricting the workflow selection also determines who can deploy changes to specific environments.

Preventing Users from Selecting a Specific Object Type

You can prevent users from selecting specific object types as they add lines to a package. *Table 5-4* contains the information you need to restrict Deployment Management object types.

Table 5-4. Settings to restrict object type selection

Setting	Value	Description
Restricted Deployment Management Object Types in the Workflow window.	Include the object type that you want to restrict.	You can associate object types with workflows so that only certain object types can be processed through the workflow. Users cannot select any object types included in the **Restricted Deployment Management Object Types** list. This is set in the Workflow window, on the **Deployment Management Settings** tab, with the **Package Line** option selected.

Approving Package Lines

All users who process package lines must meet the following conditions:

Table 5-5. Settings to enable package processing

Setting	Value	Description
License	Deployment Management or Configuration	This license gives a user access to the PPM Workbench and standard interface. Users can act on all workflow steps (decisions and executions) in the PPM Workbench.
Access Grants linked to the Security Group	Deployment Mgmt: Edit Packages	This access grant lets the user generate, edit, and delete packages. To edit the package, user must be its creator, an assigned user, a member of the assigned security group, or a member of the security group for the workflow step.
	Deployment Mgmt: Edit All Packages	This access grant lets the user edit or delete packages at any time.

Enabling Users to Act on a Specific Workflow Step

You must specify who can act on each step in a deployment workflow. Only users listed on the **Security** tab in the Workflow Step window can process that step.

Deleting a Package

To determine who can delete a package, use the settings listed in *Table 5-6*.

Table 5-6. Settings required to enable a user to delete packages

Setting	Value	Description
License	Deployment Management	This license provides a user with access to the PPM Workbench and advanced package processing options.
Access Grants linked to the Security Group	Deployment Mgmt: Edit Packages	A user with this access grant can delete a package he owns but has not submitted.
	Deployment Mgmt: Edit All Packages	A user with this access grant can delete any package to which he has access.

Overriding Package Security

Table 5-7 lists the settings you must configure to enable a user to view, edit, and delete any package.

Table 5-7. Settings to override package security

Setting	Value	Description
License	Deployment Management or Configuration	This license gives a user access to the PPM Workbench and advanced package processing options.
Access Grants	Deployment Mgmt: Edit All Packages	A user with this access grant can view, edit, and delete any package.
	Deployment Mgmt: Override Deployment Mgmt Participant Restriction	A user with this access grant can view the detailed information on a restricted package in which the user is not an active participant.

Users with the System: Ownership Override access grant can edit Deployment Management configuration entities, regardless of ownership restrictions.

6 Project and Task Security

In This Chapter:

Overview of Project and Task Security

This chapter addresses the data and process security related to creating and processing projects in HP Project Management. Configuring this data and process security typically involves changing several settings, including licenses, access grants, entity-level settings, and field-level settings. This section provides information about the settings required to secure the specified actions or data.

The screen and function access that access grants provide is cumulative. If a user belongs to three different security groups, he has the access provided to all of the groups combined. Therefore, to restrict certain screen and feature access, you must remove the user from any and all security groups that have that access.

To see all security groups that are assigned specific access grants, use the **Access Grants** tabs in the User window. You can then:

- Remove the user from the security group (using the **Security Group** tab in the User window)
- Remove the access grants from the security group (in the Security Group window). Do this only if no one in that security group needs the access that this access grant provides.

Viewing Projects and Tasks

To allow users to view projects and tasks, assign one of the licenses and access grant combinations listed in *Table 6-1*.

Table 6-1. Settings required to view projects and tasks (page 1 of 2)

Setting	Value	Description
License	■ Project Management ■ Portfolio Management ■ Configuration ■ Demand Management ■ Time Management ■ Program Management ■ Configuration	Any one of these licenses makes project-level information on the **Project Summary** tab available.
License	Project Management	The **Project Management** license allows users to: ■ Access to work plans, tasks, work-plan baselines, and earned value information. ■ Log and manage project control requests (issues, risks, scope changes). ■ Define or manage project types or work-plan templates. ■ Access task-level information and to log actuals (assigned resources only).
License	Time Management	The **Time Management** license allows resources to: ■ Log time through a timesheet (for projects that allow it. ■ Access task-level information and to log actuals (assigned resources only).

Table 6-1. Settings required to view projects and tasks (page 2 of 2)

Setting	Value	Description
License	Demand Management	The **Demand Management** license allows users to log and manage project control requests (issues, risks, scope changes) and access the all HP Demand Management functionality.
License	Portfolio Management	The **Portfolio Management** and **Configuration** licenses allow resources to log and manage project control requests (issues, risks, scope changes).
Access Grants linked to the Security Group	Project Mgmt: View Projects	The Project Mgmt: View Projects access grant lets resources view project definitions in the standard interface. **Note:** The Project Mgmt: Edit Projects and Project Mgmt: Edit All Projects access grants also provide viewing privileges, but enable editing and processing functions.

To restrict users from viewing projects and tasks, use the settings listed in *Table 6-2*.

Table 6-2. Settings to restrict a user from viewing projects and tasks (page 1 of 2)

Setting	Value	Description
License	(REMOVE) Project Management	Removing the Project Management license from users prevents them from viewing project- or task-related pages or windows in HP Project Management. It also restricts their use of methodology entities (project types and work plan templates). **Note:** Removing just the Project Management license is not sufficient to remove all project access, since other licenses are sufficient.
Access Grant	(REMOVE) Project Mgmt: View Projects; Edit Projects; Edit All Projects	Removing these access grants from users prevents them from viewing projects and tasks through Project Management.

Table 6-2. Settings to restrict a user from viewing projects and tasks (page 2 of 2)

Setting	Value	Description
Access Grant	(REMOVE) View/Edit Work Plan Cost Data	Further restricts who can view or edit the costs associated with the project. Removing the access grants for Budgets, Benefits, Staffing Profiles prevents the user from looking at these entities across all projects. Participants on the project process are also considered project participants. This means that anything specified in the request and workflow can add to the participants. If you want to restrict project participants, you must also configure security for the request type and workflow. To limit visibility of the project-level fields and lifecycle, set up security on the request type and workflow used for the project. (This includes field-level security.)
Users who can view this project and its tasks	All Users Only participants (Project Managers, Summary Task Owners, Assigned Resources, Assigned Resource Groups, Stakeholders, and Process Participants)	Restricts who can view projects and tasks to participants. A participant can be a: ■ Project manager ■ Assigned task resource or task owner ■ Member of an assigned security group ■ Program manager ■ Stakeholder
Budget, Benefit, and Cost information on the Project and Tasks can be viewed by	■ All Users who can view the project and its tasks ■ Project Managers and Stakeholders ■ Project Managers, Stakeholders, Summary Task Owners and Process Participants	Restricts who can view the costs associated with the project and its tasks.

Controlling Resources on the Project

Project managers can specify which users can serve as project resources. The project's staffing profile typically defines the resources available to the project.

When assigning resources to the project work plan, the project manager can choose from resources named on the staffing profile and resources that are members of resource pools that the project manager manages. Any resources that are not available by these means must be requested from other resource pools, using staffing profiles.

Creating Projects

You can control which users can create projects and tasks. Any users with the licenses and access grants list in *Table 6-3* can create projects.

Table 6-3. Settings required to create a project

Setting	Value	Description
License	■ Project Management ■ Portfolio Management ■ Configuration ■ Demand Management	Lets users create projects from Project Management in the standard interface. The Demand Management license lets a user create a project through a workflow.
Access Grants (only one is required)	Project Mgmt: Create Projects and Project Mgmt: Edit Projects	Lets users create projects.
	Project Mgmt: Edit All Projects	Lets users edit projects and override (or remove) references on projects or tasks.

Editing Project Information

To edit project information, a user must have one of the following licenses:

- Project Management
- Demand Management
- Portfolio Management
- Program Management
- Configuration

In addition to a required license, a user must also have one of the following access grants to edit project information:

- **Edit Projects.** The Edit Projects access grant gives edit access to project-level fields and process, subject to any restrictions defined through the request type or workflow.
- **Edit All Projects.** The Edit All Projects access grant gives edit access to any project, including those for which the user would not otherwise meet participant requirements. This includes the ability to perform edits reserved for the project manager.

Some editing functions are limited to the project managers assigned to the project. These are:

- Modify settings
- Modify participant groups
- Override the overall project health
- Create, edit, schedule, or delete the project work plan
- Create the project staffing profile from the project overview page (also requires access grants for this entity)
- Create the project budget from the project overview page (also requires access grants for this entity)
- Create, delete, and set the active work plan baselines (requires additional grants)
- Delete projects (requires additional grants)

Editing Work Plan Information

To edit work plan information, a user must have one of the following:

- Project Management license and either the Edit Projects or Edit All Projects access grant
- Configuration license

Users who have permission to edit work plan information can create, update, schedule, and delete work plans and their associated tasks. They can also access earned value data.

Managing Project Baselines

To manage project baselines, a user must have one of the following licenses:

- Project Management
- Configuration

In addition to a required license, a user must also have one of the following access grants to manage project baselines:

- **Manage Work Plan Baselines.** The Manage Work Plan Baselines access grant (in addition to the grants required to edit work plan information) allows users to create and manage work plan baselines.
- **Manage All Work Plan Baselines.** The Manage All Work Plan Baselines access grant allows users to manage baselines, even if the user cannot otherwise edit the work plan.

To strictly limit who can take baselines to a small group, you can remove the Managing Work Plan Baselines access grant from all users, and then provide the Manage All Work Plan Baselines grant to the small central group. This prevents a project manager from baselining his or her own project, thereby centralizing control.

Updating Tasks

You can determine which users can record progress on their assigned work plan tasks by using the licenses and access grants listed in *Table 6-4* and *Table 6-5*.

Table 6-4. Settings required to update tasks

Setting	Value	Description
License	Project Management or Configuration Time Management	The Project Management, Time Management, and Configuration licenses let resources update progress on their assigned tasks in the My Tasks portlet. The Time Management license allows unassigned resources to log time against the project through HP Time Management (if the project settings allow it.)
Access Grants	Project Mgmt: Update Tasks (Required)	If a user is specified as a resource on the project, he can update tasks.
	Project Mgmt: Edit All Projects	If a user is assigned to tasks in the work plan, he can use the My Tasks portlet to report progress on multiple tasks.
	Project Mgmt: Edit Projects	If the user is assigned to tasks in the work plan, he can use the My Tasks portlet to record progress on multiple tasks.

To prevent users from updating tasks, set the following:

Table 6-5. Settings to restrict a user from updating tasks

Setting	Value	Description
License	(REMOVE) Project Management	Remove this license from users to prevent them from accessing projects and tasks.
Access Grant	(REMOVE) Project Mgmt: Update Tasks	Remove this access grant from users to prevent them from updating tasks in the My Tasks portlet.

To prevent users with Time Management licenses from logging time through HP Time Management, the project manager can change the HP Time Management integration setting on the project that determines who can log time. Alternatively, the project manager can turn off HP Time Management integration.

Overriding Project Security

Users who have the access grants listed in *Table 6-6* can view and edit any project.

Table 6-6. Settings to override request security

Setting	Value	Description
Access Grants	Project Mgmt: Edit All Projects	View and edit any project.
	Project Mgmt: View All Projects	View the detailed information on a restricted project on which the user is not an active participant.

7 Resource Management Security

In This Chapter:

Overview of Resource Management Security

This chapter addresses the data and process security related to Resource Management in PPM Center. Configuring data and process security typically involves configuring licenses, access grants, entity-level settings, and field-level settings. The following sections provide information about the settings required for to secure actions or data related to Resource Management features.

The screen and function access that access grants provide is cumulative. A user who belongs to three different security groups has access to the user interface and functionality provided to all three groups combined. Therefore, to restrict screen and feature access, you remove the user from any and all security groups that has that access.

To see all security groups that are assigned specific access grants, use the **Access Grants** tabs in the User window. You can then:

- Remove the user from the security group (using the **Security Group** tab in the User window).
- Remove the access grants from the security group (in the Security Group window). Do this only if no one in that security group requires the access that this access grant provides.

This chapter provides information on how to enable certain functions. By default, users are not expected to have access to or be able to modify information related to budgets, cost, resource pools, staffing profiles, or skills. The following sections provide instructions on how to enable the viewing and editing of these areas.

Working with Resources

Each user has an associated resource information page that is used to capture information about the user such as his title, direct manager, and work capacity.

Viewing Resource Information

To allow a user to view resource information, use the settings described in *Table 7-1*.

Table 7-1. Settings to allow users to view resource information

Setting	Value	Description
Access Grant (only one is required)	Resource Mgmt: View my personal resource info only	Lets users view only their own personal resource information.
	Resource Mgmt: View all resources	Lets users view any resource information in the system.

Modifying Resource Information

To allow a user to modify resource information, assign him one of the access grants listed in *Table 7-2*.

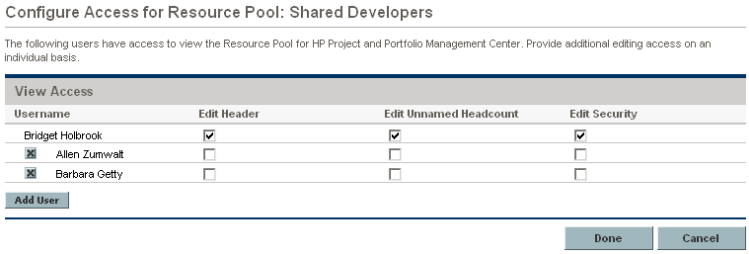
Table 7-2. Settings to allow users to modify resource information

Setting	Value	Description
Access Grant (only one is required)	Resource Mgmt: Edit only resources that I manage	Edit resource information for resources that list the current user as the Direct Manager. A resource's Direct Manager is displayed on the View Resource page.
	Resource Mgmt: Edit All Resources	Edit the resource information for any resource.

Working with Resource Pools

To control user actions on resource pools, use a combination of access grants and settings in the Configure Access for Resource Pool page, which is shown in *Figure 7-1*.

Figure 7-1. Configure Access for Resource Pool page



Viewing Resource Pools

To allow a user to modify resource pool information, use the settings listed in *Table 7-3*

Table 7-3. Settings to allow users to view resource pool information

Setting	Value	Description
Access Grant (only one is required)	Resource Mgmt: View Resource Pools	View resource pool information if the user has view access on the Configure Access for Resource Pool page.
	Resource Mgmt: View All Resource Pools	View resource pool information for all resource pools. **Note:** This grant provides unlimited view access to any resource pool. To provide more limited view access, consider using the Resource Mgmt: View Resource Pool access grant.
Configure Access for Resource Pool	View Access	Users who are included in the **View Access** list and have the Resource Mgmt: View Resource Pools access grant can view the resource pool information.

Creating Resource Pools

To allow a user to create resource pools, use the settings listed in *Table 7-4*.

Table 7-4. Settings to allow users to create resource pools

Setting	Value	Description
Access Grant	Resource Mgmt: Edit Resource Pools	Create a resource pool.
	Resource Mgmt: Edit All Resource Pools	Create a resource pool.
	Resource Mgmt: Create Resource Pools (required)	Create resource pools using the standard interface. The user must also have either the Resource Mgmt: Edit Resource Pools or Resource Mgmt: Edit All Resource Pools access grant.

Modifying Resource Pools

To allow a user to modify resource pool information, use the settings listed in *Table 7-5*.

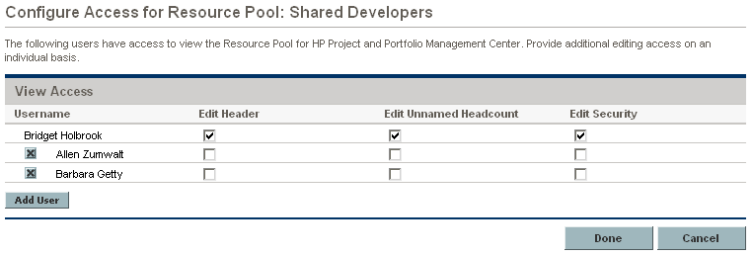
Table 7-5. Settings to allow users to modify resource pools (page 1 of 2)

Setting	Value	Description
Access Grant (only one is required)	Resource Mgmt: Edit All Resource Pools	Edit and delete any resource pool.
	Resource Mgmt: Edit Resource Pools	Edit resource pool information, if the user has been granted edit access on the Configure Access for Resource Pool page (*Figure 7-2*). Delete these resource pools if given sufficient access in the Configure Access for Resource Pool page for that resource pool.

Table 7-5. Settings to allow users to modify resource pools (page 2 of 2)

Setting	Value	Description
Additional Editing Access	Edit Basic Resource Pool Information	Used in conjunction with the Resource Mgmt: Edit Resource Pools access grant. Lets the user edit resource pool header fields and notes. The user cannot change the periods or any information in the **Resource Pool Breakdown** section.
	Edit Plan	Lets the user edit the periods and the information in the **Resource Pool Breakdown** section.
	Edit Security	Lets the user edit the list of users who can modify the resource pool using the Configure Access for Resource Pool page.

Figure 7-2. Configure Access for Resource Pool page



Working with Skills

Access to skills is controlled through access grants.

Viewing Skills

To enable a user to view skill information, assign the Resource Mgmt: View All Skills access grant.

Creating, Modifying, and Deleting Skills

To allow a user to modify any skills defined in PPM Center, assign the Resource Mgmt: Edit All Skills access grant.

Working with the Organization Model

Access to the organization model is set through access grants.

Viewing the Organization Model

To allow a user to view the organization model and organization unit detail pages in PPM Center, assign the Resource Mgmt: View Organization access grant.

Modifying Organization Definitions

To allow a user to modify organization information, assign one of the access grants listed in *Figure 7-6*.

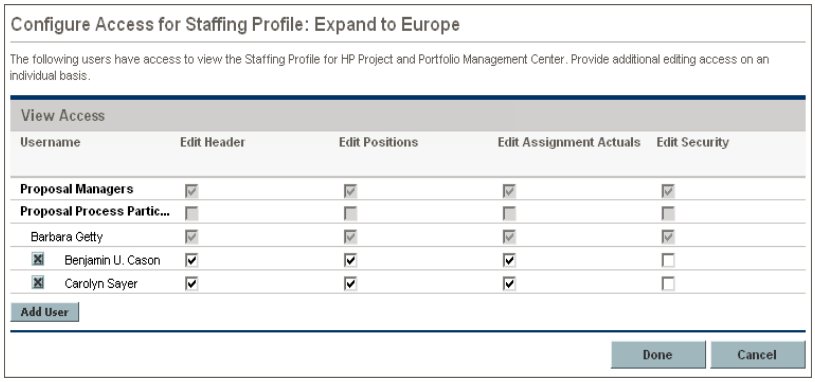
Table 7-6. Settings to modify organization information.

Setting	Value	Description
Access Grant (only one is required)	Resource Mgmt: Edit Entire Organization	Edit and delete any organization unit.
	Resource Mgmt: Edit Only Organization Units That I Manage	Edit organization unit information for units that list the current user as the manager in the View Organization Unit page. Also delete any of these organization units.

Working with Staffing Profiles

User actions relating to staffing profiles are controlled by a combination of access grants and settings in the Configure Access for Staffing Profile page, which is shown in *Figure 7-3*.

Figure 7-3. Configure Access for Staffing Profile page



Viewing Staffing Profiles

To allow a user to view staffing profile information, use the settings listed in *Table 7-7*.

Table 7-7. Settings to allow users to view resource pool information

Setting	Value	Description
Access Grant (only one is required)	Resource Mgmt: View Staffing Profiles	View staffing profile information if the user has view access on the Configure Access for Staffing Profile page.
	Resource Mgmt: View All Staffing Profiles	View staffing profiles information for all Staffing profiles. **Note:** This grant provides unlimited access to view any staffing profile. To provide more limited view access, consider using the Resource Mgmt: View Staffing Profiles grant.
Configure Access for Staffing Profile	View Access	Users included in the **View Access** list and who have the Resource Mgmt: View Staffing Profiles access grant can view the staffing profile information.

Creating Staffing Profiles

To allow a user to create a staffing profile, use the settings listed in *Table 7-8*.

Table 7-8. Settings to allow users to create staffing profiles

Setting	Value	Description
Access Grant	Resource Mgmt: Edit Staffing Profiles	Create a new staffing profile.
	Resource Mgmt: Edit All Staffing Profiles	Create a new staffing profile.
	Resource Mgmt: Create Staffing Profiles (required)	Create staffing profiles using the standard interface. The user must also have either the Resource Mgmt: Edit Staffing Profiles or Resource Mgmt: Edit All Staffing Profiles access grant.

Modifying Staffing Profiles

To allow a user to modify staffing profile information, use the settings listed in *Table 7-9*.

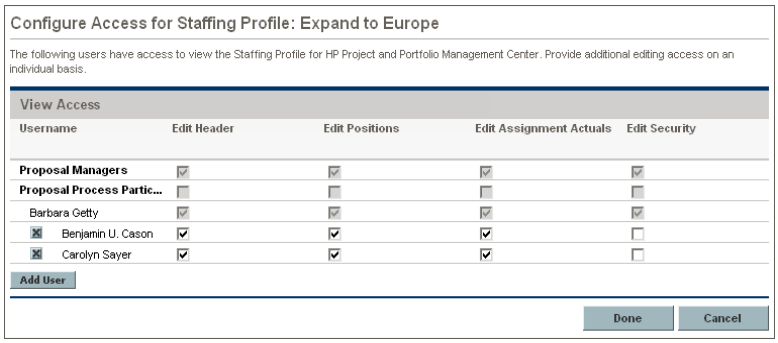
Table 7-9. Settings to allow users to modify staffing profiles (page 1 of 2)

Setting	Value	Description
Access Grant	Resource Mgmt: Edit All Staffing Profiles	Edit and delete any staffing profile.
	Resource Mgmt: Edit Staffing Profiles	Edit staffing profile information when the user has edit access to the Configure Access for Staffing Profile page. Delete these staffing profiles when given sufficient access in the Configure Access for Staffing Profile page for that staffing profile.

Table 7-9. Settings to allow users to modify staffing profiles (page 2 of 2)

Setting	Value	Description
Additional Editing Access	Edit Basic Staffing Profile Information	Used in conjunction with the Resource Mgmt: Edit Staffing Profiles access grant, lets the user edit staffing profile header fields and notes. The user cannot change the periods or any information in the **Staffing Profile Breakdown** section.
	Edit Plan and Actuals	Lets the user edit the Periods and the information in the **Staffing Profile Breakdown** section. Also lets users view and edit the planning and actuals data in the **Profile Allocation** table.
	Edit Actuals	Let the user edit the Periods and the information in the **Staffing Profile Breakdown** section. Also lets the user to view and edit the actuals data in the **Profile Allocation** table.
	Edit Security	Lets the user use the Configure Access for Staffing Profile page to edit the list of users who can modify the staffing profile.

Figure 7-4. Configure Access for Staffing Profile page



Working with Calendars

Regional calendars and resource calendars have separate sets of access grants. Access grants for regional calendars do not provide access to resource calendars, and vice versa.

Viewing and Editing Regional Calendars

To allow a user to view or edit regional calendars, use the settings listed in *Table 7-10*.

Table 7-10. Settings to allow users to view or edit regional calendars

Setting	Value	Description
Access Grant (only one is required)	Resource Mgmt: View Regional Calendars	Allows users to view regional calendars, but not resource calendars.
	Resource Mgmt: Edit Regional Calendars	Allows users to view and edit regional calendars. Does not provide the ability to view resource calendars.

Viewing and Editing Resource Calendars

To allow a user to view or modify calendar-related resource information, use the settings listed in *Table 7-11*.

Table 7-11. Settings to allow users to modify resource information

Setting	Value	Description
Access Grant (only one is required)	Resource Mgmt: Edit only resources that I manage	Lets a user edit resource information, including the regional and resource calendars, for resources that list the current user as the Direct Manager. The Direct Manager for a resource is displayed on the View Resource page.
	Resource Mgmt: Edit all resources	Lets a user edit the resource information, including the regional and resource calendar, for any resource.
	Resource Mgmt: Edit My Calendar	Lets a user edit his own resource calendar.
	Resource Mgmt: View all resources	Lets a user view the resource calendar for all resources.
	Resource Mgmt: View my personal resource info only	Lets a user view his own resource calendar, but not edit it.

Users must have a license for one of the following:

- Demand Management
- Project Management
- Program Management
- Portfolio Management
- System-Level Configuration

Additional Protection for Resource Information

This section addresses how users can gain unauthorized access to sensitive resource information (including billing rates), and how to prevent this unauthorized access.

Users Who Are Assigned the Configurator License

Users who have the Configuration license can create entities such as reports, and then use those entities to query the database for sensitive data. To prevent this activity, remove the Configuration license. For information about how to remove licenses from a user or set of users, see *Removing Licenses Using the Assign Licenses Wizard* on page 45.

Technically, users are not required to have the Configuration license in a production environment.

Members of Security Groups with View or Edit Access to Cost Data

Users who belong to a security group that is assigned either the Cost: View Project, Program, and Time Sheet Cost Data access grant or the Cost: Edit Work Plan Cost Data access grant, can see or edit skill rates, resource rates, or project costs. The user could divide the actual cost of a task by the actual effort to calculate the billing rate for a resource. Without one of these access grants, a user cannot see the actual cost of a task. Therefore, HP recommends that you remove these access grants from all security groups and assign them only to individual project managers.

Members of Security Groups with View or Edit Access to Resource Data

Users who belong to security groups with one of the following Resource Management access grants assigned to it can access the user attribute window and view all attributes except for cost:

- Resource Management: Edit All Resources
- Resource Management: Edit only resources that I manage
- Resource Management: View all resources
- Resource Management: View my personal resource info only

To prevent such unauthorized access to resource attributes, remove these access grants from all security groups, and assign them only to the users within Human Resources who are responsible for entering cost rate information into the system.

Users Who Have the Administrator Password

To migrate code from the development environment to the staging environment, and then to the production environment, the administrator password is required. A user with Administrator access can assign licenses or security groups to grant visibility to resource attributes. HP recommends that, in the staging and production environments, you give the “admin” user password only to an administrator level user within the IT organization.

Users Who Run the Unsecured "User Detail Report"

The User Detail Report queries the database for information, and then displays some user attributes. (It does not report on resource rate.) Because this report is not secured, anyone who runs it can potentially access sensitive resource information. To prevent this from occurring, secure this report to the “admin” user only and to Human Resources members.

Secure all reports to their intended audiences. For information about how to secure reports, see the *Reports Guide and Reference*.

Users with the Sys Admin: Server Tools - Execute SQL Runner Access Grant

Users who belong to a security group that has the Sys Admin: Server Tools - Execute SQL Runner access grant assigned, can access resource data by running database queries from the PPM Workbench. To ensure that this access grant is not misused, make sure that you link it only to the PPM Administrator security group, and to no other.

8 Cost and Budget Data Security

In This Chapter:

Overview of Cost and Budget Data Security

Configuring data and process security often involves setting licenses, access grants, entity-level settings, and field-level settings. This chapter addresses the data and process security related to financial functions (cost and budgets) in PPM Center.

By default, users cannot view or modify information related to budgets or cost. The following sections provide information on how to enable users to view and modify budget and cost information in PPM Center, as well as information on the settings required to secure the actions or data related to features in HP Financial Management.

The screen and function access that access grants provide is cumulative. A user who belongs to three different security groups has access to all of the user interface and functionality provided to the three groups combined. Therefore, to restrict certain screen and feature access, you remove the user from any security group that grants that access.

You can click the **Access Grants** tabs in the User window to see all of the security groups that have been given specific access grants. You can then:

- Remove the user from the security group (using the **Security Group** tab on the User window)
- Remove the access grants from the security group (in the Security Group window). Do this only if no one in that security group needs the access that the access grant provides.

Working with Cost Data

In PPM Center, cost data can be associated with tasks, projects, programs, resources, and skills.

Viewing Cost Data

To view cost information, a user must have the Financial Mgmt: View Project, Program, and Time Sheet Cost Data access grant. This grant lets the user view cost data related to tasks, projects, programs, resources, and skills. The user must also have view access to these entities.

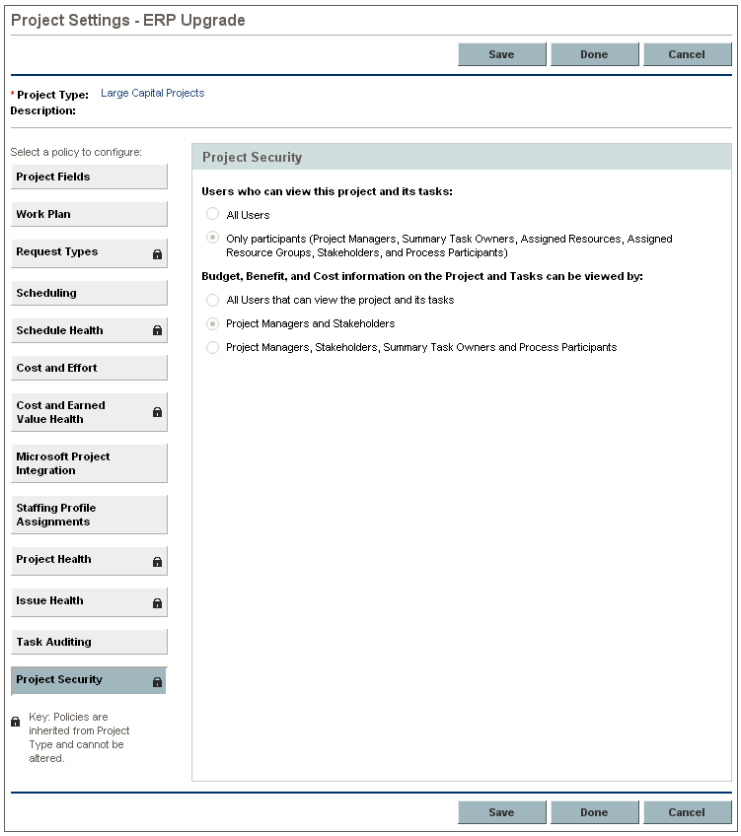
Making Project Cost Data Visible to Users

If Financial Management is enabled for a project, you can use the **Project Security** section of the Project Settings page (see *Figure 8-1* on page 111) to specify who can view cost information. You can make cost information on the project and tasks visible to one of the following user groups:

- All users who can view the project and its tasks
- Project managers and stakeholders
- Project managers, stakeholders, summary task owners and process participants

To change these settings in the Project Settings page, you must have the Financial Mgmt: Edit Cost Security access grant.

Figure 8-1. Project Security section of the Project Settings page



Users in the selected group can access the **Cost and Effort** and the **Cost and Earned Value Health** sections of the Project Settings page.

You can use a combination of security settings and access grants to provide a granular level view of cost data. You could, for instance, provide all users with cost data access, but provide just a subset of those users with the Financial Mgmt: View Project, Program, and Time Sheet Cost Data access grant.

Making Program Cost Data Visible to Users

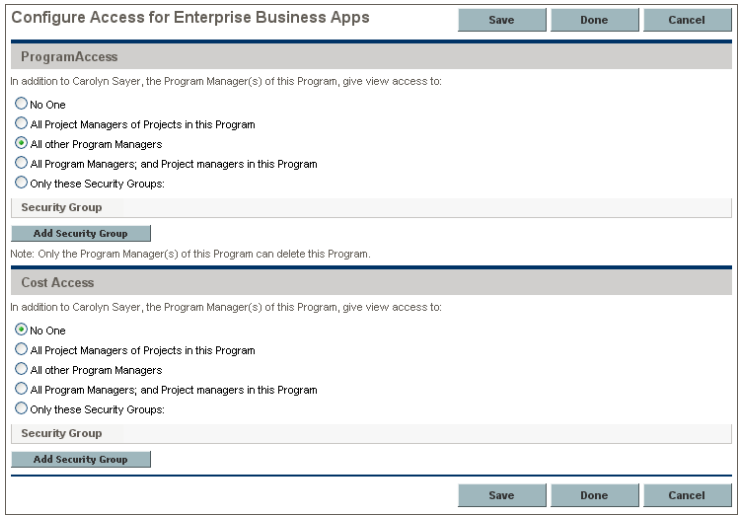
If Financial Management is enabled for a program, you can specify who can view the related cost information. (Enable Financial Management in the **Financial Management Settings** section at the top of the Program Settings page.)

On the Configure Access page, which is shown in *Figure 8-2*, you can make program cost information available to one of the following user groups:

- Only the program manager
- All project managers of projects in this program
- All other program managers
- All program managers; and project managers in this program
- Only specified security groups

To change these settings on the Configure Access page, you must have the Financial Mgmt: Edit Cost Security access grant.

Figure 8-2. Configure Access page for programs



Modifying Cost Data

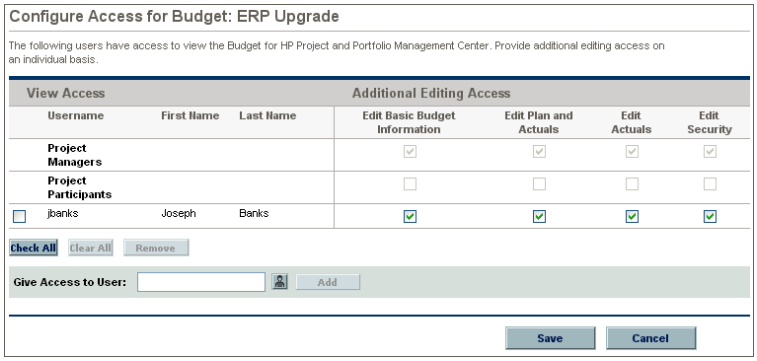
To modify cost data, users must have the Financial Mgmt: Edit Work Plan Cost Data access grant. This grant lets the user edit cost data related to tasks, projects, programs, resources, and skills. The user must also have the required permission to access these entities.

For information on how to allow users to view cost information, see *Viewing Cost Data* on page 110.

Working with Budgets

To enable users to view, create, or modify budgets, use a combination of access grants and settings on the Configure Access for Budget page, which is shown in *Figure 8-3*.

Figure 8-3. Configure Access for Budget page



Viewing Budgets

To allow a user to view a budget, use the settings listed in *Table 8-1*.

Table 8-1. Settings to view budget information

Setting	Value	Description
Access Grant (only one is required)	Financial Mgmt: View Budgets	Lets a user with view access to the Configure Access for Budget page to view budget information.
	Financial Mgmt: View All Budgets	Lets a user view budget information for all budgets. **Note:** This grant provides unlimited view access to any budget. To provide more limited view access, consider using Financial Mgmt: View Budgets.
Configure Access for Budgets	View Access	Users included in the View Access list and have the View Budgets access grant can view the budget information.

Creating Budgets

To allow a user to create a budget, use the settings listed in *Table 8-2*.

Table 8-2. Settings to create budgets

Setting	Value	Description
Access Grant	Financial Mgmt: Edit Budgets	Allows the user to edit any particular budget that also grants that user edit access on its Configure Access page (**Additional Editing Access** fields).
	Financial Mgmt: Edit All Budgets	Allows the user to edit any budget in the system.
	Financial Mgmt: Create Budgets (required)	Create budgets using the standard interface. To perform this function, the user must also have either the Financial Mgmt: Edit Budgets or Financial Mgmt: Edit All Budgets access grant.

Modifying Budgets

To allow users to modify budget information, use the settings on the Configure Access for Budget page shown in *Figure 8-4* on page 116. These settings are described in *Table 8-3*.

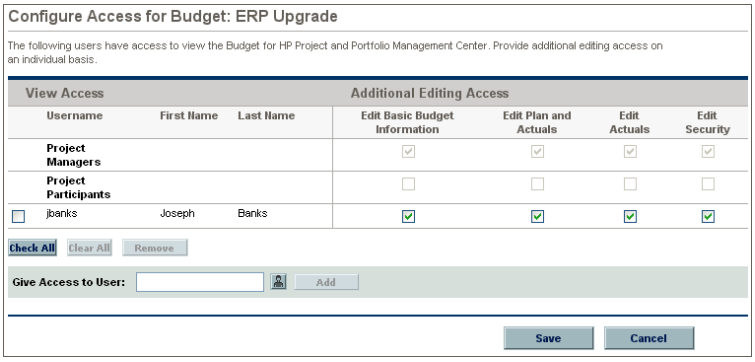
Table 8-3. Settings to allow users to modify budgets (page 1 of 2)

Setting	Value	Description
Access Grant (only one is required)	Financial Mgmt: Edit All Budgets	Edit and delete any budget.
	Financial Mgmt: Edit Budgets	Edit budget information when the user has been granted edit access in the Configure Access for Budget page. Delete these budgets when given sufficient access in the Configure Access for Budget page for that budget.

Table 8-3. Settings to allow users to modify budgets (page 2 of 2)

Setting	Value	Description
Additional Editing Access	Edit Basic Budget Information	Used in conjunction with the Financial Mgmt: Edit Budgets access grant, lets the user edit budget header fields, user data, and notes. The user cannot change the Periods or any information in the **Budget Breakdown** section.
	Edit Plan and Actuals	Used in conjunction with the Financial Mgmt: Edit Budgets access grant, lets the user edit the Periods and the information in the **Budget Breakdown** section. Also lets the user view and edit the planning and actuals data in the **Budget Breakdown** table.
	Edit Actuals	Used in conjunction with the Financial Mgmt: Edit Budgets access grant, lets the user edit the Periods and the information in the **Budget Breakdown** section. Also lets user view and edit actuals data in the **Budget Breakdown** table.
	Edit Security	Used in conjunction with the Financial Mgmt: Edit Budgets access grant, lets the user edit the list of users who can use the Configure Access for Budget page (*Figure 8-4*) to modify the budgets.

Figure 8-4. Configure Access for Budget page



Working with Activities

You can configure users to view, create, or modify activities. These actions are controlled by access grants.

Viewing Activities

To allow a user to view activity information, assign the Config: View Activities access grant.

Creating and Modifying Activities

To allow a user to create, modify, or delete activities, assign the Config: Edit Activities access grant.

Working with Regions

To allow users to view, create, or modify regions, assign the access grants listed in *Table 8-4*.

Table 8-4. Access grants for working with regions

To allow user to	Access Grant	Description
View regions	Resource Mgmt: View Regions	Lets users view region information.
Create or modify regions	Resource Mgmt: Edit Regions	Lets users view, create, edit, or delete regions.

Working with Financial Exchange Rates and Currencies

To control who can view, create, or modify financial exchange (FX) rates, you use the same access grants that you use to control who can modify currency. *Table 8-5* lists these access grants.

Table 8-5. Access grants for working with financial exchange rates

To allow user to	Access Grant	Description
View financial exchange rate information	Financial Mgmt: View Financial Exchange Rates	Lets users view financial exchange rate information.
Create or modify financial exchange rate	Financial Mgmt: Edit Financial Exchange Rates	Lets users view, create, edit, or delete financial exchange rates.

9 PPM Dashboard Security

In This Chapter:

Controlling User Access to Portlets in the PPM Dashboard

The PPM Dashboard gives users access to PPM Center data through the portlets (system and custom) displayed on their PPM Dashboard pages. To control user access to any portlet, you specify which users can access it. You can also control user access to a custom portlet by disabling the portlet. (You cannot disable a system portlet.) This section provides details on how to do both.

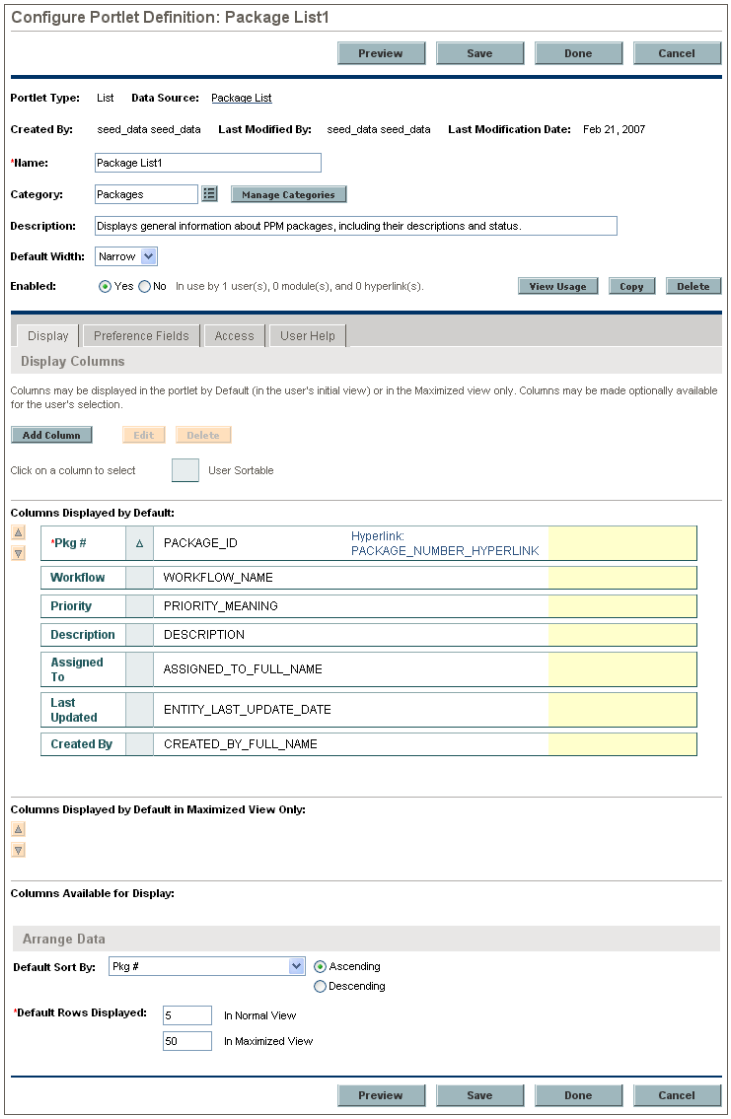
For information about how to configure security for PPM Dashboard modules, see the *Creating Portlets and Modules* guide.

Disabling Custom Portlets

Although you cannot disable built-in system portlets in PPM Center, you can disable portlets customized for your site.

To disable a custom portlet:

1. In the standard interface, select **Administration > Portlet Definitions > Configure Portlet Definitions.**
2. On the Configure Portlet Definitions page, search for, and then open the custom portlet that you want to disable.



3. In the portlet description area at the top of the page, next to **Enabled,** select **No.**

   Disabling the portlet deletes it from all PPM Dashboard pages that previously displayed them.

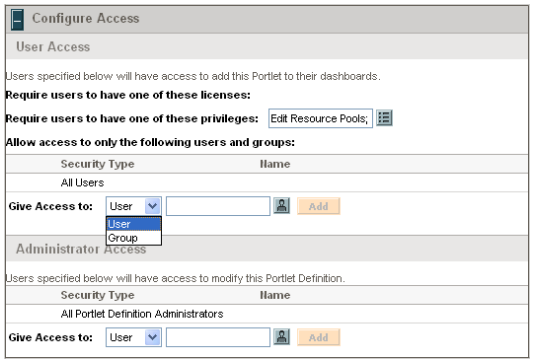
4. Click **Save.**

Restricting User Access

You can control who can add a system or custom portlet to their PPM Dashboard. For example, you may want to restrict the package-related portlets to members involved in deployments. Enabling only the portlets that a specific user needs makes it easier for that user to personalize his own PPM Dashboard because there are fewer irrelevant portlets from which to choose.

To specify which users can use a portlet on their PPM Dashboard:

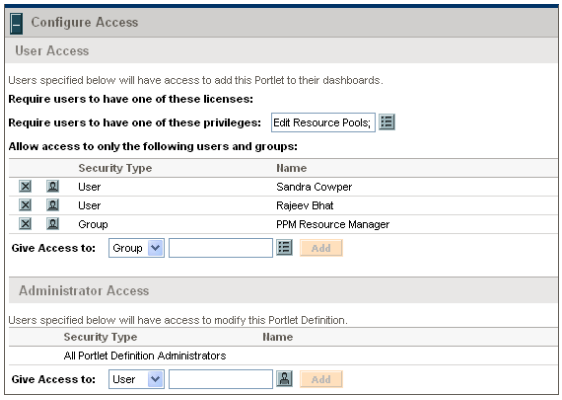
1. In the standard interface, select **Administration > Portlet Definitions > Configure Portlet Definitions.**
2. On the Configure Portlet Definitions page, search for, and then open the portlet definition to configure.
3. Scroll to the **Configure Access** section.



4. In the **User Access** subsection, in the **Give Access to** list, select **User** or **Group.**
5. Select the users or security groups.

6. Click **Add.**

   The selections are listed in the **Configure Access** section.



7. Click **Save.**

You can restrict access by specifying multiple security groups and users for each portlet. Only members of the specified security group or the specified users can add this portlet to their PPM Dashboard.

You can also restrict access by choosing a specific license or access grant from the **Require users to have one of these licenses/privileges** fields. Only users who have the required licenses or access grants can add this portlet to the PPM Dashboard.

Restricting Data to Participants

The PPM Dashboard respects any participant restrictions configured for requests, packages, and projects. If these items are restricted, only users who are directly involved with them can view associated data on the PPM Dashboard. Restricted items are not displayed in portlets or returned in searches.

The participant-restriction model is supported by all PPM Center system portlets. Custom portlets are not supported. They display the information specified in the SQL query that defines the portlet.

10 Configuration Security

In This Chapter:

Overview of Configuration Security

To configure security for PPM Center configuration entities, you can specify who has permission to:

- Change a workflow
- Change each object type
- Change request types
- Change user and security group definitions

Setting Ownership for Configuration Entities

Different groups of users in PPM Center have ownership and control over the configuration entities. These groups are referred to as *ownership groups*. Unless global permission has been provided to all users for an entity, ownership group members are the only users who can edit, delete, or copy that entity. To complete those tasks, the ownership groups must also have the required access grant for the entity. For example, a user must have the Config: Edit Workflows access grant to edit workflows and workflow steps.

You can assign multiple ownership groups to the various entities. Ownership groups are defined in the Security Group window. Security groups become ownership groups when used in the ownership capacity.

You can specify ownership groups for the following entities involved in your process:

- Environments
- Environment groups
- Object types
- Report types
- Request header types
- Request types
- Security groups
- Special commands
- User definitions

- Validations
- Workflows
- Workflow steps

The ownership setting is accessed through the individual entity windows in the Workflow Workbench.

For example, to set the ownership for a workflow:

1. Log on to PPM Center.
2. From the menu bar, select **Administration > Open Workbench.**

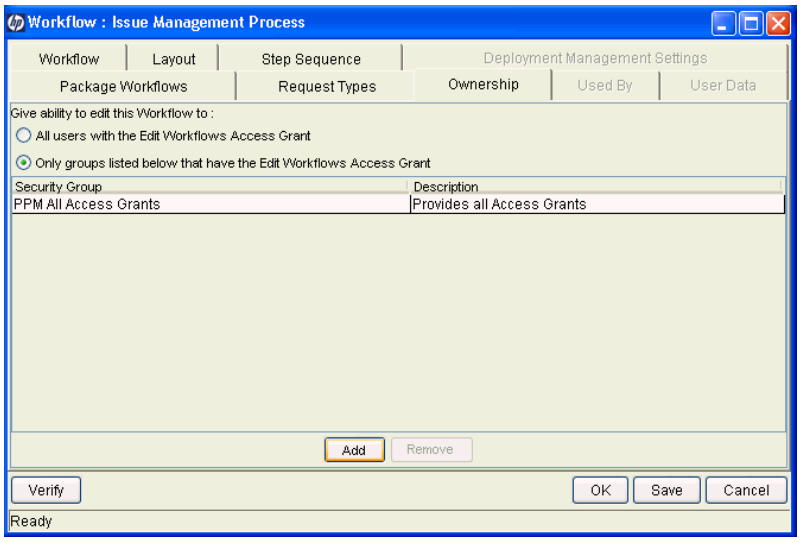
   The PPM Workbench opens.
3. From the shortcut bar, select **Configuration > Workflows.**

   The Workflow Workbench opens.
4. Click **List.**
5. On the **Results** tab, in the **Workflow Name** column, double-click the name of a workflow for which you want to configure ownership.

   The Workflow window opens to the **Layout** tab.
6. Click the **Ownership** tab.
7. Click **Only groups listed below that have the Edit Workflows Access Grant.**
8. Click **Add.**

   The Add Security Group window opens.
9. Select one or more security groups.
10. Do one of the following:
    - To add the current security group and continue adding security groups, click **Add.**
    - To add the current security group and close the window, click **OK.**

On the **Ownership** tab, the **Security Group** column lists the security group(s) you selected.



11. Do one of the following:

    - To save the selection and close the Workflow window, click **OK.**
    - To save the selection and leave the Workflow window open, click **Save.**

The System: Ownership Override access grant lets the user access and edit configuration entities, even if that user does not belong to the ownership groups associated with the entities. Assign this access grant only to high-level users who may be required to configure processes for multiple groups.

Removing Access Grants

You can also restrict the ability to modify configuration entities by removing the user from any security group that grants that access.

Use the **Access Grants** tabs in the User window to see all security groups where specific access grants are included. You can do one of the following:

- Remove the user from the security group (using the **Security Group** tab in the User window).
- Remove the access grants from the security group (in the Security Group window).

Do this only if no one in that security group needs what this access grant provides.

Table 10-1 lists the access grants that provide users with edit access to various PPM Center configuration entities.

Table 10-1. Access grants for editing configuration entities (page 1 of 2)

Category	Access Grant Name	Description
Config	Edit Activities	View, create, edit, or delete activities in the PPM Dashboard.
Config	Edit Notification Templates	Create, edit, and delete notification templates in the Notification Templates Workbench.
Config	Edit Report Types	Create, edit, and delete report types in the Report Types Workbench.
Config	Edit Special Commands	Create, edit, and delete special commands in the Special Command Workbench.
Config	Edit User Data	Create, edit, and delete user data definitions in the User Data Workbench.
Config	Edit Validation Values	Create, edit, and delete validation values in the Validation Workbench.
Config	Edit Validations	Create, edit, and delete validations in the Validation Workbench.
Config	Edit Workflows	Create, edit, and delete workflows in the Workflows Workbench.

Table 10-1. Access grants for editing configuration entities (page 2 of 2)

Category	Access Grant Name	Description
Demand Mgmt	Edit Request Header Types	Create, edit, and delete request header types in the Request Header Types Workbench.
Demand Mgmt	Edit Request Types	Create, edit, and delete request types in the Request Types Workbench.
Deployment Mgmt	Edit Object Types	Create, edit, and delete object types in the Object Types Workbench.
Environments	Edit Environments	Create, edit, and delete environments in the Environments Workbench.
Sys Admin	Configure Modules	Create and configure Modules, which are then used to distribute PPM Dashboard pages.
Sys Admin	Edit Security Groups	Create, edit, and delete security groups in the Security Groups Workbench.
Sys Admin	Edit Users	Create, edit, and delete users in the Users Workbench.
System	Edit Portlet Definition	Create, edit, and delete portlets in the Portlets Workbench.
Time Mgmt	Edit Charge Codes	Create, edit, and delete charge codes in the Charge Codes Workbench.
Time Mgmt	Edit Override Rules	Create, edit, and delete override rules in the Override Rules Workbench.
Time Mgmt	Edit Time Sheet Policies	Create, edit, and delete policies in the Time Sheet Policies Workbench.

11 Service Provider Functionality

In This Chapter:

Recommended Practice: Service Provider Functionality

HP recommends that, for your organization, you create a group of PPM Center users that no users in the system outside of this group can modify. This prevents these users from being locked out of the system and ensures that they always maintain a specific set of access rights.

To configure your PPM Center instance to use this "super-user" functionality, perform the following steps:

Step 1. Create a service provider user.

To create a service provider user:

1. Log on to PPM Center with administrator privileges.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Sys Admin > Users.**

   The User Workbench opens.
4. Click **New User.**

   The User window opens to the **User Information** tab.
5. In the **Username** box, type a name like `Restricted User 1.`
6. Enter values in all required fields (displayed in red text).
7. In the **System Level Licenses** section, select the **Configuration** and **User Administration** checkboxes.
8. Click **OK.**

Step 2. Create the service provider security group.

To create the service provider security group:

1. From the PPM Workbench shortcut bar, select **Sys Admin > Security Groups.**
2. Click **New Security Group.**

   The Security Group window opens to the **Users** tab.

3. In the **Name** box, type `Restricted Users.`

The name Restricted Users is not mandatory. You can enter a different name for this security group.

4. Next to **Enabled,** select **Yes.**
5. On the **Users** tab, click **Add New User to this Group.**

   The Users dialog box opens.
6. Select the Restricted User 1 user you created in step 1 to this security group, and then click **Add.**
7. Click the **Access Grants** tab, and then assign the following access grants to this security group.
   - Sys Admin: Edit Users
   - Sys Admin: Edit Security Groups

Ensure that the user has all of the access grants required to open the PPM Workbench, and to create, edit, and delete users and security groups.

8. Click **OK.**

Step 3. Set ownership on the user.

To set ownership on the user:

1. From the PPM Workbench shortcut bar, select **Sys Admin > Users.**

   The User Workbench opens.
2. Locate and open the Restricted User 1 user record.
3. Click the **Ownership** tab.
4. Under **Give ability to edit this User to,** select **Only groups listed below that have the Edit Users access grant.**
5. Click **Add.**

   The Add Security Group window opens.
6. Locate and select the Restricted Users security group.
7. Click **OK.**
8. Click **Save.**

Step 4. Set ownership on the security group.

To set ownership on the security group:

1. From the PPM Workbench shortcut bar, select **Sys Admin > Security Groups.**

   The Security Group Workbench opens.

2. Locate and open the Restricted Users security group record.
3. The Security Group: Restricted Users window opens.
4. Click the **Ownership** tab.
5. Click the **Ownership** tab.
6. Under **Give ability to edit this Security Group to,** select **Only Groups listed below that have the Edit Security Groups Access Grant.**
7. Click **Add.**
8. Locate and select the Restricted Users security group.
9. Click **Add.**
10. Click **Save.**

Step 5: Add a server configuration parameter.

To add a server configuration parameter:

1. Open the `<PPM_Home> server.conf` file in a text editor such as Notepad.
2. Add the following line to the file:

   ```
   com.kintana.core.server.SERVICE_PROVIDER_SECURITY_
   GROUP=Restricted Users
   ```

   The `server.conf` parameter value is case-sensitive. So, for example, if the security group name is Restricted Users, and if you add the line `com.kintana.core.server.SERVICE_PROVIDER_SECURITY_ GROUP=RESTRICTED Users` to the server.conf file, then the security restriction does not work.

3. Save the `server.conf` file.
4. Restart the PPM Server.

Step 6. Test the functionality.

To test the functionality of the new user group:

1. Log on to PPM Center as an administrator, and check to ensure that you *cannot* edit the Restricted User 1 user or the Restricted Users security group.
2. Log on to PPM Center as Restricted User 1, and ensure that you *can* edit the Restricted User 1 user and the Restricted Users security group.

Step 7. Create another user to assign to the Restricted Users security group.

To create another user to assign to the Restricted Users group:

1. After you perform steps 1 through 6, log on to PPM Center as Restricted User 1.
2. From the menu bar, select **Administration > Open Workbench.**

   The PPM Workbench opens.
3. From the shortcut bar, select **Sys Admin > Users.**

   The User Workbench opens.
4. Click **List.**
5. On the **Results** tab, in the **Username** column, locate and click **Restricted User 1.**
6. Click **Copy.**

   The Copy User window opens.
7. Enter a new user name and password, and then confirm the password.
8. Click **OK.**

   The User Workbench prompts you to indicate whether you want to edit the user.
9. Click **No.**

The new user has the same licenses, access grants, and security group association as Restricted User 1 has.

A Access Grants

Access grants enable certain activities within PPM Center. PPM Center comes with predefined access grants. Installing an HP Deployment Management Extension may introduce additional access grants. *Table A-1* on page 137 lists the available access grants and provides a description of each.

View access grants provide read-only access to screens and entities. Users who do not have a view access grant cannot see certain workbenches and windows.

Edit access grants typically enable a user to view, create, modify, and delete entities in certain circumstances. For example, if you have the Edit Requests access grant, you can delete requests that you have created.

For details on specific access grants, see *Table A-1* on page 137.

Table A-1. Access grants (page 1 of 15)

Category	Access Grant Name	Description
Config	Edit Activities	Modify activities in the Activities Workbench.
Config	Edit Notification Templates	Create, update, and delete notification templates in the Notification Templates Workbench.
Config	Edit Report Types	Create, update, and delete report types in the Report Types Workbench.
Config	Edit Special Commands	Create, update, and delete special commands in the Special Command Workbench.
Config	Edit User Data	Create, update, and delete user data definitions in the User Data Workbench.
Config	Edit Validation Values	Create, update, and delete validation values in the Validations Workbench.
Config	Edit Validations	Create, update, and delete validations in the Validation Workbench.
Config	Edit Workflows	Generate, update, and delete workflows in the Workflows Workbench.
Config	View Activities	View activities in the Activities Workbench.
Config	View Notification Templates	View notification template definitions in the Notification Templates Workbench.

Table A-1. Access grants (page 2 of 15)

Category	Access Grant Name	Description
Config	View Report Types	View report type definitions in the Report Types Workbench.
Config	View Special Commands	View special command definitions in the Special Command Workbench.
Config	View User Data	View user data definitions in the User Data Workbench.
Config	View Validations	View validations in the Validations Workbench.
Config	View Workflows	View workflow definitions in the Workflows Workbench.
Demand Mgmt	Access Request Query Builder	Use the request query builder on the Search Requests page.
Demand Mgmt	Change Request Type	Change the request type for existing requests.
Demand Mgmt	Edit All Contacts	Edit and delete contacts using the Contact Workbench.
Demand Mgmt	Edit All Requests	Perform advanced request processing actions: creating, editing, deleting, changing the request's workflow, and overriding references. ■ User always has permission to edit the request. ■ Override and/or remove any references on any request. ■ User always has permission to delete or cancel a request. ■ User can change the workflow when creating and editing a request.
Demand Mgmt	Edit Contacts	Create and update contacts in the Contact Workbench.
Demand Mgmt	Edit Demand	Access the Demand Management scheduling functions, the consolidated picture of demand, and all other Demand Management menu items related to scheduling or managing demand.

Table A-1. Access grants (page 3 of 15)

Category	Access Grant Name	Description
Demand Mgmt	Edit Request Header Types	Create, update, and delete request header types in the Request Header Types Workbench.
Demand Mgmt	Edit Request Types	Create, update, and delete request types in the Request Types Workbench.
Demand Mgmt	Edit Requests	Perform basic request processing actions: create requests, edit certain requests, and delete requests that you have not submitted. ■ Allows the user to generate requests. ■ User cannot change the workflow when creating or editing a request. ■ Allows the user to edit the request as specified on the **User Access** tab in the Request Type window. ■ Allows the user to delete the request as specified on the **User Access** tab in the Request Type window. ■ Allows the user to cancel the request as specified on the **User Access** tab in the Request Type window.
Demand Mgmt	Override Demand Mgmt Participant Restriction	Allows the user to review a request regardless of whether the user is allowed to view as defined on the request type's **User Access** tab.
Demand Mgmt	View All Contacts in Request	View all contacts in a request, even if a company is associated with the request.
Demand Mgmt	View Contacts	View the contact definition in the Contact Workbench.
Demand Mgmt	View Request Header Types	View request header type definitions in the Request Header Types Workbench.
Demand Mgmt	View Request Types	View the request type definition in the Request Types Workbench.

Table A-1. Access grants (page 4 of 15)

Category	Access Grant Name	Description
Demand Mgmt	View Requests	View requests in the Request Types Workbench.
Deployment Mgmt	Edit All Packages	Edit or delete any packages.
Deployment Mgmt	Edit All Releases	Create, edit and delete any release using the Releases Workbench. A user with this grant can: ■ Create a release ■ Be designated as the release manager in the Release window ■ Edit or delete any release in PPM Center (regardless of whether he is specified as the release manager in the Release Management window).
Deployment Mgmt	Edit Object Types	Create, edit, and delete object types in the Object Types Workbench.
Deployment Mgmt	Edit Packages	Perform basic package processing actions: create, edit certain related packages, and delete certain packages that have not been submitted. ■ To edit the package, user must be its creator, the “assigned to” user, a member of the assigned group or a member of the workflow step’s security group. ■ User cannot delete a package if it has been released or if user is not the owner.

Table A-1. Access grants (page 5 of 15)

Category	Access Grant Name	Description
Deployment Mgmt	Edit Releases	Perform basic release processing actions in the Releases Workbench: create, edit, process, and delete certain related releases. A user with this grant can: ■ View any release ■ Be designated as the release manager ■ Create releases ■ Edit or delete any release that he created ■ Act on any distribution workflow steps where he is included in the step security. ■ Edit or delete a release that he did not create (only if he is designated as the release manager in the Release Management window).
Deployment Mgmt	Override Deployment Mgmt Participant Restriction	View detailed information on a restricted package for which the user is not an active participant.
Deployment Mgmt	Submit Environment Refreshes	Create and submit an environment refresh in the Env Refresh Workbench.
Deployment Mgmt	View Environment Refreshes	View environment refresh definitions in the Env Refresh Workbench.
Deployment Mgmt	View Object Types	View object type definitions in the Object Types Workbench.
Deployment Mgmt	View Packages	View packages in the standard interface or the Package Workbench.
Deployment Mgmt	View Releases	View release definitions in the Releases Workbench. Act on any distribution workflow steps that include the user in the step security.
Environments	Edit Environments	Create, update and delete environments in the Environment Workbench.
Environments	View Environments	View environment definitions in the Environment Workbench.

Table A-1. Access grants (page 6 of 15)

Category	Access Grant Name	Description
Financial Mgmt	Approve Budgets	Change the **Budget Status** value on the Modify Budget page to **Approved.** The user must also have the Update Budgets Status grant and either the Edit Budget or Edit All Budgets grant to perform this function. Note that **Approved** is available in the **Budget Status** list only if you have this grant.
Financial Mgmt	Create Budgets	Create budgets using the standard interface. The user must also have either the Edit Budgets or Edit All Budgets grant to perform this function.
Financial Mgmt	Create Financial Benefits	The user can create new financial benefits. This grant is supplemental to the Edit Financial Benefits or Edit All Financial Benefits access grant.
Financial Mgmt	Edit All Budgets	The user can edit all budgets in the system.
Financial Mgmt	Edit All Financial Benefits	The user can edit all financial benefit in the system.
Financial Mgmt	Edit Budgets	Edit budget information if the user has been granted edit access on the Configure Access for Budget page.
Financial Mgmt	Edit Cost Rate Rules	Create, edit, and delete cost rate rules.
Financial Mgmt	Edit Cost Security	Edit cost security settings for a project in the Project Settings window. Edit cost security settings for a program on the Program Security Configuration page. **Note:** For this grant to be relevant, the user must also be able to edit the project settings and program security.
Financial Mgmt	Edit Financial Benefits	The user can edit any financial benefit for which he is on the specified Edit list.
Financial Mgmt	Edit Financial Exchange Rates	Create and update financial exchange rates.

Table A-1. Access grants (page 7 of 15)

Category	Access Grant Name	Description
Financial Mgmt	Edit Work Plan Cost Data	Edit cost data related to tasks, projects, programs, resources and skills. The user must also have access to edit these entities.
Financial Mgmt	Update Budget Status	Change the **Budget Status** value on the Modify Budget page. The user must also have either the Edit Budgets or Edit All Budgets grant to do this.
Financial Mgmt	Update Financial Benefit Status	The user can update the Financial Benefit Status, but nothing else. Supplemental to the Edit Financial Benefits or Edit All Financial Benefits access grant.
Financial Mgmt	View All Budgets	View budget information for all budgets in PPM Center.
Financial Mgmt	View All Financial Benefits	The user can view any financial benefit in the system.
Financial Mgmt	View Budgets	View budget information when the user has been granted view access on the Configure Access for Budget page.
Financial Mgmt	View Cost Rate Rules	View cost rate rules on the Cost Rate Rules page.
Financial Mgmt	View Financial Benefits	The user can view any financial benefit for which he is on the specified **View** or **Edit** list.
Financial Mgmt	View Financial Exchange Rates	The user can view financial exchange rates.
Financial Mgmt	View Project, Program, and Time Sheet Cost Data	View cost data related to tasks, projects, programs, resources, and skills. The user must also have access to view these entities.
PMO	Edit All Programs	Create and update any program.
PMO	Edit Programs	Update programs where the user is specified as the program manager.
PMO	View Programs	View program definitions.

Table A-1. Access grants (page 8 of 15)

Category	Access Grant Name	Description
Portfolio Mgmt	Configure Portfolio Management	Gives the user access to the Configure Portfolio Management page where he can set portfolio tracking and categorization metrics.
Portfolio Mgmt	Edit All Scenario Comparisons	View, edit, and delete any scenario comparisons in the system, and create new scenario comparisons.
Portfolio Mgmt	Edit Scenario Comparison	The user can view, edit, and delete any scenario comparison for which he is on the specified **Edit** list, and can create new scenario comparisons.
Portfolio Mgmt	Portfolio Manager	Provides the user with access to the following additional Portfolio Management portlets and visualizations: ■ Portfolio by Category ■ Current Portfolio Map ■ View Current Portfolio ■ Resource by Category
Portfolio Mgmt	View Scenario Comparison	The user can view any scenario comparison for which he is on the specified **View** or **Edit** list.
Project Mgmt	Create Projects	Create projects through the standard interface. The user must also have either the Project Mgmt: Edit Projects or Project Mgmt: Edit All Projects access grant.
Project Mgmt	Edit All Projects	Edit all projects, even if the user does not otherwise meet the participant restrictions on the project. This includes the ability to perform functions reserved for the project manager.
Project Mgmt	Delete Projects	Delete projects that do not have actuals logged. The user must also have the Project Mgmt: Edit Projects access grant and be assigned as a project manager on the project, or have the Project Mgmt: Edit All Projects grant.

Table A-1. Access grants (page 9 of 15)

Category	Access Grant Name	Description
Project Mgmt	Delete Projects with Actuals	Delete projects, even if actuals have been logged. The user must also have the Project Mgmt: Delete Projects and associated access grants.
Project Mgmt	Edit Project Types	Create, edit and delete project types. Editing can be further restricted through ownership controls defined in the project type.
Project Mgmt	Edit Projects	Edit projects and work plans. If the users is editing project-level fields and the project process, any security defined on the project process request type and workflow is enforced. **Note:** Some functions are limited to the project managers for the project. These are: ■ Modify settings ■ Modify participant groups ■ Override the overall project health ■ Create, edit, schedule, or delete the project work plan ■ Create the project staffing profile from the project overview page (also requires access grants for this entity) ■ Create the project budget from the project overview page (also requires access grants for this entity) ■ Create, delete, and set the active work plan baselines (requires additional grants) ■ Delete projects (requires additional grants)
Project Mgmt	Edit Work Plan Templates	Create and edit work plan templates. Editing can be further restricted through ownership controls defined in the work plan template.

Table A-1. Access grants (page 10 of 15)

Category	Access Grant Name	Description
Project Mgmt	Manage All Work Plan Baselines	Create, update, delete, and set work plan baselines active for any project the user can view, even if the user is not a project manager for the project.
Project Mgmt	Manage Work Plan Baselines	Create, update, delete, and set work plan baselines as active. The user must also be the project manager for the project and have either the Edit Projects access grant, or the Edit All Projects access grant.
Project Mgmt	Synchronize Work Plans	Integrate work plans between Microsoft® Project and PPM Center.
Project Mgmt	View All Projects	View all projects, even if the user does not otherwise meet the participant restrictions on the project.
Project Mgmt	Update Tasks	Allows assigned resources to update their work plan tasks through the My Tasks portlet.
Project Mgmt	View Project Types	View project types.
Project Mgmt	View Projects	View projects for which the user meets defined participant restrictions.
Project Mgmt	View Work Plan Templates	View work plan templates.
Resource Mgmt	Create Resource Pools	Create resource pools using the standard interface. The user must also have either the Resource Mgmt: Edit Resource Pools or Resource Mgmt: Edit All Resource Pools grant.
Resource Mgmt	Create Staffing Profiles	Create staffing profiles using the standard interface. The user must also have either the Resource Mgmt: Edit Staffing Profiles or Resource Mgmt: Edit All Staffing Profiles grant.
Resource Mgmt	Edit All Resource Pools	Edit or delete any resource pool.
Resource Mgmt	Edit All Resources	Edit the resource information for any resource defined in PPM Center.

Table A-1. Access grants (page 11 of 15)

Category	Access Grant Name	Description
Resource Mgmt	Edit All Roles	Create, edit, and delete all roles defined in PPM Center.
Resource Mgmt	Edit All Skills	Create, edit, and delete all skills defined in PPM Center.
Resource Mgmt	Edit All Staffing Profiles	Allows the user to edit or delete any staffing profile in the system.
Resource Mgmt	Edit Entire Organization	Edit and delete any organization unit.
Resource Mgmt	Edit My Calendar	A user who also has the View All Resources access grant can edit his or her own calendar information.
Resource Mgmt	Edit Only Organization Units That I Manage	Edit organization unit information for units that list the current user as the manager in the View Organization Unit page. Also delete any of these organization units.
Resource Mgmt	Edit only resources that I manage	Edit resource information for resources that list the current user as the Direct Manager. A resource's Direct Manager is displayed on the View Resource page.
Resource Mgmt	Edit Regional Calendars	Create, edit, and delete regional calendars defined in PPM Center.
Resource Mgmt	Edit Resource Pools	Edit resource pool information if the user has been granted edit access on the Configure Access for Resource Pool page. Delete these resource pools if given sufficient access on the Configure Access for Resource Pool page for that resource pool.
Resource Mgmt	Edit Staffing Profiles	Edit staffing profile information if the user has been granted edit access on the Configure Access for Staffing Profile page. Delete these staffing profiles if given sufficient access on the Configure Access for Staffing Profile page for that staffing profile.

Table A-1. Access grants (page 12 of 15)

Category	Access Grant Name	Description
Resource Mgmt	Edit Regions	Create, edit, and delete all regions defined in PPM Center. The user must also have the Configuration license to use this grant.
Resource Mgmt	Update Staffing Profile Status	Change the Staffing Profile Status value on the Modify Staffing Profile page. To use this grant, the user must also have either the Edit Staffing Profiles or Edit All Staffing Profiles grant.
Resource Mgmt	View All Resource Pools	View resource pool information for all resource pools.
Resource Mgmt	View All Resources	View the resource information page for any resource defined in PPM Center.
Resource Mgmt	View All Roles	View all roles defined in PPM Center.
Resource Mgmt	View All Skills	View all skills defined in PPM Center.
Resource Mgmt	View All Staffing Profiles	Allows the user to view any staffing profile in the system.
Resource Mgmt	View my personal resource info only	View only the user's own resource information page.
Resource Mgmt	View Organization	View the organization model and organization unit detail pages.
Resource Mgmt	View Regional Calendars	View all regional calendars defined in PPM Center.
Resource Mgmt	View Regions	View all regions defined in PPM Center.
Resource Mgmt	View Resource Pools	View resource pool information if the user has been granted view access on the Configure Access for Resource Pool page.
Resource Mgmt	View Staffing Profiles	View staffing profile information if the user has been granted view access on the Configure Access for Staffing Profile page.

Table A-1. Access grants (page 13 of 15)

Category	Access Grant Name	Description
Sys Admin	Configure Modules	Create, edit, and delete modules on Module Configuration in the PPM Dashboard page. View and set the default dashboard on the Set Default Dashboard in the PPM Dashboard page.
Sys Admin	Distribute Modules	View, publish, and distribute modules, pages and portlets to PPM Dashboards on the Distributing Modules Dashboard page.
Sys Admin	Edit Security Groups	Create, update, and delete security groups in the Security Groups Workbench. The user must also have the Edit Users access grant.
Sys Admin	Edit Users	Create, update, and delete users in the Users Workbench.
Sys Admin	Migrate PPM Objects	Migrate configuration objects (such as workflows and request types) using the Migrators.
Sys Admin	Server Administrator	Stop the PPM Server, log on to the application when the server is started in restricted mode, and send messages via kWall.sh.
Sys Admin	Server Tools: Execute Admin Tools	Execute administration reports in the Admin Tools window and view the SQL Runner window in the Server Tools Workbench.
Sys Admin	Server Tools: Execute SQL Runner	Execute SQL statements in the SQL Runner window and view the Admin Tools window in the Server Tools Workbench.
Sys Admin	Synchronize Meta Layer	Perform reporting meta layer synchronizations using the Report Types Workbench.
Sys Admin	View Security Groups	View security group definitions in the Security Groups Workbench.
Sys Admin	View Server Tools	View the SQL Runner and Admin Tools screens in the Server Tools Workbench.

Table A-1. Access grants (page 14 of 15)

Category	Access Grant Name	Description
Sys Admin	View Users	View user definitions in the Users Workbench.
System	Edit Dependent References	Create and edit dependency relationships between entities and their references.
System	Edit Portlet Definition	Create, edit, and delete portlets in the Portlets Workbench.
System	Edit All Reports	Use the Reports Workbench to delete any submitted report.
System	Override Document Check Out	Override document check out.
System	Override Key Fields Segmentation	View all information contained in restricted key fields. Key fields include: ■ **Resource** and **Resource Group** fields in HP Project Management tasks ■ **Assigned User, Assigned Group** and **Contacts** fields in HP Demand Management requests ■ **Assigned User** and **Assigned Group** fields in HP Deployment Management packages
System	Ownership Override	Access and edit all configuration entities even if the user is not a member of one of the entity's ownership groups.
System	Submit Reports	Submit reports in PPM Center.
System	View Portlet Definition	View portlet definitions in the Portlets Workbench.
Time Mgmt	Approve Time Sheets	Approve or reject time sheets if the resource is a direct report or if the time sheet has been delegated to the user.
Time Mgmt	Close Time Sheets	Close or freeze time sheets if the resource is a direct report or if the time sheet has been delegated to the user.

Table A-1. Access grants (page 15 of 15)

Category	Access Grant Name	Description
Time Mgmt	Edit Charge Codes	Create, modify, and delete charge codes in the Charge Codes Workbench.
Time Mgmt	Edit Override Rules	Create, modify, and delete override rules in the Override Rules Workbench.
Time Mgmt	Edit Resource Time Mgmt Settings	Makes the **Time Management** tab visible to Resource Management users.
Time Mgmt	Edit Time Sheet Policies	Create, modify, and delete time sheet policies in the Time Sheet Policy Workbench.
Time Mgmt	Edit Time Sheets	Edit time sheets if the resource is a direct report or if the time sheet has been delegated to the user.
Time Mgmt	Edit Work Allocations	View and edit work allocations. The user can also close or delete allocations he created.
Time Mgmt	Edit All Work Allocations	View, edit, delete, and close any work allocation.
Time Mgmt	View All Time Sheets (Summary Info Only)	View only summary info for all time sheets.
Time Mgmt	View Charge Codes	View charge code definitions in the Charge Code Workbench.
Time Mgmt	View Override Rules	View override rules in the Override Rules Workbench.
Time Mgmt	View Time Sheet Policies	View time sheet policies.
Time Mgmt	View Time Sheets	View time sheet information for a user.
Time Mgmt	View Work Allocations	View work allocations in Time Management.

B License Types

In This Appendix:

License Types

To log on to PPM Center, a user must have a license. PPM Center offers three types of user licenses: Product, Configuration, and User Administrator. Each license type is designed to suit different business needs and responsibilities, and, therefore, grants a different set of functionality. This appendix addresses the license types available for PPM Center.

- Product licenses

  Product licenses are for users who require basic product features and access to data. Product licenses provide access to PPM Center features in the standard (HTML) interface, including the PPM Dashboard, and the PPM Workbench, depending on the product license used.

  The product licenses are as follows:

  - Demand Management
  - Project Management
  - Program Management (requires Demand Management and Project Management licenses)
  - Portfolio Management (requires Demand Management license)
  - Deployment Management
  - Time Management

- PPM Configuration license

  The PPM Configuration license provides access to all product features through both the PPM Workbench and the standard interface. It gives access to all product features available to a product license user, as well as more advanced configuration functionality through the PPM Workbench. For example, a user with the Configuration license does not require the Project Management Product license to perform the tasks associated with project management.

- PPM User Administrator license

  The PPM User Administrator license is for users responsible for administering PPM Center users and security, as well as the application itself. You must have this license to configure user accounts and security groups, and to run reports related to importing new users through the Open Interface. This license also provides access to the system administration functionality of the PPM Center licensed at your site.

User access to screens and functions in PPM Center are controlled by a combination of license and access grants. The following sections address only the licenses required to perform specific tasks. For additional details on access grants, which are also required, see Appendix A, *Access Grants,* on page 137.

Deployment Management Extension Licenses

HP Deployment Management Extension licenses are provided for an entire site; that is, they are not assigned to individual users. Extension licenses enable additional screens and fields in PPM Center. For details, see the documentation for the Extensions installed at your site.

C Licenses and User Roles

This appendix addresses the typical user functions and required licenses by user types and by product/license type. *Table C-1* on page 157 lists the licenses required by, and recommended for, different types of users. *Table C-2* on page 160 lists the user roles and functions based on product/license types.

Table C-1. Product licenses by user type (page 1 of 3)

User Type	Tasks	Required and Recommended () Licenses (Unless noted with an asterisk*, these are product licenses.)
Business User	Submit requests, monitor status of own requests, and provide user sign-off.	■ Demand Management
Business Project Manager	Create, plan, and monitor project workplans—update tasks; assign resources; schedule, define project exception rules; set notifications; maintain project templates, manage scope changes, issues, and risk. Manage resource skills, pools, profiles, and capacity. Manage project budget and expenses. Synchronize with Microsoft Project.	■ Demand Management ■ Program Management ■ Project Management ■ (Time Management)
Business Analyst	Monitor initiative (schedule and cost) status; act on SLA exceptions; track issues; manage scope changes, issues, and risk. Manage portfolio.	■ Demand Management ■ Portfolio Management ■ Program Management ■ Project Management
Business Manager	Monitor initiative (schedule, cost, earned value) status, act on SLA exceptions, prioritize portfolio.	■ Demand Management ■ Portfolio Management ■ Program Management ■ Project Management

Table C-1. Product licenses by user type (page 2 of 3)

User Type	Tasks	Required and Recommended () Licenses (Unless noted with an asterisk*, these are product licenses.)
IT Management: CIOs, IT VPs, Directors, Enterprise Architects, CTOs	Monitor status of initiatives (schedule and cost), drill down on SA exceptions, control and prioritize portfolio. Monitor resource use. Manage resource capacity and IT budgets.	■ Demand Management ■ Portfolio Management ■ Program Management ■ Project Management ■ (Time Management) ■ (Deployment Management)
Process and Project participants: IT Support Analyst, QA, team member, Change Control	Participate in project tasks and in request processes. Execute project tasks and update task status. Actively resolve requests—update request information, perform approvals, assign requests, prioritize requests, move requests through the workflow.	■ Demand Management ■ Project Management ■ (Time Management)
Engineering Team: Developer, Infra-structure (DBA / Sysadmin / Web Admin), Release Manager, Operations	Create packages, update package information, perform approvals, schedule and execute migrations. Update tasks. Create and manage deployment releases.	■ Deployment Management
Portfolio Manager, Program Manager, IT Controller	Manage portfolio. Manage rating and prioritization of projects. Perform what-if portfolio scenarios. Manage scope changes, issues, and risk. Manage resource skills, pools, profiles, and capacity. Manage project budget and expenses.	■ Demand Management ■ Portfolio Management ■ Program Management ■ Project Management ■ (Time Management)

Table C-1. Product licenses by user type (page 3 of 3)

User Type	Tasks	Required and Recommended () Licenses (Unless noted with an asterisk*, these are product licenses.)
Project Manager	Create, plan, and monitor project workplans—update tasks, assign resources, schedule, define project exception rules, set notifications, maintain project templates. Manage resource skills, pools, profiles, and capacity. Manage project budget and expenses. Synchronize with Microsoft Project (if required).	■ Project Management ■ (Time Management)
PPM Center User Administrator	Common administration functions, including set up users and assign security.	■ Demand Management, PPM User Administration license*
PPM Center Administrator, Process Owner / Implementer	Common administration functions such as configure user-defined project information, and configure report types and PPM Dashboard portlets. Configure object types, model process workflows; and configure business rules.	■ Demand Management, PPM Configuration license*

Table C-2. User roles and functions by product license type (page 1 of 5)

Product	License Type	User Type	Primary Tasks Performed with this License Type
PPM Dashboard	Any	All	Overall visibility of status and metrics, drill down to a specific level of detail on requests, task, projects, and packages requiring action or further review.
HP Demand Management	Configuration	IT Process Analyst	Configure workflows and request types.
	Project Management	Project Manager, Resource Manager	Create and manage resource pools and project resource profiles. Manage resource capacity and use. Create and manage budgets for departments, programs, and projects.
	Demand Management	Business User, Requestor	Submit requests, monitor the status of own request, and provide user sign-off.
		Analyst, IT Support Staff, Request Contact	Participate in the request processes and actively resolve requests—update request information, perform approvals, assign requests, prioritize requests, move requests through the workflow.
		Upper-level Manager, Business Analyst, Change Control Team, Project Manager, Program Manager	Monitor SLAs and act on exceptions, run reports, and perform approvals. Prioritize demand, assign requests. participate in deployment management.

Table C-2. User roles and functions by product license type (page 2 of 5)

Product	License Type	User Type	Primary Tasks Performed with this License Type
HP Portfolio Management	Portfolio Management	Portfolio Manager, Business Analyst, Program Manager, Enterprise Architect, CTO, IT Controller	Manage IT portfolio. Explore what-if scenarios. Evaluate value and mix of current and proposed projects. Rank and rate projects. Create and manage resource pools and project resource profiles. Manage resource capacity and utilization. Create and manage budgets for departments, programs, and projects. Track and compare actuals to budgets, perform earned value analysis.
HP Program Management	Program Management	Program Manager	Prioritize programs and projects. Manage program and project initiation; monitor resource utilization; monitor program status, scope changes, issues, and risk. Act on exceptions.

Table C-2. User roles and functions by product license type (page 3 of 5)

Product	License Type	User Type	Primary Tasks Performed with this License Type
HP Project Management	Project Management	Project Manager, Project Lead	Create, plan, and monitor project workplans—update milestones, baselines, tasks; assign resources; schedule, define project exception rules; set notifications; maintain project templates. Monitor status and critical path. Define resource and regional calendars.
		Project Manager, Resource Manager	Create and manage resource pols and project resource profiles. Manage resource capacity and utilization. Create and manage budgets for departments, programs, and projects. Define resource and regional calendars.
		Project Administrator	Configure user-defined project information/fields, define project notifications. Define resource and regional calendars.
		Upper-Level Manager, Other Stakeholder, Program Manager	Monitor project status and drill down on exceptions. Track and compare actuals to budgets, perform earned value analysis.
HP Resource Management	Project Management, Demand Management	IT Manager, Project Manager, IT HR	Base functionality is included with the PPM Center Foundation. IT supports creating, viewing, updating, and assigning: skills, resource details (capacity, rate, utilizations, availability), and organization model.
		Portfolio Manager, Program Manager, Project Manager	Create and update resource pools and staffing profiles.

Table C-2. User roles and functions by product license type (page 4 of 5)

Product	License Type	User Type	Primary Tasks Performed with this License Type
HP Time Management	Time Management	Staff	Enter time sheets by hour or time against work items.
		Manager	Review, freeze, and approve timesheets. Close, cancel timesheets. Delegate functions. Compare work item budgets versus actuals.
		Time Management Analyst	Establish work allocations and charging rules by work item, department, job/role. Configure start-end dates and periods, and approval hierarchies.
HP Financial Management	Project Management, Demand Management	All Users	Base functionality is included with the PPM Center Foundation and supports the ability to view budgets and associated visualizations.
	Portfolio Management, Program Management, or Project Management	Portfolio Manager, Program Manager, Project Manager	Create and update budgets.
		IT Manager, Portfolio Manager, Program Manager, Project Manager, Business Analyst	Display earned value analysis information and visualization.

Table C-2. User roles and functions by product license type (page 5 of 5)

Product	License Type	User Type	Primary Tasks Performed with this License Type
HP Deployment Management	Deployment Management	Developer	Create and update packages for deployment, monitor package status.
		DBA, System Administrator, Configuration Manager, Tech. Project Lead, Release Manager	Create packages, update package information, perform approvals, schedule and execute migrations. Create, manage, and perform deployment releases. Assign packages to developers.
	Configuration	Release Mgmt Analyst	Configure object types and workflows.
	Deployment Management	IT Manager, QA and Business Analyst	View that status of deployment packages and perform QA approvals.
All Products	User Admin	PPM Center Administrator	Set up users, manage licenses, assign security.
All Products	Configuration	PPM Center Configurator	Create and configure report types, portlets, request types, request header types, object types, workflows, environments, validations, activities. Configure security for standard portlets.

Index

S

T

U

W