Mercury IT Governance Center™

Security Model
Guide and Reference

Version: 6.0

MERCURY™

Mercury
379 North Whisman Road
Mountain View, CA 94043
Tel: (650) 603-5200
Toll Free: (800) TEST-911
Customer Support: (877) TEST-HLP
Fax: (650) 603-5300

If you have any comments or suggestions regarding this document, please send email to documentation@mercury.com.

Publication Number: ITG60Security1104A

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

In This Chapter:

About This Document

This document details the features that can be used to control user access to certain data and functions in the Mercury IT Governance Center™. Using a combination of license allocations, access grants, and other security-related features, you can limit user access to product screens, fields, and functionality. This document presents an overview of the data security model and provides instructions for controlling access to different entities.

Each chapter covers a particular topic:

- Chapter 1, *Introduction*, on page 11

  Includes an overview of the Mercury IT Governance Center security model, and details the document's intended audience and related guides.

- Chapter 2, *Users and Security Groups*, on page 17

  Provides instructions for creating users and providing them with screen and function access to the Mercury IT Governance Center.

- Chapter 3, *Managing Your Mercury IT Governance Licenses*, on page 35

  Provides instructions for assigning licenses to users. This includes assigning licenses on a user by user basis as well as assigning licenses simultaneously to a group of users.

- Chapter 4, *Request Security*, on page 43

  Discusses security settings and permissions related to creating, processing, and managing requests in Mercury Demand Management™.

- Chapter 5, *Package Security*, on page 65

  Discusses security settings and permissions related to creating, processing, and managing packages in Mercury Change Management™.

- Chapter 6, *Project and Task Security*, on page 73

  Discusses security settings and permissions related to creating, processing, and managing projects in Mercury Project Management™.

- Chapter 7, *Resource Management Security*, on page 81

  Discusses security settings and permissions related to Mercury Resource Management™.

- Chapter 8, *Cost and Budget Data Security*, on page 93

  Discusses security settings and permissions related to the financial management functionality in Mercury IT Governance Center.

- Chapter 9, *Dashboard Security*, on page 103

  Discusses security settings and permissions related to the the Mercury IT Governance Dashboard™.

- Chapter 10, *Configuration Security*, on page 109

  Discusses security settings and permissions related to configuring Mercury IT Governance Center.

- Appendix A: *Access Grants* on page 115

  Lists the access grants used to control user access to specific features and screens.

- Appendix B: *License Types* on page 127

  Discusses the user access provided by each license.

- Appendix C: *Licenses and User Roles* on page 131

  A more granular look at licenses, this appendix breaks down this information by:

  - Product license by user type
  - User roles and functions by product and license type

Who Should Read This Document

This document is for the following audience types:

- Application administrators
- Application developers or configurators
- System or instance administrators
- Database administrators

Related Documents

Related documents for this book are:

- *Guide to Documentation*
- *Key Concepts*
- All user guides
- All configuration guides

For More Information

For information about these documents and how to access them, see the *Guide to Documentation*.

Overview of Mercury IT Governance Center Security Model

Businesses often need to control access to certain information and business processes. This can be done to protect sensitive information, such as employee salaries, or to simplify business processes by hiding data that is irrelevant to the user. Mercury IT Governance Center includes a set of features to help control data and process security on the following levels:

- Limiting who can access certain windows or pages.
- Limiting who can view or edit certain fields.
- Limiting the data displayed in sensitive fields or screens.
- Limiting which users can view, create, edit, or process Mercury IT Governance entities (requests, packages, projects, portfolios, programs, and so forth.).
- Limiting which users can view, create, or edit configuration entities (workflow, request types, object types, security groups, and so forth).
- Limiting which users can alter the security settings.

The following devices control the data and process security in Mercury IT Governance Center. These features can be combined in a number of ways to provide a secure system:

- **Licenses**

  Each user is assigned a license that provides them with the option to be granted basic access to a set of Mercury IT Governance product-related screens and functions. Licenses dictate available behavior but need to be used in conjunction with access grants to enable specific fields and functions. For example, a user with a Demand Management license, but without any access grants, can log onto the system, but will not be able to create any requests.

- **Access Grants**

  Linked to users through security groups, access grants define which windows and functions users can view, edit or perform actions in. Access grants also provide varying levels of control over certain entities and fields.

- **Entity-level restrictions**

  Settings on the entity that specify who can create, edit, process, and delete Mercury IT Governance entities (such as requests, packages or projects). You can also control which request types and object types can be used with certain workflows. These restrictions are often configured in the configuration entities (workflow, request type, object type, and so forth).

- **Field-level restrictions**

  For each custom field that you define in the Mercury IT Governance Center, you can configure when it is visible or editable. For some fields, you can additionally specify which users can view or edit the field.

- **Configuration-level restrictions**

  You can specify, using ownership groups settings, which users can modify configuration entities in the system. For example, you can control who is allowed to edit an existing workflow. This allows you to guarantee that only appropriate users are altering your Mercury IT Governance–controlled processes.

Chapter

2

Users and Security Groups

In This Chapter:

Overview of Users and Security Groups

This chapter provides instructions for creating Mercury IT Governance Center users and providing them with appropriate screen and function access.

Creating Users

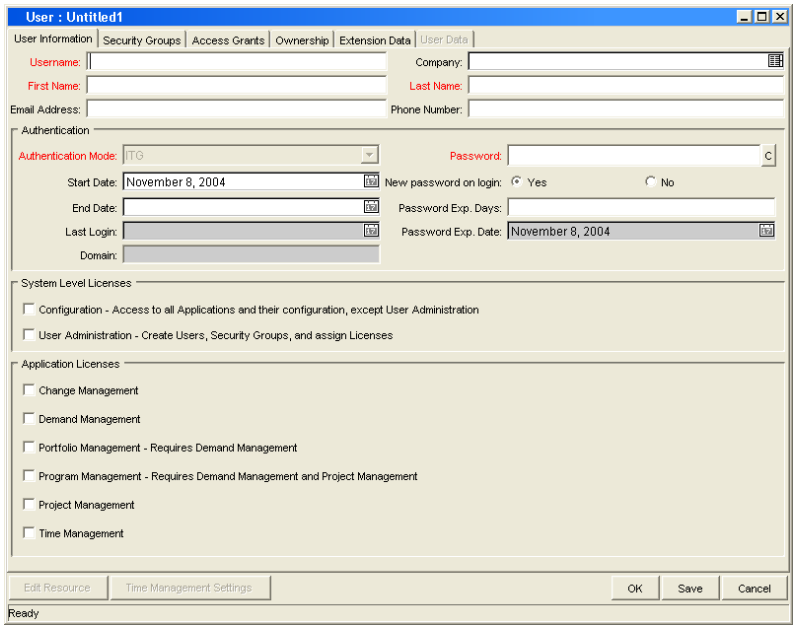
Mercury IT Governance Center users are created and defined in the User Workbench. Enterprises with a large number of users can use additional methods of user creation. For example, it is possible to import user information from other existing databases into interface tables, and then directly into the Mercury IT Governance Center database. Similarly, users can be imported from an LDAP server, through the interface tables, into the application.

Creating a User–Process Overview

To create a new user:

1. Click **New User** on the User Workbench or select **File > New > User.**

   The User window opens.



2. Enter the following required information: Username, First Name, and Last Name.

   The username must be unique in Mercury IT Governance Center.

3. Enter the general information in the appropriate fields.

   Refer to *Table 2-1* for a detailed description of each field on the **User Information** tab.

4. Create a password for the user.

   a. Click the button to the right of the required Password field.

      The Enter or Change Password window opens.

   b. Enter a password in the Enter New Password field, and confirm in the Confirm New Password field.

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

   c. Click **OK** to close the window.

5. Specify when the password will expire using either of the following methods:

   - Select **Yes** for New password on login to force the user to reset the password.
   - Use the Password Exp. Days field to specify the number of days that a user has to change the password. When a value is entered in this field, the Password Exp. Date field is automatically updated.

6. Select a method for the user's authentication from the Authentication Mode field.

   Possible values are **ITG, LDAP, NTLM,** and **SITEMINDER.** If **ITG** is chosen, then authentication is performed using the internal User Database of Mercury IT Governance Center. If another authentication mode is chosen, authentication is performed using the enterprise directory database server. This field's behavior can be set in the `server.conf` file by modifying the AUTHENTICATION_MODE parameter.

7. To give the user a user administrator license, select the User Administration checkbox.

   Selecting this option provides this user with access to all user configuration functionality for the products licensed at your site. The User Administration license is required to configure user accounts and security groups.

8. From the System Level Licenses and Application Licenses sections, select the products and license types to associate with the user.

   The Application Licenses provide access to the applications indicated. The **Configuration** license provides access to all product functionality available through the Workbench and HTML interfaces. For more detailed information, see *Managing Your Mercury IT Governance Licenses* on page 35. Users without an application license checked will not see that product's shortcut groups or menu items.

   Tip: You can assign licenses to multiple users using the License Workbench. See *Managing Your Mercury IT Governance Licenses* on page 35 for details.

9. In the **Security Groups** tab, link the desired security groups to the user to specify the user's functional roles and access grants. See *Linking Users to Security Groups* on page 23 for instructions.

10. In the **Ownership Groups** tab, select the ownership groups who will have the right to edit, copy or disable this user. See *Setting Ownership for Configuration Entities* on page 110.

11. Click **OK.**

    The new user can now log onto Mercury IT Governance Center using the username and password.

Table 2-1. User window: User Information tab fields

Fields	Definition
Username	Unique name for a user's account. The name entered to log onto Mercury IT Governance Center.
Company	The company the user works for. The values in this auto-complete list are set by the following validation: CRT - Company.
First Name	The first name of the specified user.

Table 2-1. User window: User Information tab fields [continued]

Fields	Definition
Last Name	The last name of the specified user.
Email Address	The email address for a user. This address is referenced in other portions of the application and should be formatted as name@domain.com.
Phone Number	The phone number for the user.
Authentication Mode	A list of the methods available for authentication. Possible values are **ITG, LDAP, NTLM,** and **SITEMINDER.** If **ITG** is chosen, then authentication is performed using the internal User Database of Mercury IT Governance Center. If another authentication mode is chosen, authentication is performed using the enterprise directory database server. See the *Open Interface Guide and Reference* for details.
Start Date	The date when a user account becomes activated.
End Date	The date on which a user account becomes disabled. You can leave this field blank to indicate no end date.
Last Login	The date of a user's last system logon. This date is deleted based on a parameter in the server.conf file, DAYS_TO_KEEP_LOGON_ATTEMPT_ROWS. 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 has not been changed from the default to another value). See the *System Administration Guide and Reference* for server.conf parameter details.
Domain	Used only when using NTLM authentication. This can be set in the `<ITG_HOME>/integration/ntlm/ntlm.conf` file.
Password	The user's password. Administrators can set restrictions on the password format: minimum length, required special characters, etc. These restrictions are specified in the `server.conf` file on the Mercury IT Governance Center Server. See the *System Administration Guide and Reference* for `server.conf` parameter details.
New Password on Logon	Setting to determine whether to ask a user to enter a new password the next time they logon.
Password Exp. Days	The number of days before a user's password expires. The first time a user logs on after the password expiration date, he will be prompted to enter a new password.

Table 2-1. User window: User Information tab fields [continued]

Fields	Definition
Password Exp. Date	The date on which a user's password expires. The value in this non-updateable field is calculated by the Password Expiration Days attribute or the Ask New Password On Logon attribute.
Configuration	Selecting this option provides this user with access to all functionality for the products licensed at your site, including configuration interfaces for all Mercury IT Governance entities (e.g. object types, request types, workflows, and validations) except users and security groups.
User Administration	The User Administration license is required to configure user accounts and security groups.
Change Management	The Change Management license provides access to all product functionality available through the Workbench interface and additional access to advanced HTML interface functions. Users that do not have this box checked will not see the Change Mgmt screen group or associated menus.
Demand Management	The Demand Management license provides access to all product functionality. Users that do not have this box checked will not see the Demand Mgmt screen group or associated 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 that do not have this box checked will not see the related menus and can not access the functionality.
Program Management	Select the Program Management license to enable user access to Program Management functions, and must be used in conjunction with a Demand Management and Project Management license. Users that do not have this box checked will not see the related menus and can not access the functionality.
Project Management	The Project Management license provides access to all Project, Resource, and Financial Management functionality available through the Workbench interface and additional access to advanced HTML interface functions. Users that do not have this box checked will not see the Project Mgmt screen group or associated menus.
Time Management	Select Time Management license to enable user access to Time Management functions in Mercury IT Governance Center. Users that do not have this box checked will not see the related menus and can not access the functionality.

Table 2-1. User window: User Information tab fields [continued]

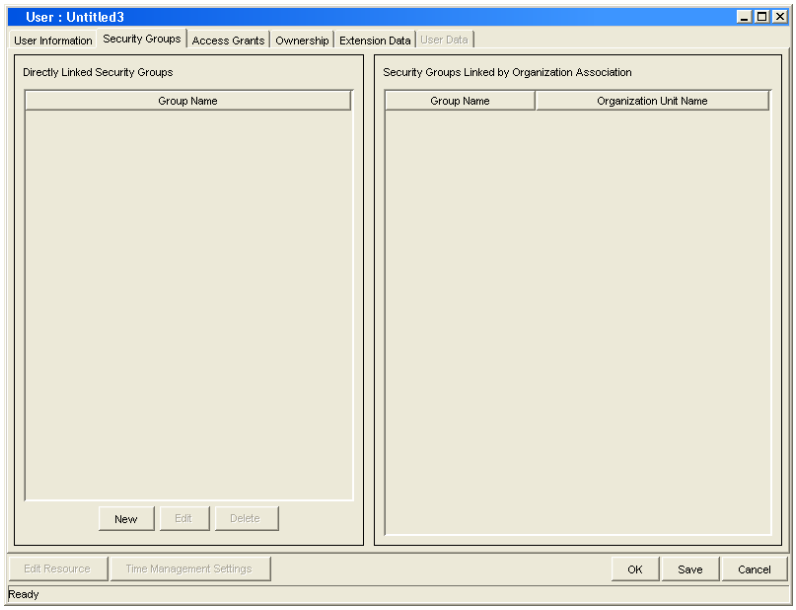
Fields	Definition
Edit Resource	Each user also has associated resource settings such as Title, Direct Manager, and Capacity. Click this button to view or edit the resource settings associated with the user.
Time Management Settings	If Time Management is licensed for a particular user, click this button to configure their time management settings. This includes defining the period type and time sheet approvers.

Linking Users to Security Groups

Users can be linked to security groups through the **Security Groups** tab of the User window. Users can also be linked to security groups through an organization model defined in Mercury IT Governance Center.

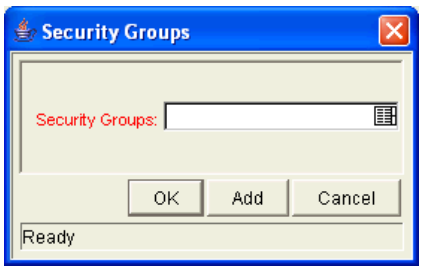
To link a user to a security group using the User window:

1. Open the User window.
2. Click the **Security Groups** tab.



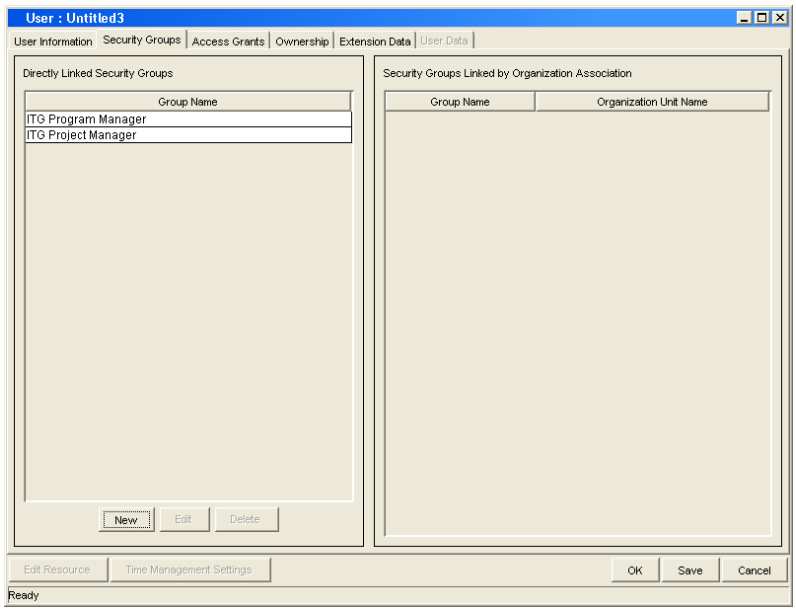
3. Click **New.**

   The Security Groups window opens.



4. From the Security Groups field, select the security groups that you would like to link to the user.

5. Click **OK** to add the list of security groups to the User window.



6. Click **Save** to save the user information.

Note

If the user is associated with an organization unit (defined in the Mercury Resource Management™ functionality), he may inherit security group associations. These security groups will be listed in the **Security Groups** tab in the Security Groups Linked by Organization Association list.

See the *Mercury Resource Management User's Guide* for details.

Configure the User's Resource Information

A resource is a person who performs work tracked by Mercury IT Governance Center. Resources can include employees, contractors, managers, or any other category your organization may need. Each user is considered a resource in Mercury IT Governance Center. For each user, you can capture information specific to that resource, such as:

- **Skills.** The main duties or abilities of the user (such as DBA or Programmer)
- **Cost Rate.** The hourly cost associated with a resource or skill, which represents the charge-back or billed cost of their labor.
- **Workload Capacity.** A percentage that indicates what portion of a resource's working day is available for planned workload items. For instance, a particular DBA may have a lot of meetings every day, and therefore is set to devote 80% of her capacity to workload items.

Entering resource information for each user is an optional activity. For instructions on configuring resource information, see the *Mercury Resource Management User's Guide*.

Importing Users from a Database or LDAP Server

Enterprises with a large number of users can create user accounts using Mercury IT Governance Center's open interface. This API uses interface tables within the Mercury IT Governance Center database instance. Data added to these interface tables is validated and eventually imported into standard database tables, generating users that can then be processed normally within Mercury IT Governance Center. Users can also be imported from an LDAP server.

Refer to the *Open Interface Guide and Reference* for full documentation on this feature. This document provides an overview of relevant database tables and provides detailed instructions for performing the user import.

Creating Security Groups

Security groups are used to control who can access certain screens and functionality in Mercury IT Governance Center.

To create a security group:

1. Open the Security Group Workbench and click **New Security Group.**

   The Security Group window opens.

2. Specify security group membership on the **Users** tab.

   Either provide a list of users or associate the group with an organization unit that has been defined in Mercury IT Governance Center.

3. Specify the screen and feature access by linking the appropriate access grants. See *Access Grants* on page 115 for a full list of access grants.

4. In the **Change Management Workflows** tab, specify which workflows users in this security group can use when deploying changes.

   This is only used when the security groups will be used in a deployment process.

5. In the **Change Management App Codes** tab, restrict the security group from using certain Application Codes when creating a package line.

   This restricts which applications each user can process objects through. This is only used when the security groups will be used in a deployment process.

Consider creating and maintaining two types of security groups:

- Security groups to control who can act on a specific workflow steps (list of users without any special access grants)
- Security groups to control who can access a particular screen or function (list of users and appropriate access grants)

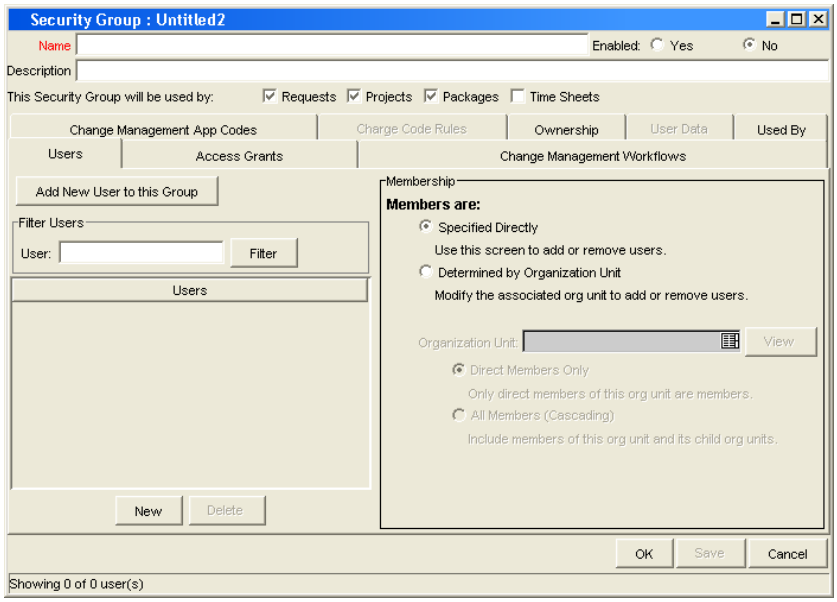
This can greatly simplify the maintenance of a security model around processes. As new users are added to the system, they can be granted appropriate screen and function access and associated with specific workflows.

Creating a Security Group by Specifying a List of Users

To generate and define a new security group:

1. Click **New Security Group** in the Security Group Workbench or select **File > New > Security Group** from the menu.

   The Security Group window opens.



2. Enter the Name and Description.

3. Select **Yes** to enable this security group.

   Only enabled security groups appear as a choice when generating or updating users or workflows.

4. Select which Mercury IT Governance Center entities (requests, projects, packages, or time sheets) will use the security group by clicking their respective checkboxes in the This Security Group will be used by field.

   These options are discussed in the following table.

Field	Description
Requests	Determines whether this security group can be used in request processing. If this box is un-checked, the security group will not appear in: • The Assigned Group field on the request. • The **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 will appear in the Assigned Group field.
Projects	Determines whether users in this security group can be used as resources on a project. This checkbox affects the following screens: • **Project Team** tab in the Project Settings window: If deselected, the users in the security group will not be available as resources (unless they belong to another security group that grants them access). • Project plan panel: If deselected, the users in the security group can not be added to the project team (unless they belong to another security group that grants them access). • Resource Group field on the Project plan panel: If deselected, the security group will not appear in the list of resource groups. Note: If a user has the System:Override Key Fields Segmentation access grant, then the above security group restrictions will not apply.
Packages	Determines whether this security group can be used in package processing. If the box is un-checked, the security group will not appear 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 will appear in the Assigned Group field.
Time Sheets	Enables the Charge Code Rules tab, where you can set who has access to certain charge codes in Mercury Time Management.

5. Link the desired users to the security group.

   a. Click **New** in the **Users** tab.

      The Users window opens.

b. From the Users field, select the desired user or users.

c. Click **OK** to add your selection to the **Users** tab.

6. Link the desired access grants.

   Each access grant enables certain functions performed on a screen. See *Access Grants* on page 115 for a description of each available access grants.

   a. Select the desired access grants in the Available Access Grants list.

   b. Click the right arrow button pointing to the Linked Access Grants list.

   The selected access grants are moved into the column.

7. Restrict the security group from using certain workflows when processing packages.

   a. Click the **Change Management Workflows** tab.

   b. Select the workflows in the Allowed Change Management Workflows list.

   c. Click the left arrow button pointing to the Restricted Change Management Workflows list.

      The selected workflows are moved into the column.

   d. If all future workflows should also be excluded, select the Always restrict new Workflows checkbox.

8. Restrict the security group from using certain Application Codes when creating a package line.

   This restricts which applications each user can process objects through.

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

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

   c. Click the left arrow button pointing to the Restricted Change Management App Codes list.

      If all future app codes are to be excluded, select the **Always restrict new App Codes** checkbox.

9. Click the **Ownership** tab and select the ownership groups that have the right to edit, copy or delete the current security group.

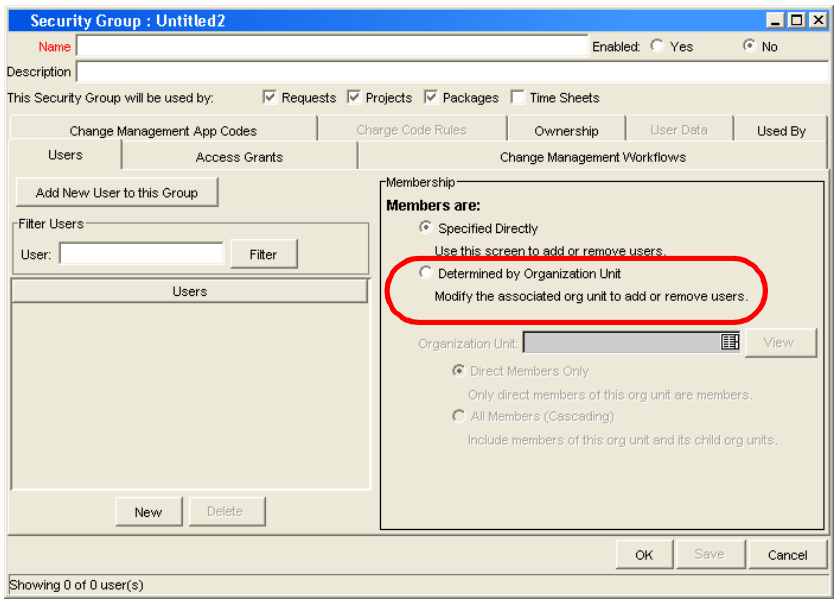
   See *Setting Ownership for Configuration Entities* on page 110 for more information about setting Ownership for a new or existing security group.

10. (Optional) Enter any necessary information in the **User Data** tab's fields.

11. Click **OK** to register the current security group and close the Security Group window. Click **Save** to save the information and leave the Security Group window open.

Using Resource Management to Control User Security

Users can also be associated to security groups through their inclusion in an organization model definition. Using the Mercury IT Governance Center resource management capabilities, a user can be placed into a model that includes security and access information. See the *Mercury Resource Management User's Guide* for details.

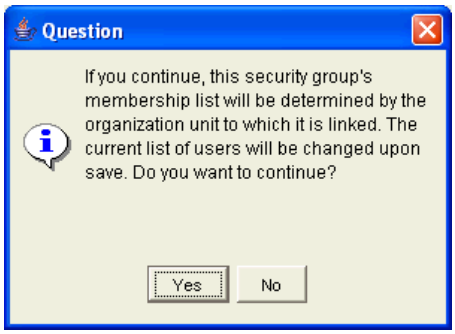


To define a security group to use the members of an organization unit:

1. Open the Security Group window.

2. Select Determined by Organization Unit in the Membership section of the **Users** tab.

The following question dialog opens.



3. Click **Yes.**

Note

When you select an organization unit to control user access to the security group, any users specified in the Users list will be replaced with the members of the organization unit.

4. Select the Organization Unit.

5. Select whether you want to include:

   - **Direct Members Only**
     Only direct members of the specified organization unit. Sub-units in the organization are not included.

   - **All Members (cascading)**
     Members of this organization unit and its child units. For example, your Quality Assurance organization unit consists of the following sub-units: Testers and Bug Fixers. If you select to Also include members of child organization units for the Quality Assurance unit, then the list of users will contain all of the resources defined in each of the units (Quality Assurance, Testers and Bug Fixers).

6. Click **OK.**

Refer to the *Mercury Resource Management User's Guide* for instructions on associating users with an organization model.

Using the Change Management App Codes Tab

Application codes (or app codes) are part of each Mercury Change Management™ Environment definition. If a site is not licensed for Mercury

Change Management, the **App Codes** tab will be grayed out and not accessible in Mercury Change Management.

For security groups containing Change Management users, the Application Codes available to security group members can be limited when new package lines are generated. This provides the ability to restrict which applications each user can process objects through. For example, software changes for an ERP system can be assigned to a specific set of users, while access to Front Office application changes can be assigned to a different set of users.

By default, a new security group gives its members access to all Change Management app codes. Use the left and right arrow buttons between the two lists in this tab to move app codes to and from the Restricted list. Any app code in the Restricted Change Management App Codes list will not be available for use by members of the security group. To completely restrict a user from using a specific app code, that app code must be excluded from all security groups of which the user is a member.

When adding lines to a package, Mercury Change Management normally has an app code default of **NONE**. This **NONE** selection can be left out of the App Code field if desired. There is a checkbox called **Force App Code Selection** in the workflow definition.

Using the Charge Code Rules Tab

The **Charge Code Rules** tab controls charge code access for security groups used with Mercury Time Management. The charge codes that are visible to a member of the security group are specified here. Charge codes can be restricted by Category, Client, or Department. A charge code that satisfies a value set by a charge code rule is visible to a member of the resource group.

For example, a charge code rule of type **Category,** with value **Billable,** makes charge codes in the Billable category visible to a member of the security group. All other categories are not displayed.

If a user is a member of a security group with no restrictions, that user will have access to all charge codes. For this reason, we recommend enabling charge code rules for all security groups.

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

Name	Description
Restrict Charge Codes to the following rules	Determines whether charge codes for this security group will be restricted. If deselected, the security group will have access to all charge codes.
Type	The type of charge code rule. Charge codes can be restricted by Category, Client, or Department.
Value	The value of the Category, Client, or Department for the allowed charge code.

Chapter

3

Managing Your Mercury IT Governance Licenses

In This Chapter:

Overview of Managing Your Licenses

Each user that is going to view or perform work in a Mercury IT Governance Center product must be given an appropriate product license. Different licenses enable different parts of the application. For example, a Project Management license grants a user access to the project planning interface, whereas a Change Management Licence grants access to the interface for creating and processing packages. See *License Types* on page 129 for a detailed discussion of each license.

Assigning Licenses in the User window

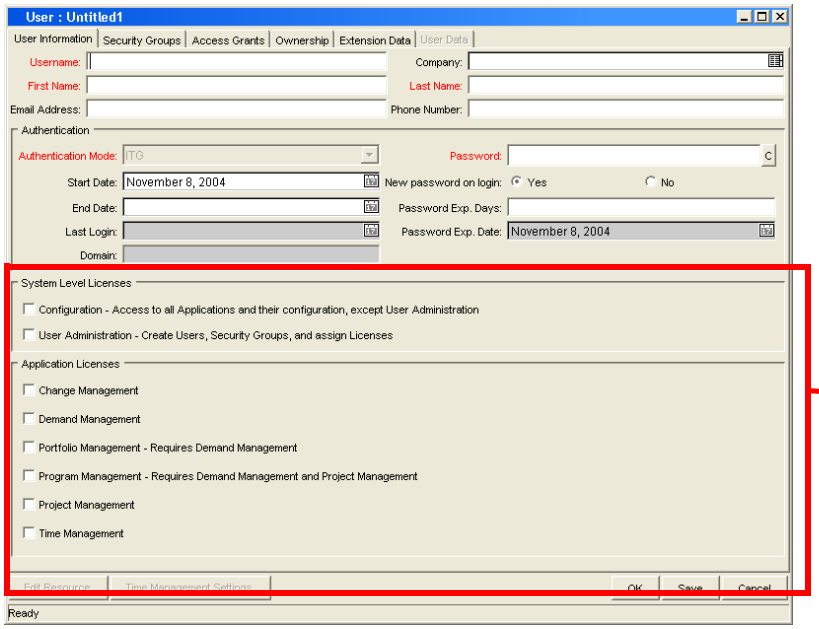
To assign a license to a single user in the User window:

1. Log on to Mercury IT Governance Center and open the Workbench.
2. From the shortcut bar, select **Sys Admin > Users.**
3. The User Workbench opens.
4. Open the User window for the user that you would like to assign a license to.
5. Select the desired licenses from the drop-down lists on the lower half of the window.

   Selecting the **Configuration** license will update the window to show that the user has standard access to all purchased Mercury IT Governance Center products, with the exception of system administration admin functions.

You can only assign licenses that have been purchased by your company. If you do not have any licenses for a particular Mercury IT Governance Center product, then that license field will be disabled.

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



6. Click **Save** to save the new license settings for the user.

Note

You must have licenses available in the system in order to successfully apply them to a user. If you do not have enough licenses available, you will receive a message upon **Save.**

Assigning Licenses to Multiple Users in the License Workbench

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

To assign licenses using the Assign License wizard:

1. Log on to Mercury IT Governance Center and open the Workbench.

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

The License Administration window opens. This window displays how many of each license is available (not used), and which Change Management Extensions are installed at your site.

3. Click **Assign Licenses.**

   The Assign Licenses wizard opens.

4. Find Users step: Locate the users that you would like to assign licenses to by entering search criteria in the fields and clicking **Next.** All users selected by the search will be assigned licenses later in the wizard process. You can specify users based on the fields defined in *Table 3-1*.

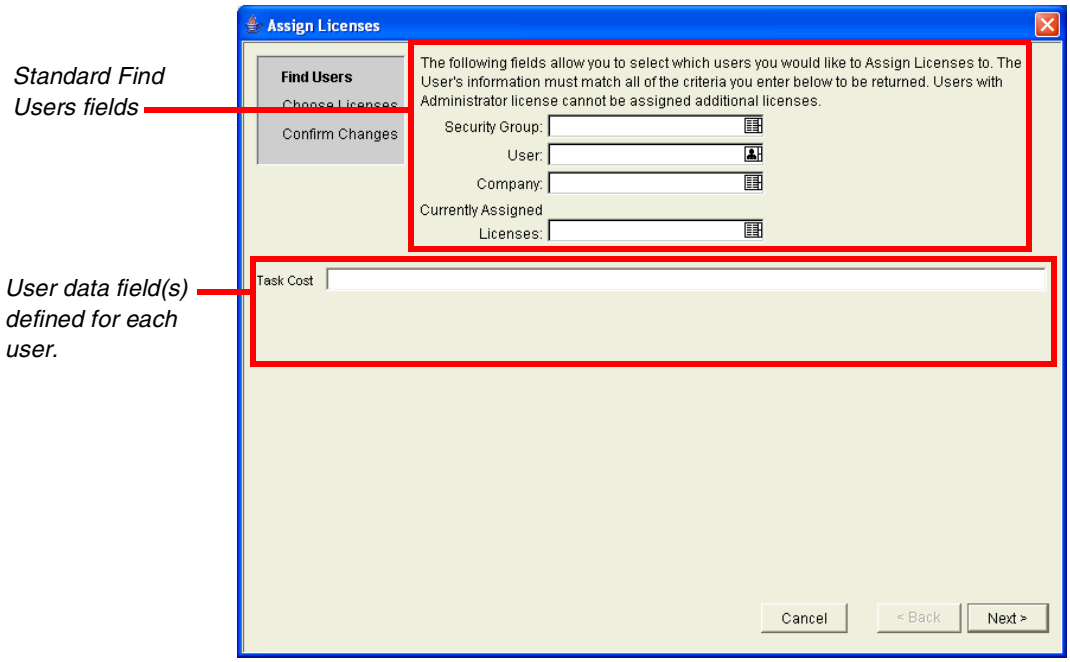


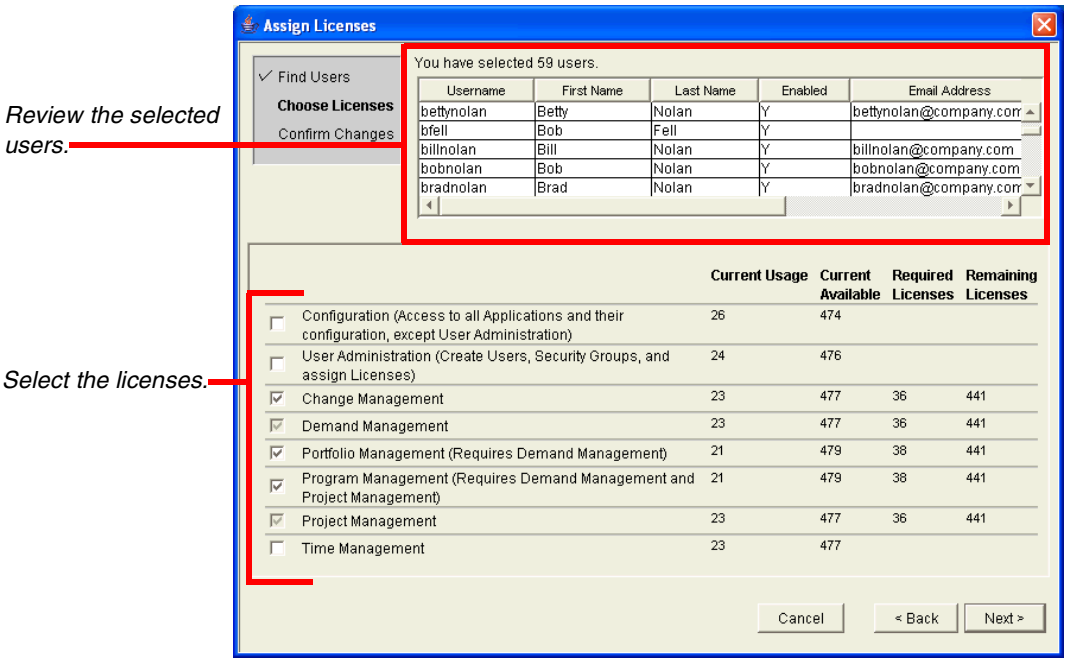
Table 3-1. License Administration Wizard - Find Users step

Fields	Definition
Security Group	Locates users that belong to a specific security group. You can select multiple security groups in this field. The search will return a list of all users that belong to any of the selected security groups.
User	Locates any users that are explicitly specified in this field.
Company	Locates users that are associated with a specific company. Companies are associated with users in the Contacts screen on the Demand Mgmt Workbench.

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

Fields	Definition
Currently Assigned Licenses	Locates all users that that currently have any of the licenses specified in this field.
User Data Fields	Search for users based on the custom 'User' user data fields defined at your site.

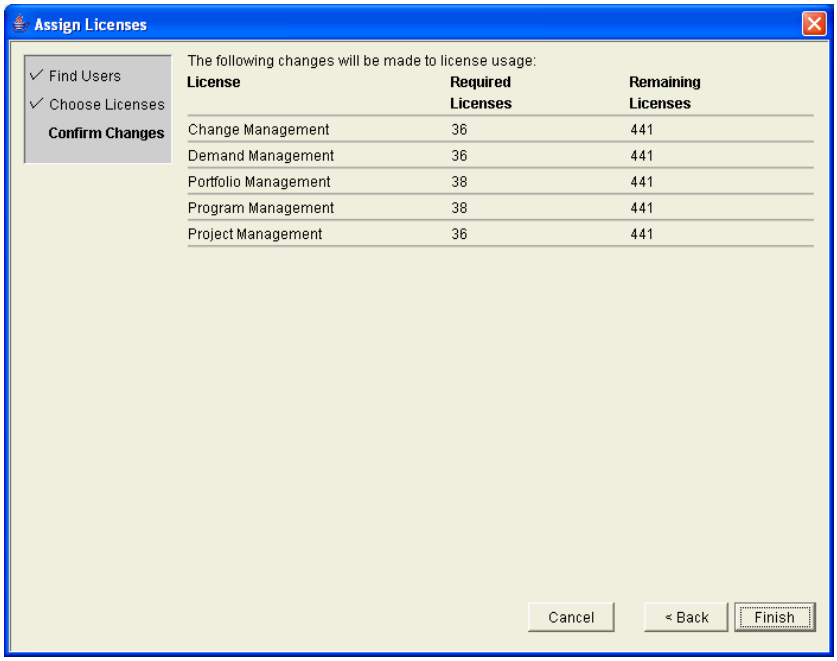
5. Choose Licenses step: Review the selected users and then specify which licenses to grant them by selecting the licenses from the license fields. Note that although all users may not be selected in the user list, the licenses specified will be applied to all of the users that meet the requirements from the Find Users step.



6. Click **Next**.

7. Confirm Changes step: Review the license assignments. Ensure that the Remaining Licenses number is greater than or equal to zero. A negative number indicates that you do not have enough available licenses to apply to the set of users. If this is a negative number, you will not be able to complete the license assignment process.

8. Click **Finish** to apply the licenses.



Note

An available license will only be used if the selected user does not already have the license. Licenses will append, not overwrite, the license specifications for a user (except when removing a license by specifying **Remove License**).

For example, John Smith meets the search requirements in the Find User step. In the Choose License step, you specify that every user should be granted a Demand Management license. John Smith already has a Configuration license. When the licenses are applied, a Demand Management license is not applied to John. Therefore, this is not counted in the Required Licenses or Remaining Licenses columns.

Removing Licenses Using the Assign License Wizard

The Assign License wizard can also be used to remove licenses from a set of users.

To remove licenses:

1. Log on to Mercury IT Governance Center and open the Workbench.
2. From the shortcut bar, select **License > Sys Admin.**

   The License Administration window opens.

3. Click **Assign Licenses.**

   The Assign License wizard opens.

4. Find Users step: Locate the users that you would like to remove licenses from by entering search criteria in the fields and clicking **Next.** All users selected by the search will be altered later in the wizard process.

5. Choose Licenses step: Select **Remove License** from the license drop-down list for whichever product licenses you wish to remove.

6. Click **Next.**

7. Confirm Changes step: Review the license changes.

8. Click **Finish** to delete the specified licenses from the selected set of users.

Assigning Licenses Using the Open Interface

Licenses can also be applied to users using the Mercury IT Governance Center Open Interface. This API uses interface tables within the IT Governance Center database instance. Data added to these interface tables is validated and eventually imported into standard database tables, generating or updating user account information.

Refer to the *Open Interface Guide and Reference* for full documentation on this feature. This document provides an overview of relevant database tables and provides detailed instructions for performing the user import.

Chapter

4

Request Security

In This Chapter:

Overview of Request Security

This chapter discusses the data and process security related to creating and processing requests in Mercury Demand Management. Mercury Demand Management enables a great deal of control over who can participate in a request resolution process. User actions can be restricted around:

- **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, access can be enabled 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. Access can also be provided dynamically by having a token resolve to provide access.
- **Managing your request resolution process**
  - Who can change the workflow
  - Who can change each request type

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

- Licenses
- Access grants
- Request type settings in 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 are then given all functionality enabled by those access grants.

Restrictions around request viewing or processing can then be imposed on the request type level.

This section lists the license and access grants settings that should be set to enable general access to request processing.

Only users with an Administrator license can create or modify user and security group accounts. Work with the 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

Users must have the Demand Management or Configuration license in order to create and process requests.

See *Licenses and User Roles* on page 131 for details on what functionality is enabled with each license. Also, the following sections discuss how the functionality provided with each access grant differs depending on the license type that the user has.

Access Grants

Table 4-1 lists the common access grants used to 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 your un-submitted requests. • 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 in the **User Access** tab on the Request Type window. • Allows the user to delete the request as specified in the **User Access** tab on the Request Type window. • Allows the user to cancel the request as specified in the **User Access** tab on the Request Type window.
Demand Mgmt: Manage 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: Override Participant Restriction	This access grant allows the user to review a request regardless of whether the user is allowed to view or not as defined in the request type's **User Access** tab.

Screen and function access provided through access grants are cumulative. If a user belongs to three different security groups, he will have all access provided to each of the groups. Therefore, to restrict certain screen and feature access, remove 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, 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). Note: only do this if no one in that security group needs the access provided in that access grant.

Note

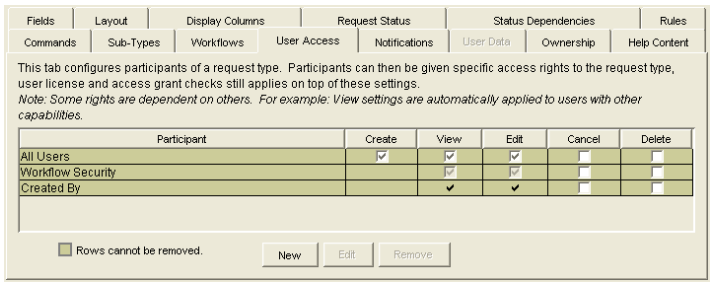
The Mercury IT Governance Center includes other specialized access grants that can be used to control access to other functions in Demand Management. See *Access Grants* on page 115 for details.

Viewing a Request

It is possible to control which users are allowed to view requests of a specific request type.

To enable all users to view requests:

1. Open the Request Type window.
2. Click the **User Access** tab.



3. In the All Users row, select the View checkbox.
4. Click **Save.**

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

1. In the Request Type window's **User Access** tab, deselect the View checkbox in the All Users row.

   By default, the View field remains selected in the Workflow Security row. This indicates that any user who is included in the associated workflow's security (defined in any workflow step in the Workflow window) can view the request.

2. Click **New.**

   The Participant Security window opens.

3. From the Security Group field, select the security group that can view requests of this request type.

4. Click **OK.**

   A new line listing the selected security group is added to the **User Access** tab.

5. On the Request Type window, click **Save.**

To enable specific users to view a request:

1. In the Request Type window's **User Access** tab, deselect the View checkbox in the All Users row.

2. Click **New.**

   The Participant Security window opens.

3. From the drop-down 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.

Selecting a value will automatically update the field below. For example, selecting **Enter a Username** will change the field below to Username.

4. Enter the specific value that corresponds to the recipient type selected above.

   This can be a username or a token.

5. Click **OK.**

   A new line listing the selected user or token is added to the **User Access** tab.

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

Creating a Request

It is possible to control who can create certain requests or use specific request types and workflows.

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

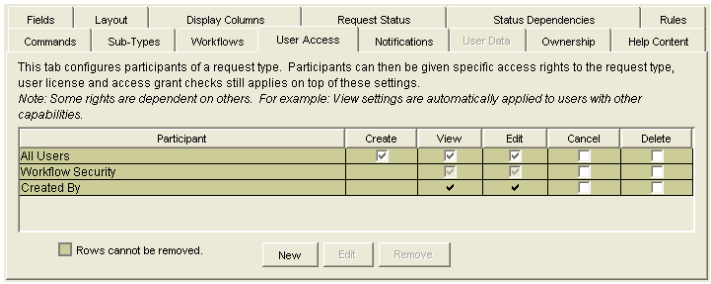
Enabling Users to Create Requests

It is possible to specify which users are allowed to create requests of a specific request type in the Request Type window's **User Access** tab. You can enable all users with appropriate access grants to create a request, or enable only certain users to create requests of a certain request type.

The **User Access** tab can include multiple lines that grant access to create or process the request. If a user meets any of the requirements listed in the tab, he will have access to perform that action in the request.

To enable all users to create and submit a request:

1. Open the Request Type window.
2. Click the **User Access** tab.



3. In the All Users row, select the Create checkbox.
4. Click **Save.**

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

1. In the Request Type window's **User Access** tab, deselect the Create checkbox in the All Users row.
2. Click **New.**

   The Participant Security window opens.
3. From the Security Group field, select the security group that can create requests of this request type.
4. Click **OK.**

   A new line listing the selected security group is added to the **User Access** tab.
5. On the **User Access** tab, click **Save.**

To enable specific users to create a request:

1. In the Request Type window's **User Access** tab, deselect the Create checkbox in the All Users row.
2. Click **New.**

   The Participant Security window opens.

3. From the drop-down list, select one of the following items:

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

   Selecting a value will automatically update the field below. For example, selecting **Enter a Username** will change the field below to Username.

4. Enter the specific value that corresponds to the recipient type selected above.

   This can be a username or a token.

5. Click **OK.**

   A new line listing the selected user or token is added to the **User Access** tab.

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

Restricting Users from Selecting a Specific Workflow

When creating a request, a workflow must be selected for the request to proceed through. It is possible to control which workflows can be used with each request type.

To restrict users from selecting a specific workflow when creating a new request.

1. In the Request Type window, click the **Workflow** tab.
2. Deselect the All Workflows are allowed for this Request Type checkbox.
3. Click **New.**

   The Workflow: New window opens.
4. From the Workflow field, select only the workflows that can be used with this request type.
5. Click **OK.**
6. The selected workflows are added to the **Workflow** tab.
7. Click **Save.**

Only workflows specified in the **Workflow** tab can be used when creating requests of this request 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 also opt to restrict all new request types.

The default request type to be used with this workflow can also be specified.

This is set on the Workflow window **Request Types** tab.

Processing a Request

It is possible to 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.

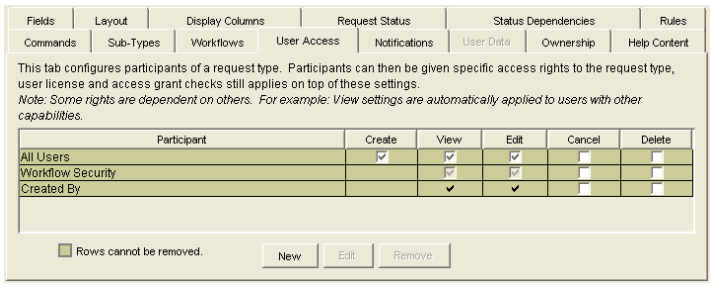
The following sections assume that your users have the appropriate license and access grants to perform basic request creation and processing.

Enabling Users to Edit Fields on a Request

It is possible to control which users are allowed to edit fields on requests of a specific request type.

To enable all users to edit fields on a request:

1. Open the Request Type window.
2. Click the **User Access** tab.



3. In the All Users row, select the Edit checkbox.
4. Click **Save.**

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

1. In the Request Type window's **User Access** tab, deselect the Edit checkbox in the All Users row.

   By default, the Edit field remains selected in the Workflow Security row. This indicates that any user who is included in the associated workflow's security (defined in any workflow step in the Workflow window) can edit request fields.

2. Click **New.**

   The Participant Security window opens.

3. From the Security Group field, select the security group that can edit requests of this request type.
4. Click **OK.**

   A new line listing the selected security group is added to the **User Access** tab. By default, the Edit field is selected.

5. On the Request Type window, click **Save.**

To enable specific users to edit a request:

1. In the Request Type window's **User Access** tab, deselect the Edit checkbox in the All Users row.

2. Click **New.**

   The Participant Security window opens.

3. From the drop-down 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.

   Selecting a value will automatically update the field below. For example, selecting **Enter a Username** will change the field below to Username.

4. Enter the specific value that corresponds to the recipient type selected above.

   This can be a username or a token.

5. Click **OK.**

   A new line listing the selected user or token is added to the **User Access** tab. By default, the Edit field is selected.

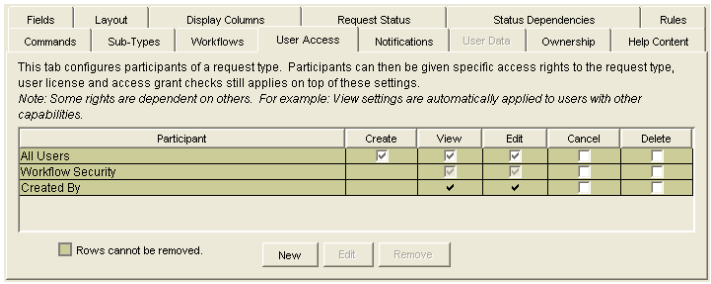
6. On the Request Type window, click **Save.**

Enabling Users to Cancel or Delete a Request

It is possible to control which users are allowed to cancel or delete requests of a specific request type.

To enable all users to cancel or delete a request:

1. Open the Request Type window.
2. Click the **User Access** tab.



3. In the All Users row, select the Cancel and Delete checkboxes.
4. Click **Save.**

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

1. In the Request Type window's **User Access** tab, click **New.**

   The Participant Security window opens.

2. From the drop-down list, select one of the following items:

- **Enter a Security Group.** Specify all users in a security group.
- **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.

Selecting a value will automatically update the field below. For example, selecting **Enter a Username** will change the field below to Username.

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

   A new line listing the selected user or token is added to the **User Access** tab.
5. In the new row, select the Cancel and Delete checkboxes.
6. On 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

It is necessary to 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 will be able to process the request at that step.

To specify the users who can act on a specific workflow step:

1. Open the workflow.

2. Click the **Layout** tab.

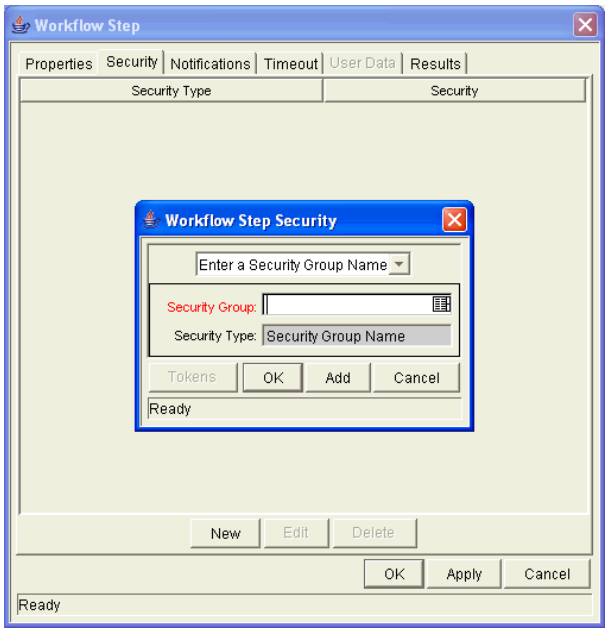
3. Double click on the step that you would like to configure.

   The Workflow Step window opens. Note: the Workflow Step window also opens when first adding a step to the **Layout** tab.

4. Click the **Security** tab.

5. Click **New.**

   The Workflow Step Security window opens.



6. Select the method for specifying the step security from the drop-down list:

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

   Selecting a value from this field automatically updates the other fields on this window. For example, selecting **Enter a Username** will change the Security Group field to Username.

7. Specify the security groups, usernames, or tokens that will control the access to this step.

8. Click **OK.**

   The security specification is added to the **Security** tab. Additional specifications can then be added to the step by clicking **New** and repeating the above process. The step's security can therefore be controlled using a combination of multiple security groups, usernames, and tokens.

9. Click **OK** to save and close the window.

Tips:

- Consider assigning a security group to each decision, execution and condition step, even though many of these steps will 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. That group could be configured with global access to act on every step in the process. Again, this could help avoid bottlenecks by providing a small group with permission to process stalled requests.
- Avoid specifying a single user as the only person who can act on a workflow step. This would require a process update (re-configuration) when that user changes roles or leaves the company. It is better to grant access dynamically using a token or security group.

Viewing and Editing Fields on a Request

A number of features can be used to restrict users from viewing or editing specific fields on a request. This field-level data security is configured using the Request Type and Request Header Type windows in the Workbench.

The following sections assume that the user has been granted standard access to view and edit the request, but does not have the Demand Mgmt: Manage Requests access grant.

Field-Level Data Security Overview

Field editability and visibility can be set in the following places in the Workbench:

- Field window: **Attributes** tab
  Used to set general view and edit access for all users.
- Field window: **Security** tab
  Used to set view and edit access for a specific list of users.
- Request Type window: **Status Dependencies** tab
  Used to set view and edit access for a field depending on the request's status.

Figure 4-1 illustrates the order that determines whether a field is visible to a particular user.

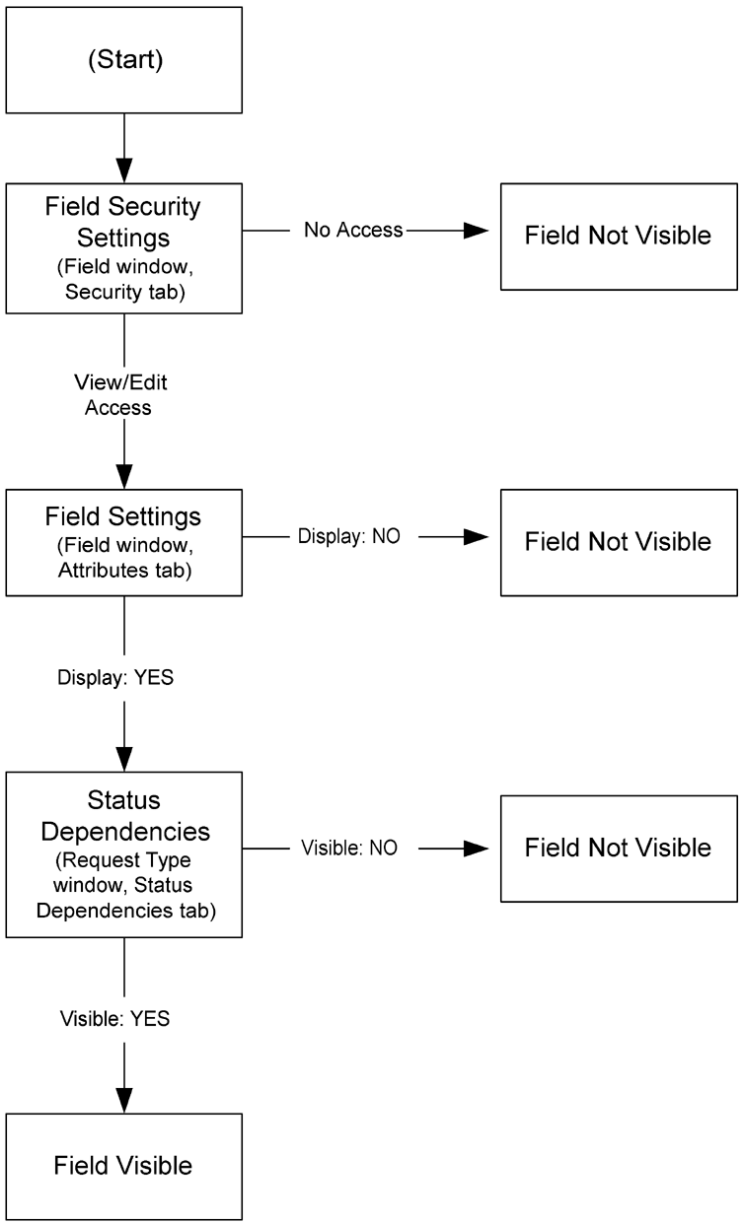


Figure 4-1. Field visibility interactions

Field Window: Attributes Tab

The **Attributes** tab can be used to set general view and edit access for all users. The following settings are used to control visibility and editability of a field:

Table 4-2. Settings to control view and edit access in the Attributes tab.

Parameter	Description
Display	Controls whether the field is visible on the request. If set to **No,** this field will not be visible to any user.
Display Only	Controls whether the field is editable on a request. If set to **Yes,** the field can not be updated.

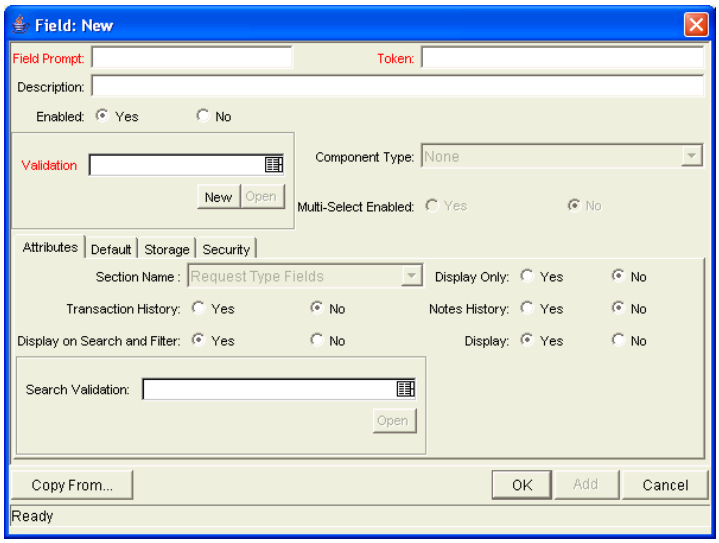


Figure 4-2. Field window: Attributes tab

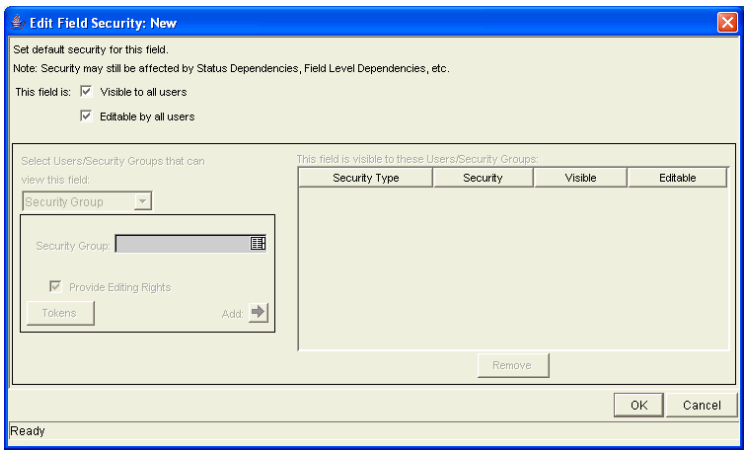
Field Window: Security Tab

The **Security** tab can be used to set view and edit access for a specific list of users.

To limit who can view and edit the field to a specific group of users:

1. In the Field window, click the **Security** tab.
2. Click **Edit.**

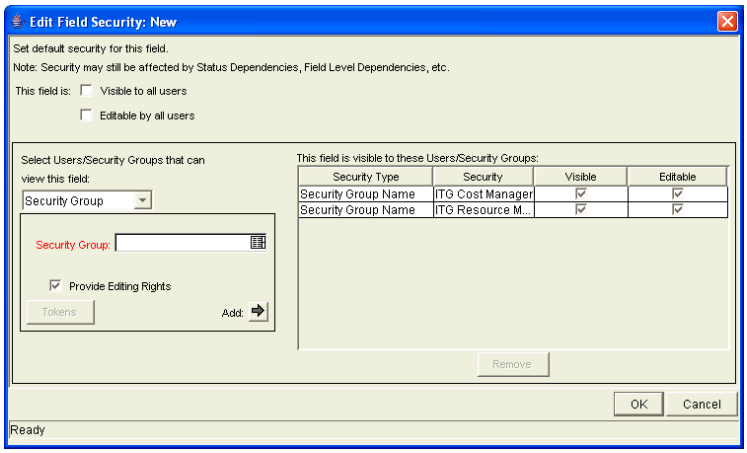
   The Edit Field Security window opens.



3. Deselect Visible to all users and Editable by all users.

4. Specify who can view or edit the field. You can select a **User, Security Group, Standard Token,** or **User Defined Token.**

5. Click the Add arrow to add the selection to the right-hand window.



6. Click **OK** to save the settings.

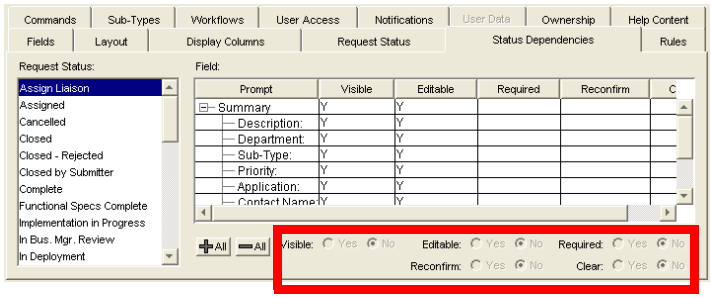
Request Type Window: Status Dependencies Tab

Request field behavior can be linked directly to the statuses of 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 the request's status using the following settings on the **Status Dependencies** tab:

Table 4-3. Settings for view and edit access in the Status Dependencies tab

Parameter	Description
Visible	Determines whether or not a field is visible for a specific request status. If it is set to Visible = **No,** then the field is not displayed.
Editable	If a field is set to Editable = **No** for a specific request status, then it is not possible to edit the field at the given request status. If a field is set up as Required, Reconfirm, or Clear, it must be set to Editable = **Yes.**



Overriding Request Security

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

Table 4-4. Settings required to override request security

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

Users with the following access grant can edit request types, regardless of Ownership restrictions:

Table 4-5. Access grant to override request type configuration security

Access Grant	Description
Ownership Override	Access and edit all configuration entities even if the user is not a member of one of the entity's ownership groups.

Chapter

5

Package Security

In This Chapter:

Overview of Package Security

This chapter discusses the data and process security related to creating and processing packages in Mercury Change Management. Mercury Change Management enables a great deal of control over who can participate in a package deployment process. User actions can be restricted around:

- **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 your deployment process**
  - 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 allows you to control which processes are being used for deployments as well as which Environments are being affected.

Screen and function access provided through access grants are cumulative. If a user belongs to three different security groups, he will have all access provided to each of the groups. Therefore, to restrict certain screen and feature access, you need to 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 (using the **Security Group** tab on the User window)
- Remove the access grants from the security group (in the Security Group window). Note: you should only do this if no one in that security group needs the access provided in that access grant.

This chapter discusses how to enable a user to view or edit items in Mercury Change Management. You can restrict access by altering the specified settings or removing the specified access grants or licenses.

Viewing a Package

You can control which users can view a package. To enable a user to view packages, set the following:

Table 5-1. Settings to view packages

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

Restricting Package Viewing to Participants

The Package Security option in the **Change Management** tab of the Workflow window lets you determine who can have access to packages that use the current workflow. Restricting access to participants means that when non-participant users search for packages, they will not see a package that uses the current workflow. In this instance, participants are defined as:

- The Assigned User
- The creator of the package
- Members of the Assigned Group
- Any users who have access to the workflow step(s)

To let all Change Management users access packages using the current workflow, select **All Users.**

To restrict the users who can access packages associated with this workflow to participants of the packages, 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

You can control which users have the ability to create and submit packages. To enable a user to create and submit a package, ensure that the following are set.

Table 5-2. Settings to enable package creation

Setting	Value	Description
License	Change Management or Configuration	The Change Management license provides a user with access to the Workbench, where the package is defined.
Access Grants linked to the Security Group (only one is required)	Change Management: Edit Packages	This access grant allows the user to generate, edit and delete certain packages. • User cannot delete a package if it has been released or if user is not the owner. • 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 security.
	Change Management: Manage Packages	This access grant allows the user to create, edit, and delete packages at anytime.
Allowed Change Management Workflows in the Security Group window	You must have at least one workflow allowed.	When creating a package, you are required to select a workflow for the package to proceed through. At least one workflow must be enabled to be able to create and submit a package. The user should select the workflow intended to process the deploying objects. This is set in the Security Group window, on the **Change Management Workflows** tab.
Allowed Change 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 such that only certain object types can be processed through the workflow. At least one object type must be enabled so that the user can create a package line when using that workflow. This is set in the Workflow window, on the **Change Management Settings** tab, under the Package Line selection.

Restricting 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 Change Management Workflows in the Security Group window	Include the workflows that you would like to restrict.	When creating a package, you are required to select a workflow for the package to proceed through. Users (in the security group) will not be able to select any workflows included in the Restricted Change Management Workflows list. Note: If a user belongs to another security group that allows the use of that workflow, the user will be able to select it. This is set in the Security Group window, on the **Change Management Workflows** tab.

Restricting the workflow selection also controls who can deploy changes to specific Environments, because the source and destination Environments are defined in the workflow step.

Restricting Users from Selecting a Specific Object Type

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

Table 5-4. Settings to restrict object type selection

Setting	Value	Description
Restricted Change Management Object Types in the Workflow window.	Include the object type that you would like to restrict.	You can associate object types with workflows such that only certain object types can be processed through the workflow. Users will not be able to select any object types included in the Restricted Change Management Workflows list. This is set in the Workflow window, on the **Change Management Settings** tab, under the Package Line selection.

Approving Package Lines

All users who will be processing package lines must meet the following conditions:

Table 5-5. Settings to enable package processing

Setting	Value	Description
License	Change Management or Configuration	This license provides a user with access to the Workbench and standard interface. Users can act on all workflow steps (decisions and executions) in the Workbench.
Access Grants linked to the Security Group	Change Mgmt: Edit Packages	This access grant allows the user to generate, edit and delete packages. 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.
	Change Mgmt: Manage Packages	This access grant allows the user to edit or delete packages at anytime.

Enabling Users to Act on a Specific Workflow Step

You need to specify who can act on each step in the deployment workflow. Only people who are specified on the **Security** tab in the Workflow Step window will be able to process that step.

Deleting a Package

You can control which users can delete a package. To enable a user to delete package, set the following:

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

Setting	Value	Description
License	Change Management	This license provides a user with access to the workbench and advanced package processing options.
Access Grants linked to the Security Group	Change Mgmt: Edit Packages	Users with this access grant can delete the package if it has not been submitted and he is the owner.
	Change Mgmt: Manage Packages	Users with this access grant can delete any package they can access.

Overriding Package Security

Users with the following settings can view, edit and delete any packages:

Table 5-7. Settings to override package security

Setting	Value	Description
License	Change Management or Configuration	This license provides a user with access to the Workbench and advanced package processing options.
Access Grants	Change Mgmt: Manage Packages	View, edit, and delete any package.
	Change Mgmt: Override Change Mgmt Participant Restriction	View the detailed information on a restricted package for which the user is not an active participant.

Users with the following access grant can edit Change Management configuration entities, regardless of Ownership restrictions:

Table 5-8. Access grant to override configuration security

Value	Description
Ownership Override	Access and edit all configuration entities even if the user is not a member of one of the entity's ownership groups.

Chapter

6

Project and Task Security

In This Chapter:

Overview of Project and Task Security

This chapter discusses the data and process security related to creating and processing projects in Mercury Project Management. Configuring this data and process security often involves a setting a number parameters: licenses, access grants, entity-level settings, and field-level settings. The following sections discuss the settings required for securing the specified actions or data.

Screen and function access provided through access grants are cumulative. If a user belongs to three different security groups, he will have all access provided to each of the groups. Therefore, to restrict certain screen and feature access, you need to 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 (using the **Security Group** tab on the User window)
- Remove the access grants from the security group (in the Security Group window). Note: you should only do this if no one in that security group needs the access provided in that access grant.

Viewing Projects and Tasks

You can control which users can view projects and tasks. By default, any users with one of the following licenses and access grants can view projects.

Table 6-1. Settings to view projects and tasks

Setting	Value	Description
License	Project Management or Configuration	The Project Management license provides a user with access to the Workbench and standard interface where they can view the project and task information.
Access Grants linked to the Security Group	Project Mgmt: View Projects	View project definitions in the Projects Workbench and standard interface. Note that the Edit Projects and Manage Projects access grants also provide viewing privileges, but also enable more advanced editing and processing functions.

To restrict users from viewing projects and tasks, set the following:

Table 6-2. Settings to restrict a user from viewing projects and tasks

Setting	Value	Description
License	(REMOVE) Project Management	Removing this license from the user keeps them from viewing any project or task related pages or windows in Mercury Project Management.
Access Grant	(REMOVE) Project Mgmt: View Projects; Edit Projects; Manage Projects	Removing these access grant from users keeps them from viewing projects and tasks.
Participant Restriction	Participant Restriction**	Restrict who can view projects and tasks to only "participants." Set in the **Security** tab on the Project Settings window.

**A participant can be the:

- Users assigned as project managers
- Users assigned as a resource on a task
- Users in an assigned resource group

Controlling Resources on the Project

Project managers can specify who will be allowed to act as resources for a project. Resources can be users and groups of users. In the **Project Team** tab, the project manager can choose to one of the following:

- Allow all users with the **Project** option enabled in their security groups to be resources for a project.
- Only allow those resources who are specified in the **Project Team** tab to be used as resources for a project. These resources are listed in the tab's Resource table. For example, only the users shown in *Figure 6-1* can be added as resources to the project.

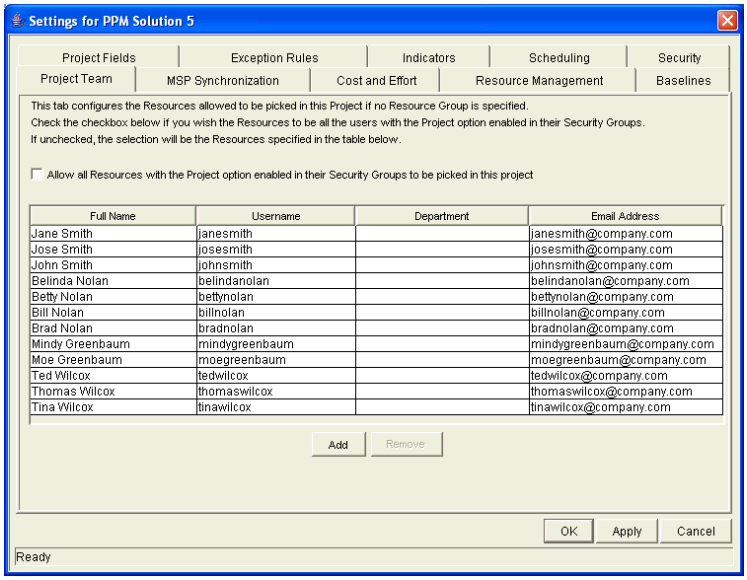


Figure 6-1. Project Team tab on the Project Settings window

Note

Exception: Users with the System: Override Key Fields Segmentation access grant can add any users as a resource to the project.

Creating Projects

You can control which users can create projects and tasks. By default, any users with one of the following licenses and access grants can view projects.

Table 6-3. Settings required to create a project

Setting	Value	Description
License	Project Management or Configuration	This license provides a user with access to the Workbench where he can create projects using the Project Workbench.

Table 6-3. Settings required to create a project

Setting	Value	Description
Access Grants (only one is required)	Project Mgmt: Edit Projects	Create projects using the Projects Workbench. Update and delete projects and subprojects when specified as the project manager.
	Project Mgmt: Manage Projects	Create, edit and delete projects. Override (or remove) references on projects or tasks.

Editing Project and Task Information

You can control which users can edit project and task information. This includes adding tasks to the project and modifying project settings. By default, users with the following licenses and access grants can edit projects.

Table 6-4. Settings required to edit a project

Setting	Value	Description
License	Project Management or Configuration	This license provides a user with access to the Workbench where he can edit projects using the Project Workbench.
Access Grants (only one is required)	Project Mgmt: Edit Projects	Update and delete projects and subprojects when specified as the project manager.
	Project Mgmt: Manage Projects	Edit and delete any projects. Override (or remove) references on projects or tasks.

Updating Tasks

You can control which users can update tasks on projects. Users with the following licenses and access grants can update tasks.

Table 6-5. Settings required to update tasks

Setting	Value	Description
License	Project Management or Configuration	This license provides a user with access to the Workbench and standard interface where they can update task status information.
Access Grants	Project Mgmt: Update Tasks (Required)	Update tasks when specified as a resource on the project.
	Project Mgmt: Manage Projects	Update multiple tasks using the Update Tasks page when participating in a project.
	Project Mgmt: Manage Projects; Project Mgmt: Override Participant Restriction	Update multiple tasks using the Update Tasks page on any project.
	Project Mgmt: Edit Projects	Update multiple tasks using the Update Tasks page when specified as project manager of a project or its parent.

To restrict users from updating tasks, set the following:

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

Setting	Value	Description
License	(REMOVE) Project Management	Removing this license from the user keeps him from accessing projects and tasks.
Access Grant	(REMOVE) Project Mgmt: Update Tasks	Removing these access grant from users keeps them from updating tasks.
Participant Restriction in the **Security** tab	Participant Restriction	Restrict who can access projects and tasks to only “participants.” Set in the **Security** tab on the Project Settings window.

Deleting Projects

Only users with the following license and access grants can delete projects.

Table 6-7. Settings to enable a user to delete a project

Setting	Value	Description
License	Project Management or Configuration	This license provides a user with access to the Workbench where he can delete projects.
Access Grants (Only one is required)	Project Mgmt: Edit Projects	Delete projects when specified as the project manager for the project or subproject.
	Project Mgmt: Manage Projects	Delete any project.

Overriding Project Security

Users with the following settings can view, edit, and delete any project:

Table 6-8. Settings to override request security

Setting	Value	Description
Access Grants	Project Mgmt: Manage Projects	View, edit and delete any project.
	Project Mgmt: Override Project Mgmt Participant Restriction	View the detailed information on a restricted project for which the user is not an active participant.

Users with the following access grant can edit Project Management configuration entities, regardless of Ownership restrictions:

Table 6-9. Access grant to override configuration security

Value	Description
Ownership Override	Access and edit all configuration entities even if the user is not a member of one of the entity's ownership groups.

Chapter

7

Resource Management Security

In This Chapter:

Overview of Resource Management Security

This chapter discusses the data and process security related to Resource Management functions in Mercury IT Governance Center. Configuring data and process security often involves a setting a number of parameters: Licenses, access grants, entity-level settings, and field-level settings. The following sections discuss the settings required for securing the actions or data related to Resource Management features.

Screen and function access provided through access grants are cumulative. If a user belongs to three different security groups, he will have all access provided to each of the groups. Therefore, to restrict certain screen and feature access, you need to 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 (using the **Security Group** tab on the User window)
- Remove the access grants from the security group (in the Security Group window). Note: you should only do this if no one in that security group needs the access provided in that access grant.

This chapter discusses how to enable certain functions. By default, users are not expected to be given access to viewing or modifying information related to budgets, cost, resource pools, staffing profiles, and skills. The following chapters provide instructions for enabling the viewing and editing of these functions.

Working with Resources

Each user has an associated resource information page. This page is used to capture information on the individual user such as Title, Direct Manager, and Capacity.

Viewing Resource Information

To allow a user to view resource information, set the following:

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	Allows users to only view their own resource information.
	Resource Mgmt: View all resources	Allows users to view any resource information in the system.

Modifying Resource Information

To allow a user to modify resource information, set the following:

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

User actions regarding resource pools are controlled by a combination of access grants and settings in the Configure Access for Resource Pool page. This page is shown in *Figure 7-1*.

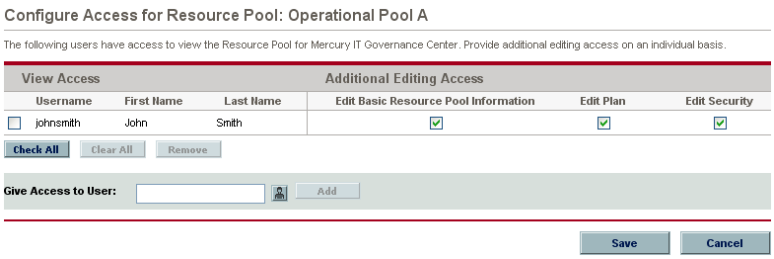


Figure 7-1. Configure Access for Resource Pool page

Viewing Resource Pools

To allow a user to modify resource pool information, set the following:

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

Setting	Value	Description
Access Grant (only one is required)	View Resource Pools	View resource pool information when the user has been granted view access in the Configure Access for Resource Pool page.
	View All Resource Pools	View resource pool information for all resource pools. Note: this grant provides unlimited access to view any resource pool. Consider using View Resource Pool to provide more limited view access.
Configure Access for resource Pool	View Access	Users included in the View Access list and have the View Resource Pools access grant can view the resource pool information.

Creating Resource Pools

To allow a user to create a resource pool, set the following:

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

Setting	Value	Description
Access Grant	Edit Resource Pools	Create a new resource pool.
	Edit All Resource Pools	Create a new resource pool.
	Create Resource Pools (Required)	Create resource pools using the standard interface. The user must also have either the Edit Resource Pools or Edit All Resource Pools grant to perform this function.

Modifying Resource Pools

To allow a user to modify resource pool information, set the following:

Table 7-5. Settings to allow users to modify resource pools

Setting	Value	Description
Access Grant (only one is required)	Edit All Resource Pools	Edit and delete any resource pool.
	Edit Resource Pools	Edit resource pool information when the user has been granted edit access in the Configure Access for Resource Pool page. Delete these resource pools when given sufficient access in the Configure Access for Resource Pool page for that resource pool.
Additional Editing Access (see Description column)	Edit Basic Resource Pool Information	Used in conjunction with the Edit Resource Pools access grant. Allows the user to edit resource pool header fields and Notes. He will not be allowed to change the Periods or any information in the Resource Pool Breakdown section.
	Edit Plan	Allows the user to edit the Periods and the information in the Resource Pool Breakdown section.
	Edit Security	Allows the user to edit the list of users who can modify the resource pool using the Configure Access for Resource Pool page.

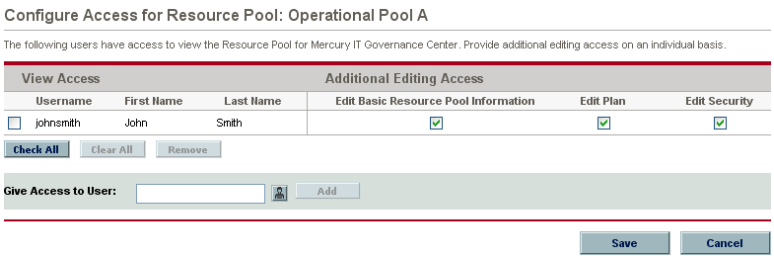


Figure 7-2. Configure Access for Resource Pool page

Working with Skills

Access to skills is controlled through access grants.

Viewing Skills

To allow a user to view skill information, set the following:

Table 7-6. Settings to allow users to view skill information

Setting	Value	Description
Access Grant	Resource Mgmt: View All Skills	Allows users to view skills defined on resources.

Creating, Modifying, and Deleting Skills

To allow a user to modify the list of skills set in Mercury IT Governance Center, set the following:

Table 7-7. Settings to allow users to create, modify, and delete skills

Setting	Value	Description
Access Grant	Resource Mgmt: Edit All Skills	Edit any skills defined in Mercury IT Governance Center.

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 organization information in Mercury IT Governance Center, set the following:

Table 7-8. Settings to view organization information.

Setting	Value	Description
Access Grant	Resource Mgmt: View Organization	View the organization model and organization unit detail pages.

Modifying Organization Definitions

To allow a user to modify organization information, set one of the following:

Table 7-9. Settings to modify organization information.

Setting	Value	Description
Access Grant (only one is required)	Edit Entire Organization	Edit and delete any organization unit.
	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. This page is shown in *Figure 7-3*.

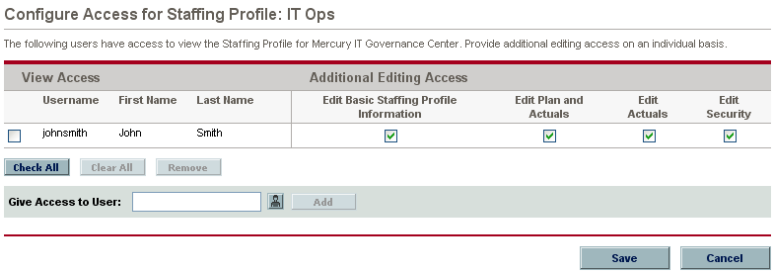


Figure 7-3. Configure Access for Staffing Profile page

Viewing Staffing Profiles

To allow a user to view staffing profile information, set the following:

Table 7-10. Settings to allow users to view resource pool information

Setting	Value	Description
Access Grant (only one is required)	View Staffing Profiles	View staffing profile information when the user has been granted view access in the Configure Access for Staffing Profile page.
	View All Staffing Profiles	View staffing profiles information for all Staffing profiles. Note: this grant provides unlimited access to view any staffing profile. Consider using the View Staffing Profiles grant to provide more limited view access.
Configure Access for Staffing Profile	View Access	Users included in the View Access list and have the View Staffing Profiles access grant can view the staffing profile information.

Creating Staffing Profiles

To allow a user to create a staffing profile, set the following:

Table 7-11. Settings to allow users to create staffing profiles

Setting	Value	Description
Access Grant	Edit Staffing Profiles	Create a new staffing profile.
	Edit All Staffing Profiles	Create a new staffing profile.
	Create Staffing Profiles (Required)	Create staffing profiles using the standard interface. The user must also have either the Edit Staffing Profiles or Edit All Staffing Profiles grant to perform this function.

Modifying Staffing Profiles

To allow a user to modify staffing profile information, set the following:

Table 7-12. Settings to allow users to modify staffing profiles

Setting	Value	Description
Access Grant	Edit All Staffing Profiles	Edit and delete any staffing profile.
	Edit Staffing Profiles	Edit staffing profile information when the user has been granted edit access in 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 7-12. Settings to allow users to modify staffing profiles

Setting	Value	Description
Additional Editing Access	Edit Basic Staffing Profile Information	Used in conjunction with the Edit Staffing Profiles access grant. Allows the user to edit staffing profile header fields and Notes. He will not be allowed to change the Periods or any information in the Staffing Profile Breakdown section.
	Edit Plan and Actuals	Allows the user to edit the Periods and the information in the Staffing Profile Breakdown section. Additionally, allows users to view and edit the planning and actuals data in the Profile Allocation table.
	Edit Actuals	Allows the user to edit the Periods and the information in the Staffing Profile Breakdown section. Additionally, allows users to view and edit the actuals data in the Profile Allocation table.
	Edit Security	Allows the user to edit the list of users who can modify the staffing profile using the Configure Access for Staffing Profile page.

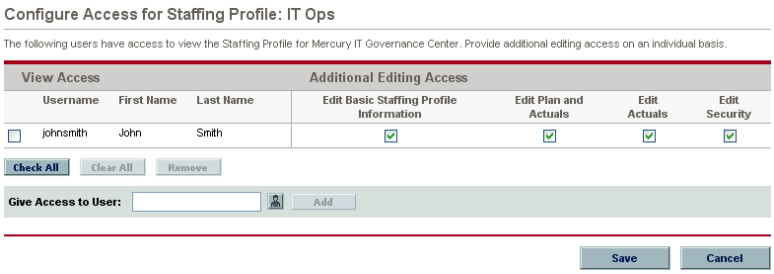


Figure 7-4. Configure Access for Staffing Profile page

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, set the following:

Table 7-13. Settings to allow users to view or edit regional calendars

Setting	Value	Description
Access Grant (only one is required)	View Regional Calendars	Allows users to only view regional calendars. Does not provide the ability to view resource calendars.
	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, set the following:

Table 7-14. Settings to allow users to modify resource information

Setting	Value	Description
Access Grant (only one is required)	Edit Resources that I Manage	Edit resource information, including Regional and resource calendar, for resources that list the current user as the Direct Manager. A resource's Direct Manager is displayed on the View Resource page.
	Edit All Resources	Edit the resource information, including regional and resource calendar, for any resource.
	Edit My Calendar	Allows a resource to edit their own resource calendar.
	View All Resources	Allows the user to view the resource calendar for all resources.
	View My Resource Info Only	Allows a resource to view their own resource calendar, but not edit it.

Chapter

8

Cost and Budget Data Security

In This Chapter:

Overview of Cost and Budget Data Security

This chapter discusses the data and process security related to financial functions (cost and budgets) in the Mercury IT Governance Center.

Configuring data and process security often involves a setting a number parameters: licenses, access grants, entity-level settings, and field-level settings. The following sections discuss the settings required for securing the actions or data related to the Mercury IT Governance Center's Financial Management features.

Screen and function access provided through access grants are cumulative. If a user belongs to three different security groups, he will have all access provided to each of the groups. Therefore, to restrict certain screen and feature access, you need to 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 (using the **Security Group** tab on the User window)
- Remove the access grants from the security group (in the Security Group window). Note: you should only do this if no one in that security group needs the access provided in that access grant.

This chapter discusses how to enable certain functions within the Mercury IT Governance Center. By default, users are not expected to be given access to viewing or modifying information related to budgets or cost. The following chapters provide instructions for enabling the viewing and editing of these functions

Working with Cost Data

Cost data can be associated with tasks, projects, programs, resources, and skills in Mercury IT Governance Center.

Viewing Cost Data

The following access grants are needed to view cost information.

Table 8-1. Access grant for viewing cost data

Access Grant	Description
Cost: View Cost Data	View Cost data related to tasks, projects, programs, resources, and skills. The user must also have access to view these entities.

Enable Cost Data for a Project

If Cost Management is enabled for a project (set in the **Cost Management** tab in the Project Settings window), you can specify who can view the related cost information. This is set in the **Security** tab in the Project Settings window. You can make cost information on the project and tasks available to one of the following options:

- All users
- Project managers for this master project only
- Project managers for the master project and all of the subprojects
- Participants for only the tasks and projects for which they are participants
- Project team only

You must have the Edit Cost Security access grant to change these settings in the Project Settings window.

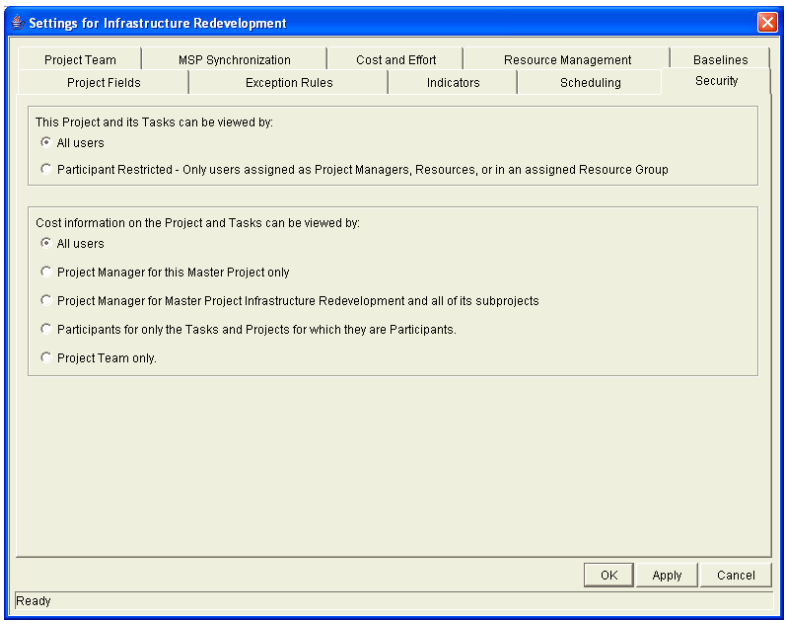


Figure 8-1. Project Settings window - Security tab

Specified users will be able to access the **Cost** and **EV Analysis** tabs on the Project window.

For example: You can provide a granular level of cost data view access by using a combination of Security settings and access grants. You could, for instance, provide All Users with cost data access, but only provide a limited set of users with the View Cost Data access grant.

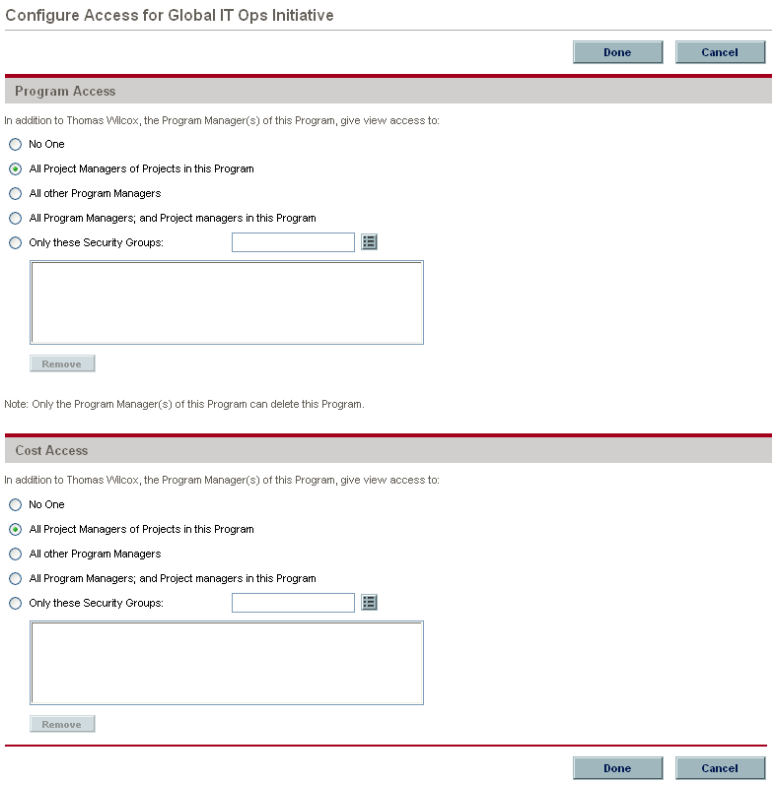
Enable Cost Data for a Program

If Cost Management is enabled for a program, you can specify who can view the related cost information. This is set in the Configure Access for Program page. You can make cost information on the program available to one of the following options:

- 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

Note

You must have the Edit Cost Security access grant to change these settings in the Configure Access for Program page.



Modifying Cost Data

Additional access grants are required to be able to modify cost data. See *Viewing Cost Data* on page 94 for information on enabling users to access (view) the cost information.

Table 8-2. Access grant for modifying cost data

Access Grant	Description
Cost: Edit Cost Data	Edit Cost data related to tasks, projects, programs, resources, and skills. The user must also have access to edit these entities.

Working with Budgets

You can configure users to view, create, or modify budgets. These actions are controlled by a combination of access grants and settings in the Configure Access for Budget page. This page is shown in *Figure 8-2*.

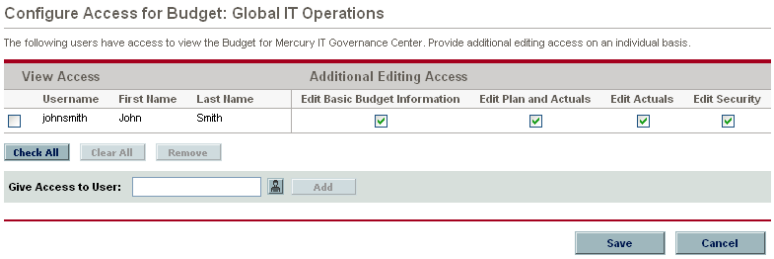


Figure 8-2. Configure Access for Budget page

Viewing Budgets

To allow a user to view a budget, set the following:

Table 8-3. Settings to view budget information

Setting	Value	Description
Access Grant (only one is required)	View Budgets	View budget information when the user has been granted view access in the Configure Access for Budget page.
	View All Budgets	View budget information for all budgets. Note: this grant provides unlimited access to view any budget. Consider using View Budgets to provide more limited view access.
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, set the following:

Table 8-4. Settings to create budgets

Setting	Value	Description
Access Grant	Edit Budgets	Create a new budget.
	Edit All Budgets	Create a new budget.
	Create Budgets (Required)	Create budgets using the standard interface. The user must also have either the Edit Budgets or Edit All Budgets grant to perform this function.

Modifying Budgets

To allow a user to modify budget information, set the following:

Table 8-5. Settings to allow users to modify budgets.

Setting	Value	Description
Access Grant (only one is required)	Edit All Budgets	Edit and delete any budget.
	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 8-5. Settings to allow users to modify budgets.

Setting	Value	Description
Additional Editing Access	Edit Basic Budget Information	Used in conjunction with the Edit Budgets access grant. Allows the user to edit budget header fields, User Data, and notes. He will not be allowed to change the Periods or any information in the Budget Breakdown section.
	Edit Plan and Actuals	Used in conjunction with the Edit Budgets access grant. Allows the user to edit the Periods and the information in the Budget Breakdown section. Additionally, allows users to view and edit the planning and actuals data in the Budget Breakdown table.
	Edit Actuals	Used in conjunction with the Edit Budgets access grant. Allows the user to edit the Periods and the information in the Budget Breakdown section. Additionally, allows users to view and edit the actuals data in the Budget Breakdown table.
	Edit Security	Used in conjunction with the Edit Budgets access grant. Allows the user to edit the list of users who can modify the budgets using the Configure Access for Budget page.

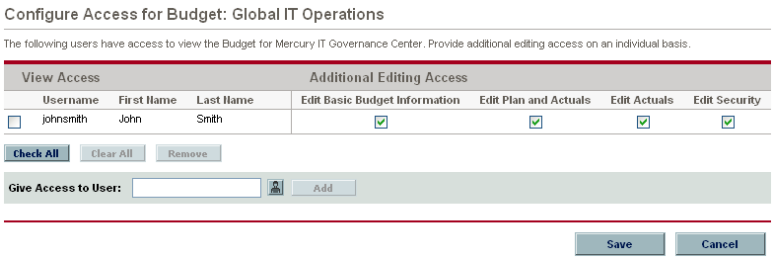


Figure 8-3. Configure Access for Budget page

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 an activity, set the following:

Table 8-6. Access grant to view activity information

Access Grant	Description
Proj Mgmt: View Activities	View activity information.

Creating and Modifying Activities

To allow a user to create or modify an activity, set the following:

Table 8-7. Access grant to create an activity

Access Grant	Description
Proj Mgmt: Manage Activities	View, create, edit, or delete activities.

Working with Regions

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

Viewing Regions

To allow a user to view a region, set the following:

Table 8-8. Access grant to view region information

Access Grant	Description
Resource Mgmt: View Regions	View region information.

Creating and Modifying Regions

To allow a user to create or modify a region, set the following:

Table 8-9. Access grant to create a region

Access Grant	Description
Resource Mgmt: Manage Regions	View, create, edit, or delete regions.

Working with FX Rates and Currencies

You can configure users to view, create, or modify FX rates. These actions are controlled by access grants. The same access grants also control access to currency modification.

Viewing FX Rates

To allow a user to view an FX rate, set the following:

Table 8-10. Access grant to view FX rate information

Access Grant	Description
Financial Mgmt: View FX Rates	View FX rate information.

Creating and Modifying FX Rates

To allow a user to create or modify an FX rate, set the following:

Table 8-11. Access grant to create a region

Access Grant	Description
Financial Mgmt: Manage FX Rates	View, create, edit, or delete FX rates.

Chapter

9

Dashboard Security

In This Chapter:

Overview of Dashboard Security

The Mercury IT Governance Dashboard provides users with quick access to Mercury IT Governance Center data through the inclusion of a number of system and custom portlets on their Dashboards.

Controlling User Access to Portlets

You can control portlet user access at two levels:

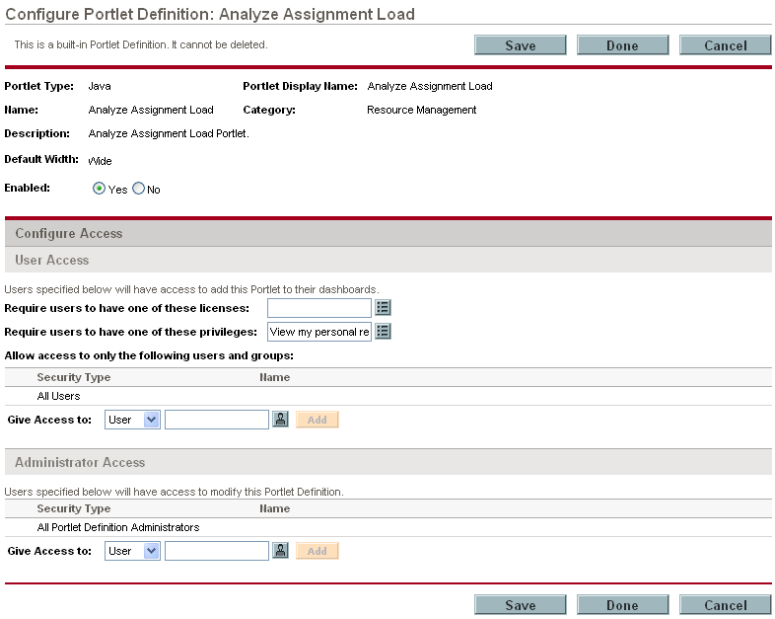
- *Disabling Portlets*
- *Restricting User Access*

Disabling Portlets

You can disable custom-built portlets at your site.

To disable a portlet:

1. In the standard interface, select **Administration > Portlet Definitions > Configure Portlet Definitions.**
2. Search for and open the portlet definition that you would like to disable.



3. Click **No** for the Enabled option.

Note

If there are any users currently using the portlet on their Dashboard, disabling the portlet will delete it from their Dashboards.

4. Click **Save.**

Restricting User Access

You can control which users can add a portlet to their Dashboard. For example, you may want to restrict the package-related portlets to only members involved in the deployments. Enabling only the portlets that a specific user needs will make it easier for that user to personalize their Dashboard, because there are fewer (non-relevant) portlets to choose from.

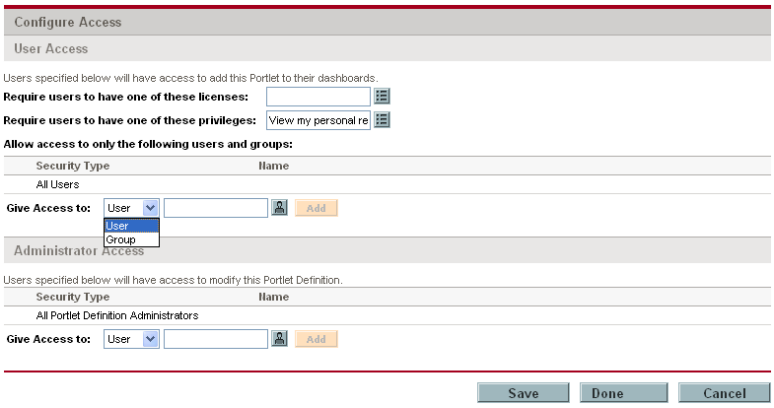
To specify which users can use the portlet on their Dashboard:

1. In the standard interface, select **Administration > Portlet Definitions > Configure Portlet Definitions.**

2. Search for and open the portlet definition that you would like to configure.

3. Scroll to the **Configure Access** section.

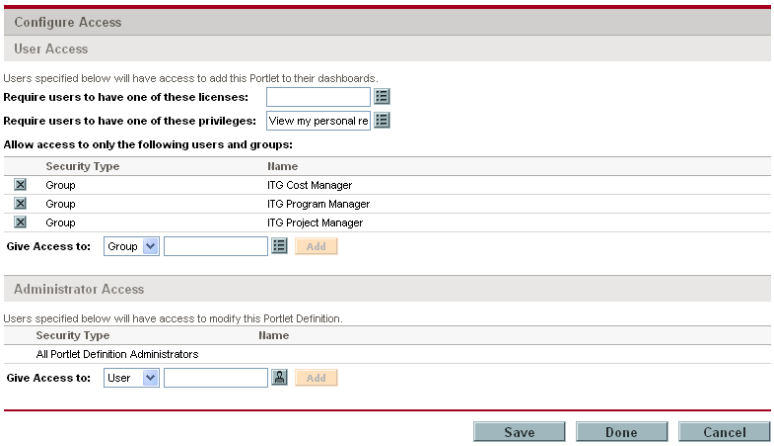
   For system portlets, the **Help Content** tab is the only displayed tab.



4. From the Give Access to drop-down list, select **User** or **Group.**

5. Select the desired users or security groups and click **Add.**

   They are added to the **Configure Access** section.



6. 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 Dashboard.

Access can also be restricted by choosing a specific license or access grant from the Require users to have one of these licenses/privileges fields. Only users with the specified licenses or access grants can add this portlet to their Dashboard.

You can restrict user access for both custom and system portlets.

Restricting Data to Participants

The Mercury IT Governance Center Dashboard respects any participant restrictions configured for requests, packages or projects. When these items are restricted, only users who are directly involved with them can view their data on the Dashboard. Restricted items will not be displayed in portlets or returned in searches.

The participant-restriction model is supported by all of Mercury IT Governance Center's system portlets. Custom portlets are not supported. They will display whatever information is specified in the SQL query that defines the portlet.

Chapter

10

Configuration Security

In This Chapter:

Overview of Configuration Security

Security can be set around the Mercury IT Governance Center's configuration entities. This includes such activities as controlling:

- Who can change a workflow
- Who can change each object type
- Who can change request types
- Who can change user and security group definitions

Setting Ownership for Configuration Entities

Different groups of users in Mercury IT Governance Center have ownership and control over the configuration entities. These groups are referred to as ownership groups. Unless a "global" permission has been designated to all users for an entity, members of ownership groups are the only users who have the right to edit, delete or copy that entity. The ownership groups must also have the proper access grant for the entity in order to complete those tasks. For example, the Edit Workflows access grant is needed 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 select to 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

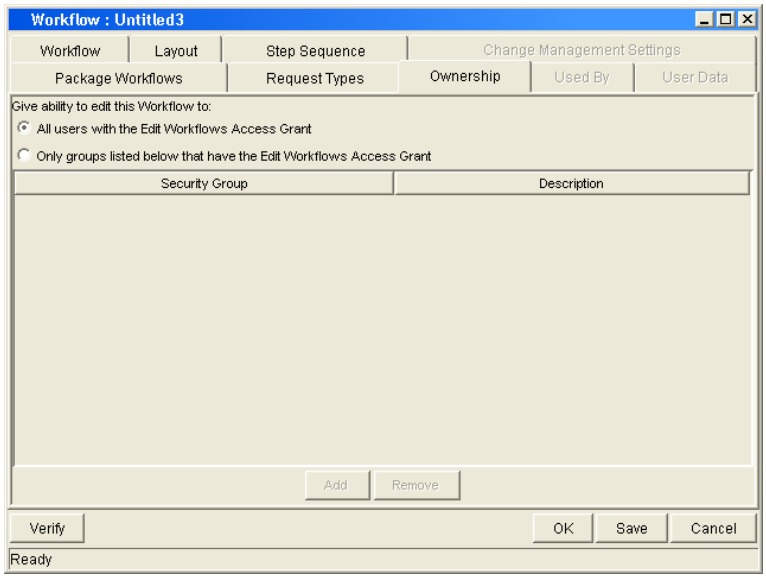
The Ownership setting is accessed through the individual entity windows in the Workbench.

For example, to set the Ownership for workflows:

1. Open the workflow.
2. Click the **Ownership** tab.
3. Click the Only groups listed below that have the Edit Workflows Access Grant radio button.
4. Click **Add.**

   The Add Security Group window opens.
5. Select the Security Group.
6. Click **Add** to add the current security group and continue adding more security groups. Click **OK** to add the current security group and close the Add Security Group window.

   The security group(s) you selected displays in the **Ownership** tab under the Security Group column.



7. Click **OK** to save the selection and close the Workflow window. Click **Save** to save the selection and leave the Workflow window open.

Note

The System: Ownership Override access grant allows the user to access and edit configuration entities even if he is not a member of one of the entity's ownership groups. This access grant should be given only to superusers who may need 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 either:

- 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). Note: You should only do this if no one in that security group needs the access provided in that access grant.

The following table lists the access grants that provide edit access to different configuration entities.

Table 10-1. Access grants for editing Mercury IT Governance Center configuration entities

Category	Access Grant Name	Description
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 Commands 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 Validations 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.
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.
Change Mgmt	Edit Object Types	Create, edit, and delete object types in the Object Types Workbench.
Project Mgmt	Edit Calendars	Create, edit, and delete project calendars in the Projects Workbench.
Project Mgmt	Edit Project Templates	Create, edit, and delete project templates in the Project Templates Workbench.
Project Mgmt	Edit Projects	Create projects using the Projects Workbench. Update and delete projects and subprojects when specified as the project manager.
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 Dashboard pages.
Sys Admin	Distribute Modules	Distribute Dashboard pages to users.

Table 10-1. Access grants for editing Mercury IT Governance Center configuration entities

Category	Access Grant Name	Description
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 Activities	Create, edit, and delete activities in the Activities 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 Mgmt Settings	Edit Time Management settings for a user in the Time Mgmt Settings Workbench. Also enables the **Time Management Settings** button in the User window.

Appendix A
Access Grants

Access grants enable certain activities within Mercury IT Governance Center. Mercury IT Governance Center comes with a pre-defined list of access grants. Installing a Mercury Change Management Extension may introduce additional access grants. *Table A-1* lists the available access grants and provides a description of each grant.

Note

View access grants provide read-only access to screens and entities. Users without the **View** access grant will be unable to see certain workbenches or 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.

Manage access grants typically enable the same functions as the Edit access grants (create, modifying, and deleting), but are less restricted. For example, if you have the Manage Requests access grant, you can delete any request in the system that you can access, even if you did not create the request.

Refer to *Table A-1* for the details on the specific access grant.

Table A-1. Access grants

Category	Access Grant Name	Description
Change Mgmt	Edit Object Types	Create, edit, and delete object types in the Object Types Workbench.
Change Mgmt	Edit Packages	Perform basic package processing actions: create, edit certain related packages, and delete certain unsubmitted packages. • 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.
Change Mgmt	Edit Releases	Perform basic release processing actions in the Releases Workbench: create, edit, process, and delete certain related releases. Users with this grant can: • View any release • Be designated as the release manager in the Release window • Create releases • Edit or delete any release that they created • Act on any Distribution workflow steps where they are included in the step's security. • Edit or delete a release that they did not create (only when they are designated as the release manager in the Release Management window).
Change Mgmt	Manage Packages	Edit or delete any packages.
Change Mgmt	Manage Releases	Create, edit and delete any release using the Releases Workbench. Users with this grant can: • Create a release • Be designated as the release manager in the Release window • Edit or delete any release in Mercury IT Governance Center (regardless of whether they are specified as the release manager in the Release Management window).
Change Mgmt	Override Change Mgmt Participant Restriction	View the detailed information on a restricted package for which the user is not an active participant.

Table A-1. Access grants [continued]

Category	Access Grant Name	Description
Change Mgmt	Submit Environment Refreshes	Create and submit an Environment Refresh in the Env Refresh Workbench.
Change Mgmt	View Environment Refreshes	View Environment Refresh definitions in the Env Refresh Workbench.
Change Mgmt	View Object Types	View object type definitions in the Object Types Workbench.
Change Mgmt	View Packages	View packages in the standard interface or the Workbench.
Change Mgmt	View Releases	View release definitions in the Releases Workbench. Act on any Distribution workflow steps where the user is included in the step's security.
Config	Edit Activities	Create, update, and delete 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 Commands 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.
Config	View Report Types	View report type definitions in the the Report Types Workbench.
Config	View Special Commands	View special command definitions in the Special Commands Workbench.
Config	View User Data	View User Data definitions in the User Data Workbench.
Config	View Validations	View validations in the Validations Workbench.

Table A-1. Access grants [continued]

Category	Access Grant Name	Description
Config	View Workflows	View workflow definitions in the Workflows Workbench.
Demand Mgmt	Edit Contacts	Create and update Contacts in the Contacts Workbench.
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 your unsubmitted requests. • 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 in the **User Access** tab on the Request Type window. • Allows the user to delete the request as specified in the **User Access** tab on the Request Type window. • Allows the user to cancel the request as specified in the **User Access** tab on the Request Type window.
Demand Mgmt	Manage Contacts	Edit and delete Contacts using the Contacts Workbench.
Demand Mgmt	Manage Demands	Access the Demand Management scheduling functions, the consolidated picture of demand, and all other Demand Management menu items related to scheduling or managing demand.
Demand Mgmt	Manage 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	Override Demand Mgmt Participant Restriction	Allows the user to review a request regardless of whether the user is allowed to view or not as defined in 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.

Table A-1. Access grants [continued]

Category	Access Grant Name	Description
Demand Mgmt	View Contacts	View the Contact definition in the Contacts 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.
Demand Mgmt	View Requests	View request type definitions in the Request Types Workbench.
Environments	Edit Environments	Create, update and delete Environments in the Environments Workbench.
Environments	View Environments	View Environment definitions in the Environments Workbench.
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** only appears in the Budget Status list if you have this grant.
Financial Mgmt	Approve Financial Benefits	The user can set the Financial Benefit Status to **Approved**, but nothing else. Supplemental to the Edit Financial Benefits or Edit All Financial Benefits access 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. Supplemental to the Edit Financial Benefits or Edit All Financial Benefits access grant.
Financial Mgmt	Edit All Budgets	Edit budget information for all budgets in Mercury IT Governance Center.
Financial Mgmt	Edit All Financial Benefits	The user can edit any financial benefit in the system.
Financial Mgmt	Edit Budgets	Edit budget information when the user has been granted edit access in the Configure Access for Budget page.
Financial Mgmt	Edit Cost Data	Edit Cost data related to tasks, projects, programs, resources and skills. The user must also have access to edit these entities.

Table A-1. Access grants [continued]

Category	Access Grant Name	Description
Financial Mgmt	Edit Cost Security	Edit Cost security settings for a project in the Project Settings window. Edit Cost security settings for a program in the Program Security Configuration page. Note: The user must also be able to edit the project settings and program security in order for this grant to be relevant.
Financial Mgmt	Edit Financial Benefits	The user can edit any financial benefit for which they are on the specified Edit list.
Financial Mgmt	Manage Financial Exchange Rates	The user can create and update Financial Exchange Rates.
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 perform this function.
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 Mercury IT Governance 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 in the Configure Access for Budget page.
Financial Mgmt	View Cost Data	View Cost data related to tasks, projects, programs, resources, and skills. The user must also have access to view these entities.
Financial Mgmt	View Financial Benefits	The user can view any financial benefit for which they are on the specified View or Edit list.
Financial Mgmt	View Financial Exchange Rates	The user can view Financial Exchange Rates.
PMO	Edit Programs	Update programs where the user is specified as the program manager.
PMO	Manage Programs	Create and update any program.
PMO	View Programs	View program definitions.
Portfolio Mgmt	Configure Portfolio Management	Provides the user with access to the Configure Portfolio Management page where they can set portfolio tracking and categorization metrics.

Table A-1. Access grants [continued]

Category	Access Grant Name	Description
Portfolio Mgmt	Edit Scenario Comparisons	The user can view, edit, and delete any scenario comparison for which they are on the specified Edit list, as well as create new scenario comparisons.
Portfolio Mgmt	Manage Scenario Comparisons	The user can view, edit, and delete any scenario comparisons in the system, as well as 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, and Resource by Category.
Portfolio Mgmt	View Scenario Comparison	The user can view any scenario comparison for which they are on the specified View or Edit list.
Project Mgmt	Edit Project Templates	Create, update, and delete project templates in the Project Templates Workbench.
Project Mgmt	Edit Projects	Create projects using the Projects Workbench. Update and delete projects and subprojects when specified as the project manager.
Project Mgmt	Manage Projects	Create, edit, and delete projects. Override (or remove) references on projects or tasks.
Project Mgmt	Override Project Mgmt Participant Restriction	View the detailed information on a restricted project for which the user is not an active participant.
Project Mgmt	Update Tasks	Update project tasks using the Projects Workbench or Dashboard.
Project Mgmt	View Project Templates	View project templates in the Project Templates Workbench.
Project Mgmt	View Projects	View project definitions in the Projects Workbench and standard interface.
Resource Mgmt	Approve Resource Pools	Change the Resource Pool Status value on the Modify Resource Pool page to **Approved.** The user must also have the Update Resource Pool Status grant and either the Edit Resource Pools or Edit All Resource Pools grant to perform this function. Note that **Approved** only appears in the Resource Pool Status list if you have this grant.

Table A-1. Access grants [continued]

Category	Access Grant Name	Description
Resource Mgmt	Approve Staffing Profiles	Change the Staffing Profile Status value on the Modify Staffing Profile page to **Approved.** The user must also have the Update Staffing Profile Status grant and either the Edit Staffing Profiles or Edit All Staffing Profiles grant to perform this function. Note that **Approved** only appears in the Staffing Profile Status list if you have this grant.
Resource Mgmt	Create Resource Pools	Create resource pools using the standard interface. The user must also have either the Edit Resource Pools or Edit All Resource Pools grant to perform this function.
Resource Mgmt	Create Staffing Profiles	Create staffing profiles using the standard interface. The user must also have either the Edit Staffing Profiles or Edit All Staffing Profiles grant to perform this function.
Resource Mgmt	Edit All Resource Pools	Edit and delete any resource pool.
Resource Mgmt	Edit All Resources	Edit the resource information for any resource defined in Mercury IT Governance Center.
Resource Mgmt	Edit All Skills	Create, edit, and delete all skills defined in Mercury IT Governance Center.
Resource Mgmt	Edit All Staffing Profiles	Edit and delete any staffing profile.
Resource Mgmt	Edit Entire Organization	Edit and delete any organization unit.
Resource Mgmt	Edit My Calendar	The user can edit their 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 Mercury IT Governance Center.
Resource Mgmt	Edit Resource Pools	Edit resource pool information when the user has been granted edit access in the Configure Access for Resource Pool page. Delete these resource pools when given sufficient access in the Configure Access for Resource Pool page for that resource pool.

Table A-1. Access grants [continued]

Category	Access Grant Name	Description
Resource Mgmt	Edit Staffing Profiles	Edit staffing profile information when the user has been granted edit access in 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.
Resource Mgmt	Manage Regions	Create, edit, and delete all regions defined in Mercury IT Governance Center.
Resource Mgmt	Update Resource Pool Status	Change the Resource Pool Status value on the Modify Resource Pool page. The user must also have either the Edit Resource Pools or Edit All Resource Pools grant to utilize this grant.
Resource Mgmt	Update Staffing Profile Status	Change the Staffing Profile Status value on the Modify Staffing Profile page. The user must also have either the Edit Staffing Profiles or Edit All Staffing Profiles grant to utilize this 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 Mercury IT Governance Center.
Resource Mgmt	View All Skills	View all skills defined in Mercury IT Governance Center.
Resource Mgmt	View All Staffing Profiles	View staffing profile information for all staffing profiles.
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 Mercury IT Governance Center.
Resource Mgmt	View Regions	View all regions defined in Mercury IT Governance Center.
Resource Mgmt	View Resource Pools	View resource pool information when the user has been granted view access in the Configure Access for Resource Pool page.
Resource Mgmt	View Staffing Profiles	View staffing profile information when the user has been granted view access in the Configure Access for Staffing Profile page.

Table A-1. Access grants [continued]

Category	Access Grant Name	Description
Sys Admin	Configure Modules	Create, edit, and delete modules in Module Configuration in the Dashboard page. View and set the default dashboard in Set Default Dashboard in the Dashboard page.
Sys Admin	Distribute Modules	View, publish, and distribute modules, pages and portlets to dashboards in the Distributing Modules Dashboard page.
Sys Admin	Edit Security Groups	Create, update, and delete security groups in the Security Groups Workbench.
Sys Admin	Edit Users	Create, update, and delete users in the Users Workbench.
Sys Admin	Migrate Kintana Objects	Migrate configuration objects (such as workflows and request types) using the Migrators.
Sys Admin	Server Administrator	Stop the Mercury IT Governance Center server, logon 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.
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	Manage Reports	Delete any submitted report using the Reports Workbench.
System	Open Workbench	Open the Mercury IT Governance Center Workbench.

Table A-1. Access grants [continued]

Category	Access Grant Name	Description
System	Override Key Fields Segmentation	View all information contained in restricted key fields. Key fields include: • Resource and Resource Group fields in Mercury Project Management tasks • Assigned User, Assigned Group and Contacts fields in Mercury Demand Management requests • Assigned User and Assigned Group fields in Mercury Change 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 Mercury IT Governance Center.
System	View Portlet Definition	View portlet definitions in the Portlets Workbench.
Time Mgmt	Approve Time Sheets	Approve or reject time Sheets when the resource is a direct report or when the time sheet has been Delegated To the user.
Time Mgmt	Close Time Sheets	Close or freeze time sheets when the resource is a direct report or when the time sheet has been Delegated To the user.
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 Time Mgmt Settings	Edit Time Management settings for a user in the Time Mgmt Settings Workbench. Also enables the **Time Management Settings** button in the User window.
Time Mgmt	Edit Time Sheets	Edit time sheets when the resource is a direct report or when the time sheet has been Delegated To the user.
Time Mgmt	Edit Time Sheet Policies	Create, modify, and delete time sheet policies in the Time Sheet Policy Workbench.
Time Mgmt	Edit Work Allocations	View and edit Work Allocations. The user can also close or delete allocations he created.
Time Mgmt	Manage 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.

Table A-1. Access grants [continued]

Category	Access Grant Name	Description
Time Mgmt	View Override Rules	View Override Rules in the Override Rules Workbench.
Time Mgmt	View Time Mgmt Settings	View Time Management settings for a user in the Time Mgmt Settings Workbench. Also enables the **Time Management Settings** button in the User window.
Time Mgmt	View Time Sheet Policies	View time sheet policies in Mercury IT Governance Center.
Time Mgmt	View Time Sheets	View a user's time sheet information.
Time Mgmt	View Work Allocations	View Work Allocations in Mercury Time Management.

Appendix B
License Types

In This Appendix:

Overview of License Types

This appendix discusses the license types available for Mercury IT Governance Center. It defines the types of available licenses: Product, Configuration, and User Administration.

License Types

Each user must have a license to log onto Mercury IT Governance Center. Mercury IT Governance Center offers three types of named user licenses: Product, Configuration, and User Administration. Each license type is meant to suit different business needs and responsibilities, and therefore grants a different set of functionality.

- Product licenses

  Product licenses are used by users who require basic product features and access to data. Product licenses provide access to Mercury IT Governance Center features in the standard HTML interface including the Mercury IT Governance Dashboard™, as well as the Workbench interface depending on the product license being used.

  The following product licenses exist:

  - Demand Management
  - Project Management
  - Program Management (requires Demand Management)
  - Portfolio Management (requires Demand Management and Project Management)
  - Change Management
  - Time Management
  - Configuration license

  The Configuration license is used by users who configure the Mercury IT Governance Center. The Configuration license provides access to nearly all

product features through both the Workbench and the standard (HTML) interface.

The Configuration license implicitly provides a user with access to all product features available to a product license user, as well as more advanced configuration functionality through Workbench. For example, a user with a Configuration license does not require an additional Project Management Product license to perform the tasks associated with Project Management; for example, updating tasks in the standard interface.

- User Administration license

  The User Administration license is used by users responsible for administering the Mercury IT Governance Center's users and security, as well as the application itself. It is required to configure user accounts and security groups, as well as run reports related to importing new users through the Open Interface. This license also provides a user with access to the System Administration functionality for the Mercury IT Governance Center licensed at your site.

User access to screens and functions in Mercury IT Governance Center are controlled by a combination of license and access grants. The following sections discuss only the licenses required to perform specific actions. For additional details on access grants which are also required, refer to the access grant documentation in *Access Grants* on page 115.

Change Management Extension Licenses

Mercury Change Management Extension licenses are provided on a site-license basis (that is, they do not have to be associated with individual users). Extension licenses enable additional screens and fields in Mercury IT Governance Center. See the documentation for the Extensions installed at your site for details.

Appendix C
Licenses and User Roles

This appendix discusses the typical user functions and required licenses by user types and by product/license type. In the following tables, the following convention is used to denote license type:

- P = Product License
- C = Configuration License
- U = User Administration License

Table C-1 lists the product licenses by user type. *Table C-2* lists the user roles and functions by product/license types.

Table C-1. Product Licenses by User Type

	User Type	Functions Performed	Demand Mgmt	Portfolio Mgmt	Program Mgmt	Project Mgmt	Time Mgmt	Change Mgmt
Line of Business	Business End-User	Submit requests, monitor status of own requests, and provide user sign-off.	P					
	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. Sync with MS Project.	P		P	P	(P)	
	Business Analyst	Monitor status of initiatives (schedule and cost); act on SLA exceptions; track issues; manage scope changes, issues, and risk. Manage portfolio.	P	P	P	P		
	Business Manager	Monitor status of initiatives (schedule, cost, earned value), act on SLA exceptions, prioritize portfolio.	P	P	P	P		

Table C-1. Product Licenses by User Type [continued]

	User Type	Functions Performed	Demand Mgmt	Portfolio Mgmt	Program Mgmt	Project Mgmt	Time Mgmt	Change Mgmt
IT	IT Management: CIOs, VPs of IT, Directors, Enterprise Architects, CTO...	Monitor status of initiatives (schedule and cost), drill down on SA exceptions, control and prioritize portfolio, monitor resource utilization—manage resource capacity and IT budgets.	P	P	P	P	(P)	(P)
	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.	P			P	(P)	
	Engineering Team: Developer, Infrastructure (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.						P
	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.	P	P	P	P	(P)	
	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. Sync with MS Project (if needed).				P	(P)	
	Mercury ITG User Administrator	Perform common administration functions like setting up users and assigning security.	U					

Table C-1. Product Licenses by User Type [continued]

	User Type	Functions Performed	Demand Mgmt	Portfolio Mgmt	Program Mgmt	Project Mgmt	Time Mgmt	Change Mgmt
	Mercury ITG Administrator, Process Owner / Implementer	Perform common administration functions like configuring user-defined project information, and configuring report types and Dashboard portlets. Configure object types, model process workflows; and configure business rules.	C					

Table C-2. User Roles and Functions by Product/License Type

Product	License Type	User Type	Primary Tasks Performed with this License Type
Dashboard	Any	All users	Overall visibility of status and metrics, drill down to appropriate level of detail on requests, task, projects, and packages requiring action or further review.
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 utilization. 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 change management process.
Portfolio Management	Portfolio Management	Portfolio Manager, Business Analyst, Program Manager, Enterprise Architect, CTO, IT Controller	Manage IT portfolio. Play 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.
Program Management	Program Management	Program Manager	Prioritize programs and projects. Manage program and project initiation process; 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 [continued]

Product	License Type	User Type	Primary Tasks Performed with this License Type
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.
		Task owner, Project Participant	Execute and update project tasks.
		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.
Resource Management	Project Management, Demand Management	IT Management, Project Manager, IT HR	Base functionality is included with the IT Governance 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.
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 stat-end dates and periods, and approval hierarchies.

Table C-2. User Roles and Functions by Product/License Type [continued]

Product	License Type	User Type	Primary Tasks Performed with this License Type
Financial Management	Project Mgmt, Demand Mgmt	All Users	Base functionality is included with the IT Governance Center Foundation and supports the ability to view budgets and associated visualizations.
	Portfolio Management or Program Management or Project Management	Portfolio Manager, Program Manager, Project Manager	Create and update budgets.
		IT Management, Portfolio Manager, Program Manager, Project Manager, Business Analyst	Display earned value analysis information and visualization.
Change Management	Change Management	Developer	Create and update packages for deployment, monitor package status.
		DBA, Sys Admin, Config. 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 Management Analyst	Configure object types and workflows.
	Change Management	IT Manager, QA and Business Analyst	View that status of deployment packages and perform QA approvals.
All Products	User Administration	Mercury ITG Administrator	Set up users, manage licenses, assign security.
All Products	Configuration	Mercury ITG Configurer	Create and configure report types, portlets, request types, request header types, object types, workflows, Environments, validations, activities. Configure security for standard portlets.

Index

O

P

R

S

T

U

W