

Mercury IT Governance Center™

**Security Model
Guide and Reference**

Version: 7.0



This manual, and the accompanying software and other documentation, is protected by U.S. and international copyright laws, and may be used only in accordance with the accompanying license agreement. Features of the software, and of other products and services of Mercury Interactive Corporation, may be covered by one or more of the following patents: United States: 5,511,185; 5,657,438; 5,701,139; 5,870,559; 5,958,008; 5,974,572; 6,137,782; 6,138,157; 6,144,962; 6,205,122; 6,237,006; 6,341,310; 6,360,332; 6,449,739; 6,470,383; 6,477,483; 6,549,944; 6,560,564; 6,564,342; 6,587,969; 6,631,408; 6,631,411; 6,633,912; 6,694,288; 6,738,813; 6,738,933; 6,754,701; 6,792,460 and 6,810,494. Australia: 763468 and 762554. Other patents pending. All rights reserved.

U.S. GOVERNMENT RESTRICTED RIGHTS. This Software Documentation is a “commercial item” as defined at 48 C.F.R. 2.101 (October 1995). In accordance with 48 C.F.R. 12.212 (October 1995), 48 C.F.R. 27.401 through 27.404 and 52.227-14 (June 1987, as amended) and 48 C.F.R. 227.7201 through 227.7204 (June 1995), and any similar provisions in the supplements to Title 48 of the C.F.R. (the “Federal Acquisition Regulation”) of other entities of the U.S. Government, as applicable, all U.S. Government users acquire and may use this Documentation only in accordance with the restricted rights set forth in the license agreement applicable to the Computer Software to which this Documentation relates.

Mercury, Mercury Interactive, the Mercury logo, the Mercury Interactive logo, LoadRunner, WinRunner, SiteScope and TestDirector are trademarks of Mercury Interactive Corporation and may be registered in certain jurisdictions. The absence of a trademark from this list does not constitute a waiver of Mercury's intellectual property rights concerning that trademark.

All other company, brand and product names may be trademarks or registered trademarks of their respective holders. Mercury disclaims any responsibility for specifying which marks are owned by which companies or which organizations.

Mercury provides links to external third-party Web sites to help you find supplemental information. The content and availability may change without notice. Mercury makes no representations or warranties whatsoever as to the content or availability.

Mercury
379 North Whisman Road
Mountain View, CA 94043
<http://www.mercury.com>

© 1997–2006 Mercury Interactive Corporation. All rights reserved.

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

Table of Contents

List of Figures	vii
List of Tables	ix
Chapter 1: Getting Started with the Mercury IT Governance Center Security Model	11
Introduction to the Mercury IT Governance Center Security Model.....	12
Security-Related Features in Mercury IT Governance Center.....	13
Providing Access to the Mercury IT Governance Applications	14
Related Documents.....	15
Chapter 2: Users and Security Groups	17
Creating Users	18
Creating a User	18
Linking Users to Security Groups.....	23
Configuring Resource Information.....	26
Importing Users from a Database or LDAP Server	26
Creating Security Groups.....	27
Creating a Security Group by Specifying a List of Users	29
Using Resource Management to Control User Security	33
Using the Deployment Management App Codes Tab	34
Using the Charge Code Rules Tab.....	35
Chapter 3: Managing Mercury IT Governance Licenses	37
Overview of License Management.....	38
Assigning Licenses from the User Workbench.....	38
Assigning Licenses to Multiple Users in the License Workbench	40
Removing Licenses Using the Assign Licenses Wizard	43

Assigning Licenses Using the Open Interface	44
Chapter 4: Request Security.....	45
Overview of Request Security	46
Prerequisite Settings for Users and Security Groups	47
Licenses	47
Access Grants.....	48
Viewing a Request	49
Creating a Request.....	52
Enabling Users to Create Requests	52
Restricting Users from Selecting a Specific Workflow	55
Processing a Request	57
Enabling Users to Edit Fields on a Request.....	57
Enabling Users to Cancel or Delete a Request.....	59
Enabling Users to Act on a Specific Workflow Step	62
Viewing and Editing Fields on a Request.....	65
Field-Level Data Security Overview	65
Field Window: Attributes Tab.....	67
Field Window: Security Tab	68
Request Type Window: Status Dependencies Tab.....	71
Overriding Request Security	72
Chapter 5: Project and Task Security	73
Overview of Project and Task Security.....	74
Viewing Projects and Tasks	75
Controlling Resources on the Project	77
Creating Projects.....	77
Editing Project and Task Information.....	78
Updating Tasks	79
Overriding Project Security	80
Chapter 6: Package Security.....	81
Overview of Package Security.....	82
Viewing a Package.....	83
Restricting Package Viewing to Participants.....	84
Creating a Package	84
Enabling Users to Create Packages.....	84
Preventing Users from Selecting a Specific Workflow	86
Preventing Users from Selecting a Specific Object Type	86

Approving Package Lines.....	87
Enabling Users to Act on a Specific Workflow Step.....	87
Deleting a Package.....	88
Overriding Package Security.....	88
Chapter 7: Resource Management Security.....	89
Overview of Resource Management Security.....	90
Working with Resources.....	91
Viewing Resource Information.....	91
Modifying Resource Information.....	91
Working with Resource Pools.....	92
Viewing Resource Pools.....	92
Creating Resource Pools.....	93
Modifying Resource Pools.....	93
Working with Skills.....	94
Viewing Skills.....	94
Creating, Modifying, and Deleting Skills.....	94
Working with the Organization Model.....	95
Viewing the Organization Model.....	95
Modifying Organization Definitions.....	95
Working with Staffing Profiles.....	96
Viewing Staffing Profiles.....	96
Creating Staffing Profiles.....	97
Modifying Staffing Profiles.....	97
Working with Calendars.....	99
Viewing and Editing Regional Calendars.....	99
Viewing and Editing Resource Calendars.....	100
Additional Protection for Resource Information.....	101
Users Who Are Assigned the Configurator License.....	101
Members of Security Groups with View or Edit Access to Cost Data.....	101
Members of Security Groups with View or Edit Access to Resource Data.....	101
Users Who Have the Administrator Password.....	102
Users Who Run the Unsecured “User Detail Report”.....	102
Users Who Are Assigned the Sys Admin: Server Tools - Execute SQL Runner Access Grant.....	102
Chapter 8: Cost and Budget Data Security.....	103
Overview of Cost and Budget Data Security.....	104
Working with Cost Data.....	104
Viewing Cost Data.....	104
Making Project Cost Data Visible to Users.....	105
Making Program Cost Data Visible to Users.....	106

Modifying Cost Data.....	107
Working with Budgets.....	108
Viewing Budgets.....	108
Creating Budgets.....	109
Modifying Budgets.....	110
Working with Activities.....	111
Viewing Activities.....	111
Creating and Modifying Activities.....	111
Working with Regions.....	111
Working with Financial Exchange Rates and Currencies.....	112
Chapter 9: Dashboard Security.....	113
Controlling User Access to Portlets in the Dashboard.....	114
Disabling Custom Portlets.....	114
Restricting User Access.....	115
Restricting Data to Participants.....	116
Chapter 10: Configuration Security.....	117
Overview of Configuration Security.....	118
Setting Ownership for Configuration Entities.....	118
Removing Access Grants.....	121
Chapter 11: Service Provider Functionality.....	125
Recommended Practice: Service Provider Functionality.....	126
Appendix A: Access Grants.....	131
Appendix B: License Types.....	145
License Types.....	146
Deployment Management Extension Licenses.....	147
Appendix C: Licenses and User Roles.....	149
Index.....	155

List of Figures

Figure 4-1	Field visibility interactions	66
Figure 7-1	Configure Access for Resource Pool page.....	92
Figure 7-2	Configure Access for Resource Pool page.....	94
Figure 7-3	Configure Access for Staffing Profile page	96
Figure 7-4	Configure Access for Staffing Profile page	98
Figure 8-1	Project Security section of the Project Settings page	105
Figure 8-2	Configure Access page for programs.....	107
Figure 8-3	Configure Access for Budget page.....	108
Figure 8-4	Configure Access for Budget page.....	111

List of Tables

Table 2-1	User window: Fields on the User Information tab	21
Table 2-2	Options used to associate security groups and entities	30
Table 2-3	Security Group window - Charge Code Rules tab fields.....	35
Table 3-1	License Administration wizard - Find Users step	41
Table 4-1	Access grants related to request creation and processing.....	48
Table 4-2	Settings required to override request security.....	72
Table 5-1	Settings required to view projects and tasks	75
Table 5-2	Settings to restrict a user from viewing projects and tasks	76
Table 5-3	Settings required to create a project	77
Table 5-4	Settings required to edit a project.....	78
Table 5-5	Settings required to update tasks.....	79
Table 5-6	Settings to restrict a user from updating tasks.....	79
Table 5-7	Settings to override request security	80
Table 6-1	Settings to view packages.....	83
Table 6-2	Settings to enable package creation.....	85
Table 6-3	Settings to restrict workflow selection.....	86
Table 6-4	Settings to restrict object type selection	86
Table 6-5	Settings to enable package processing.....	87
Table 6-6	Settings required to enable a user to delete packages.....	88
Table 6-7	Settings to override package security	88
Table 7-1	Settings to allow users to view resource information.....	91
Table 7-2	Settings to allow users to modify resource information.....	91

List of Tables

Table 7-3	Settings to allow users to view resource pool information.....	92
Table 7-4	Settings to allow users to create resource pools.....	93
Table 7-5	Settings to allow users to modify resource pools.....	93
Table 7-6	Settings to modify organization information.....	95
Table 7-7	Settings to allow users to view resource pool information.....	96
Table 7-8	Settings to allow users to create staffing profiles	97
Table 7-9	Settings to allow users to modify staffing profiles.....	97
Table 7-10	Settings to allow users to view or edit regional calendars.....	99
Table 7-11	Settings to allow users to modify resource information.....	100
Table 8-1	Settings to view budget information	108
Table 8-2	Settings to create budgets.....	109
Table 8-3	Settings to allow users to modify budgets.....	110
Table 8-4	Access grants for working with regions	111
Table 8-5	Access grants for working with financial exchange rates.....	112
Table 10-1	Access grants for editing configuration entities	121
Table A-1	Access grants.....	131
Table C-1	Product licenses by user type	149
Table C-2	User roles and functions by product license type	152

Chapter

1

Getting Started with the Mercury IT Governance Center Security Model

In This Chapter:

- *Introduction to the Mercury IT Governance Center Security Model*
 - *Security-Related Features in Mercury IT Governance Center*
 - *Providing Access to the Mercury IT Governance Dashboard*
 - *Providing Access to Mercury IT Governance Center Products*
 - *Related Documents*
-

Introduction to the Mercury IT Governance Center Security Model

Businesses must often control access to information and business processes. This can be done to protect sensitive data, 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 limit the following:

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

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

Security-Related Features in Mercury IT Governance Center

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

- **Licenses**

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

[Chapter 3, *Managing Mercury IT Governance Licenses*, on page 37](#) provides instructions on how to assign licenses to individual users or to groups of users. [Appendix B, *License Types*, on page 145](#) provides information about the specific access that each license provides. [Appendix C, *Licenses and User Roles*, on page 149](#) contains detailed information about product licenses.

- **Access Grants**

Access grants are linked to users through security groups. They determine the windows and functions in which users can view information or perform actions. Access grants also provide levels of control over specific entities and fields. [Chapter 2, *Users and Security Groups*, on page 17](#) contains information on how to create users and give them access to information and functionality in Mercury IT Governance Center. The tables in [Appendix A, *Access Grants*, on page 131](#) provide information about all of the access grants used to control user access to specific features and parts of the Mercury IT Governance Center user interface.

- **Entity-level restrictions**

Settings on the entity that specify who can create, edit, process, and delete Mercury IT Governance Center 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 set in the configuration entities (workflow, request type, object type, and so on).

- **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 also specify who can view or edit the field.

- **Configuration-level restrictions**

To specify who can modify configuration entities in the system, you can use ownership group settings. For example, you can control who can edit existing workflows. This ensures that only qualified users can modify your Mercury IT Governance Center–controlled processes. For information about the security settings and permissions required to configure Mercury IT Governance Center, see [Chapter 10, Configuration Security](#), on page 117.

Mercury recommends that you maintain two levels of system administrators for your organization. [Chapter 11, Service Provider Functionality](#), on page 125 contains information about how to create administrator-level users whose records cannot be modified by other users.

Providing Access to the Mercury IT Governance Applications

The process for configuring security for individual Mercury IT Governance Center applications can vary:

- For information about the security settings required to create, process, and manage requests in Mercury Demand Management™, see [Chapter 4, Request Security](#), on page 45.
- For information about the security settings required to create, process, and manage packages in Mercury Deployment Management™, see [Chapter 6, Package Security](#), on page 81.
- For information about the security settings required to create, process, and manage projects in Mercury Project Management™, see [Chapter 5, Project and Task Security](#), on page 73.
- For details on the security settings related to Mercury Resource Management™, see [Chapter 7, Resource Management Security](#), on page 89.
- For details on the security settings related to Mercury Financial Management™, see [Chapter 8, Cost and Budget Data Security](#), on page 103.
- All Mercury IT Governance Center user and configuration guides contain some level of security-related information related to the product that the document describes.

- For information about the security settings that users require to access and use the Mercury IT Governance Dashboard™, see [Chapter 9, *Dashboard Security*](#), on page 113.

Related Documents

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

- *Mercury Demand Management User's Guide*
- *Mercury Demand Management Configuration Guide*
- *Mercury Deployment Management User's Guide*
- *Mercury Deployment Management Configuration Guide*
- *Mercury Project Management User's Guide*
- *Mercury Project Management Configuration Guide*
- *Mercury Program Management User's Guide*
- *Mercury Program Management Configuration Guide*
- *Mercury Portfolio Management User's Guide*
- *Mercury Portfolio Management Configuration Guide*
- *Mercury Resource Management User's Guide*
- *Configuring the Standard Interface*
- *Commands, Tokens, and Validations Guide and Reference*
- *Mercury-Supplied Entities Guide* (includes descriptions of all Mercury IT Governance Center portlets, request types, and workflows)



Chapter
2

Users and Security Groups

In This Chapter:

- *Creating Users*
 - *Creating a User*
 - *Linking Users to Security Groups*
 - *Configuring Resource Information*
 - *Importing Users from a Database or LDAP Server*
 - *Creating Security Groups*
 - *Creating a Security Group by Specifying a List of Users*
 - *Using Resource Management to Control User Security*
 - *Using the Deployment Management App Codes Tab*
 - *Using the Charge Code Rules Tab*
-

Creating Users

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

Creating a User

To create a user:

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

The Mercury IT Governance Workbench opens.

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

The User Workbench window opens.

4. Click **New User**.

The User window opens.

The screenshot shows the 'User' window in the Mercury IT Governance Workbench. The window is titled 'User : Untitled2' and has a blue title bar. The main area is divided into several sections: 'User Information' (with fields for Username, First Name, Last Name, Company, Email Address, and Phone Number), 'Authentication' (with fields for Authentication Mode, Password, Start Date, End Date, Last Login, Password Exp. Days, and Password Exp. Date), 'System Level Licenses' (with checkboxes for Configuration and User Administration), and 'Application Licenses' (with checkboxes for Demand Management, Deployment Management, Portfolio Management, Program Management, Project Management, and Time Management). At the bottom of the window, there are buttons for 'Edit Resource', 'OK', 'Save', and 'Cancel'. The status bar at the very bottom shows 'Ready'.

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



Note

You must specify a username that is unique in Mercury IT Governance Center.

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

For a description of a control on the **User Information** tab, see [Table 2-1 on page 21](#).

7. In the **Authentication** section, do the following:
 - a. In the **Authentication Mode** list, select a user authentication method for the new user.

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



Note

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

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

This password is encrypted in the user interface and in the database.
- c. If you want the user to create a password the first time he or she logs on to Mercury IT Governance Center, next to **New password on login**, leave **Yes** selected. Otherwise, select **No**.
- d. To specify the number of days the password is to remain valid, in the **Password Exp. Days** field, type the number of days that the user has to change the password.

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

8. To assign the user a system-level license, under **System Level Licenses**, do one or both of the following:
 - To give the user access to all product functionality available through the Mercury IT Governance Workbench and standard interfaces in Mercury IT Governance Center (except for user and security group administration), select the **Configuration - Access to all Applications and their configuration, except User Administration** option.
 - To give the user permission to administer the users and security groups for all Mercury products licensed at your site, select the **User Administration - Create Users, Security Groups, and assign Licenses** option.



Note

To assign licenses to multiple users at one time, use the License Workbench. For details on how to do this, see [Assigning Licenses to Multiple Users in the License Workbench on page 40](#).

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



Note

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

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

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

For information about how to link the user to security groups, see [Linking Users to Security Groups on page 23](#).

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

For information about how to select the users or security groups that can configure a user, see [Setting Ownership for Configuration Entities on page 118](#).

12. Click **OK**.

The new user can now log on to Mercury IT Governance Center.

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

Field Name	Description
Username	Unique user account name to be used to log on to Mercury IT Governance Center.
Company	The company for which the user works. The values in this list are set by the following validation: CRT - Company.
First Name	The user's first name.
Last Name	The user's last name.
Email Address	The user's email address in the format <code>name@domain.com</code> . This address is referenced elsewhere in the application.
Phone Number	The user's phone number.
Authentication Mode	A list of the available authentication methods. Possible values are ITG , LDAP , NTLM , and SITEMINDER . If you select ITG , then authentication is performed using the internal user database of Mercury IT Governance Center. If you select another authentication mode, authentication is performed using the enterprise directory database server. For details, see the <i>Open Interface Guide and Reference</i> .
Start Date	The date on which a user account is to be activated.
End Date	The date on which a user account expires. You can leave this field empty.
Last Login	The date of a user's last system logon. This date is deleted based on the <code>DAYS_TO_KEEP_LOGON_ATTEMPT_ROWS</code> parameter in the <code>server.conf</code> file. The default value for this parameter is 14 days. If there is no value in the Last Login field, the user has not logged in for at least 14 days (assuming the parameter default value has not changed). For detailed information about server configuration parameters, see the <i>System Administration Guide and Reference</i> .
Domain	Used only if you use NTLM authentication. Set the value for this in the <code><ITG_HOME>/integration/ntlm/ntlm.conf</code> file.
Password	The user password. Administrators can set restrictions on the password format: minimum length, required special characters, and so on. These restrictions are specified in the <code>server.conf</code> file on the Mercury IT Governance Server. For detailed information about server configuration parameters, see the <i>System Administration Guide and Reference</i> .
New password on login	Setting to determine whether to ask a user to enter a new password the next time they log on.

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

Field Name	Description
Password Exp. Days	The number of days before a user password expires. The first time a user logs on after the password expiration date, he is prompted to create a new password.
Password Exp. Date	The date on which a password expires. The value in this field is calculated based on the Password Expiration Days value or the Ask New Password On Logon attribute.
Configuration	Select this option to give the user access to all functionality for the products licensed at the site, including configuration interfaces for all Mercury IT Governance Center entities (such as object types and request types) except users and security groups.
User Administration	The User Administration license is required to configure user accounts and security groups.
Deployment Management	The Deployment Management license provides access to all product functionality available through the Mercury IT Governance Workbench interface and additional access to advanced standard interface functions. If this checkbox is not selected, the user cannot see the Deployment Management screen group or menus.
Demand Management	The Demand Management license provides access to all product functionality. If this checkbox is not selected, the user cannot see the Demand Management screen group or menus.
Portfolio Management	The Portfolio Management license provides access to Portfolio Management functionality, and must be used in conjunction with a Demand Management license. Users who do not have this selected cannot see the related menus and can not access the functionality.
Program Management	The Program Management license gives a user access to Program Management functions. This license must be used in conjunction with Demand Management and Project Management licenses. Users who do not have this license cannot see the related menus or access the functionality.

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

Field Name	Description
Project Management	The Project Management license provides access to all Project Management, Resource Management, and Financial Management functionality. Users who do not have this license cannot create or view projects or resources.
Time Management	The Time Management license gives users access to Time Management functions in Mercury IT Governance Center. If this is not selected, the user cannot see the Time Management menus or access the functionality. Users for whom timesheets are to be submitted must also have this license.
Edit Resource	Each user has associated resource settings such as Title, Direct Manager, and Capacity. Click this button to view or edit these resource settings.



Note

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

Linking Users to Security Groups

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

To link a user to a security group:

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

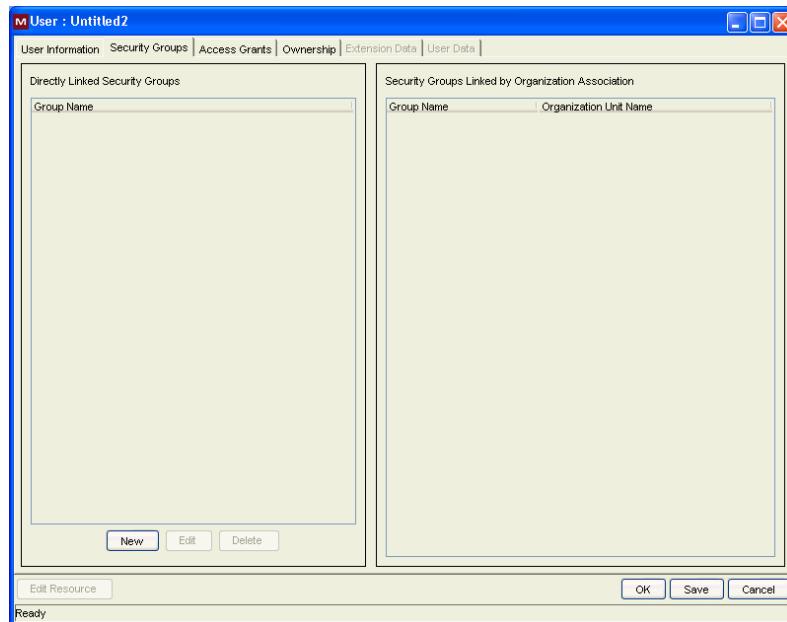
The Mercury IT Governance Workbench opens.

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

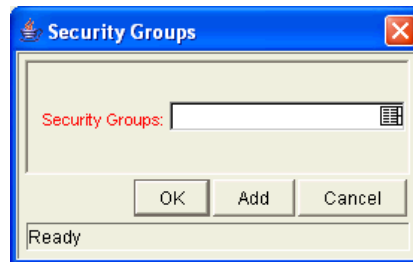
The User Workbench opens.

4. Use the **Query** tab to locate the user who you want to add to security groups.

5. On the **Results** tab, double-click the row that displays the user name.
The User window opens to the record for the user you selected.
6. Click the **Security Groups** tab.



7. Click **New**.
The Security Groups window opens.



8. In the **Security Groups** field, click the auto-complete button.
The Validate dialog box opens.
9. Under **Available**, in the **Security Group** column, select one or more security groups to link to the user.



Note

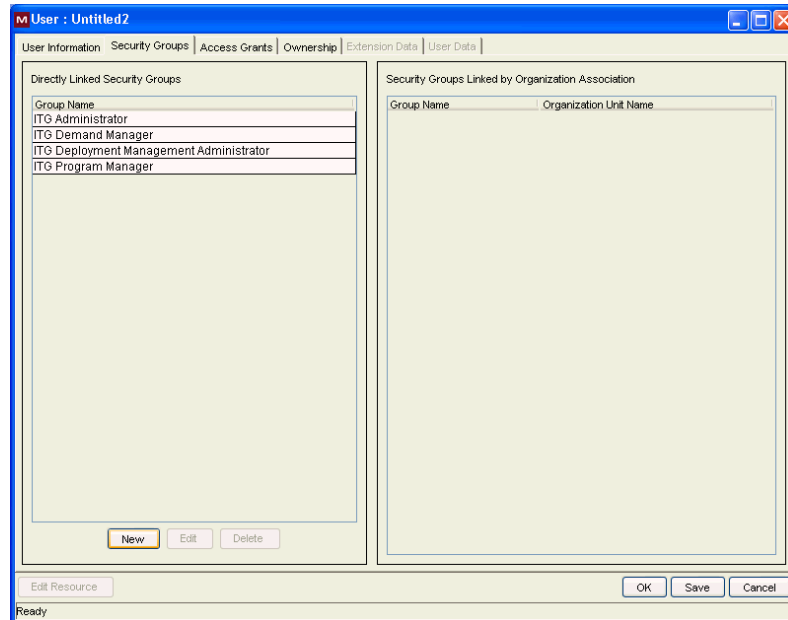
You can use the **Ctrl** or **Shift** key to select multiple groups.

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

11. Click **OK**.

The Security Groups dialog box lists your selection(s).

12. Click **OK**.



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



Note

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

13. Click **OK**.

Configuring Resource Information

A resource is something or someone assigned to work. Resources can include employees, contractors, managers, consulting groups, supplies, or any other category your organization requires. A user is considered a resource in Mercury IT Governance Center. You can capture user information specific to the user's role as a resource, including:

- User skills or roles such as database administrator or programmer
- The hourly rate associated with the resource or skill, which represents the charge-back or billed labor cost
- Workload capacity, represented as the percentage of the working day that the resource is available for planned work items

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

Importing Users from a Database or LDAP Server

If your organization has many users, you can use the Mercury IT Governance Center open interface to create user accounts. 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 to generate users who you can then process normally within Mercury IT Governance Center. You can also import user information from LDAP servers.

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

Creating Security Groups

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

To create a security group:

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

The Mercury IT Governance Workbench opens.

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

The Security Group Workbench window opens.

4. Click **New Security Group**.

The Security Group window opens.

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

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

8. To make this group selectable, do one of the following:

To select group members directly:

- a. On the **Users** tab, click **Add New User to this Group**.

The Users dialog box opens.

- b. In the **Users** field, click the selector button.

The Validate window opens.

- c. In the **Available** section, select the users to add to the security group.

- d. Click **OK**.

- e. In the Users dialog box, click **OK**.

Alternatively, to add users based on their organization unit associations:

- a. In the **Membership** section of the **Users** tab, under **Members are**, select **Determined by Organization Unit**.

- b. In the **Organization Unit** field, enter the name of an organizational unit.

- c. If you want to associate just the members of this organization unit with the new security group, leave **Direct Members Only** selected. If you also want to include members of the child organization units of the selected unit, click **All Members (Cascading)**.

9. To specify user interface and feature access, click the **Access Grants** tab, and then select the access grants to assign to the security group.



Note

For a complete list of access grants, see [Appendix A, Access Grants](#), on page 131.

10. If the security group is to be used in deployment, do the following:
 - a. Click the **Deployment Management Workflows** tab, and then specify the workflows that members of this security group can use to deploy changes.
 - b. On the **Deployment Management App Codes** tab, restrict the security group from using specific application codes in creating package lines.

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

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

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

Creating a Security Group by Specifying a List of Users

To create a security group:

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

The Mercury IT Governance Workbench opens.

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

The Security Group Workbench opens.

4. Click **New Security Group**.

The Security Group window opens.

5. In the **Name** field, type a name for the group.

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

Only the names of enabled security groups are available when generating or updating users or workflows.

8. To the right of **This Security Group will be used by**, select the checkboxes for the Mercury IT Governance Center entities that you want to use the security group.

Table 2-2 lists the available checkboxes.

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

Field Name	Description
Requests	<p>Determines whether this security group can be used in request processing. If this checkbox is not selected, the security group is not displayed in:</p> <ul style="list-style-type: none"> ■ Assigned Group field on the request ■ User Access tab in the Request Type window—this restricts users in the security group from selecting a request type when creating a request. <p>Note: If a user has the System: Override Key Fields Segmentation access grant, then the security group is displayed in the Assigned Group field.</p>
Projects	<p>Determines whether members of this security group can serve as project resources. This checkbox affects the following controls:</p> <ul style="list-style-type: none"> ■ Project Team tab in the Project Settings window. If the checkbox is cleared, users in the security group cannot serve as resources unless they belong to another security group that grants them access. ■ Project plan panel. If the checkbox is cleared, you cannot add members of this security group to the project team unless they belong to another security group that grants them access. ■ Resource Group field on the Project plan panel: If the checkbox is cleared, the security group is not included in the list of resource groups. <p>Note: If a user has the System: Override Key Fields Segmentation access grant, then these security group restrictions do not apply.</p>

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

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

9. To link selected users to the security group:

a. On the **Users** tab, click **New**.

The Users window opens.

b. In the **Users** field, select one or more users.

c. Click **OK**.

10. Link the access grants, as follows:



Note

Each access grant enables certain functions performed on a screen. For a description of each access grant, see [Appendix A, Access Grants, on page 131](#).

a. In the **Available Access Grants** list, select one or more access grants.

b. Click the right-pointing arrow.

c. Click **OK**.

11. Restrict the security group from using certain workflows when processing packages, as follows:

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

b. Select the workflows in the **Allowed Deployment Management Workflows** list.

- c. Click the left-pointing arrow.

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

- d. To exclude all future workflows, select the **Always restrict new Workflows** checkbox.
12. Restrict the security group from using certain application codes when creating a package line.

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

- a. Click the **Deployment Management App Codes** tab.
- b. Select the app codes in the **Allowed Deployment Management App Codes** list.
- c. Click the left-pointing arrow.

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

- d. To exclude all future app codes, select the **Always restrict new App Codes** checkbox.
13. Click the **Ownership** tab, and then select the ownership groups that you want to be able to edit, copy, or delete the current security group.

For more information about how to set ownership for a security group, see [Chapter 10, Configuration Security](#), on page 117.

14. On the **User Data** tab, enter any necessary information.
15. To save your changes, do one of the following:
 - To register the current security group and close the Security Group window, click **OK**.
 - To save the information and leave the Security Group window open, click **Save**.

Using Resource Management to Control User Security

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

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

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

The Mercury IT Governance Workbench opens.

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

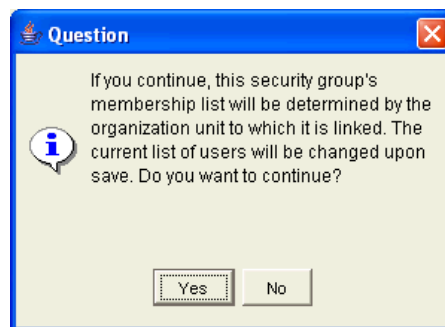
The Security Group Workbench opens.

4. Click **New Security Group**.

The Security Group window opens.

5. On the **Users** tab, in the **Membership** section, select **Determined by Organization Unit**.

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



6. Click **Yes**.



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

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

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

9. Click **OK**.

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

Using the Deployment Management App Codes Tab

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

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

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

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

Using the Charge Code Rules Tab

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

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



Note

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

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

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

Chapter

3

Managing Mercury IT Governance Licenses

In This Chapter:

- *Overview of License Management*
 - *Assigning Licenses from the User Workbench*
 - *Assigning Licenses to Multiple Users in the License Workbench*
 - *Removing Licenses Using the Assign Licenses Wizard*
 - *Assigning Licenses Using the Open Interface*
-

Overview of License Management

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

The following sections contain the procedures you use to assign Mercury IT Governance Center product licenses from the User Workbench and using the Assign Licenses wizard. For a detailed description of each license, see [Appendix B, *License Types*, on page 145](#).

Assigning Licenses from the User Workbench

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

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

The Workbench opens.

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

The User Workbench opens.

4. Click **List**.

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

5. Double-click the record for the user to whom you want to assign a license. The User window opens and displays the record for the user you selected.

The screenshot shows the 'User : csayer' window with the following details:

- User Information:** Username: csayer, First Name: Carolyn, Last Name: Sayer, Email Address: csayer@acme.com.
- Authentication:** Authentication Mode: ITG, Password: *****.
- System Level Licenses:**
 - Configuration - Access to all Applications and their configuration, except User Administration
 - User Administration - Create Users, Security Groups, and assign Licenses
- Application Licenses:**
 - Demand Management
 - Deployment Management
 - Portfolio Management - Requires Demand Management
 - Program Management - Requires Demand Management and Project Management
 - Project Management
 - Time Management

6. To assign the user a system-level license, under **System Level Licenses**, do one or both of the following:
 - To give the user access to all product functionality available through the Workbench and standard interfaces in Mercury IT Governance Center (except for user and security group administration), select the **Configuration - Access to all Applications and their configuration, except User Administration** checkbox.
 - To give the user permission to administer the users and security groups for all Mercury products licensed at your site, select the **User Administration - Create Users, Security Groups, and assign Licenses** checkbox.
7. Under **Application Licenses**, select all of the checkboxes that correspond to the application licenses you want to assign to the user.



Note

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

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

8. Click **Save**.

Note

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

Assigning Licenses to Multiple Users in the License Workbench

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

To assign licenses using the Assign Licenses wizard:

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

The Workbench opens.

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

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

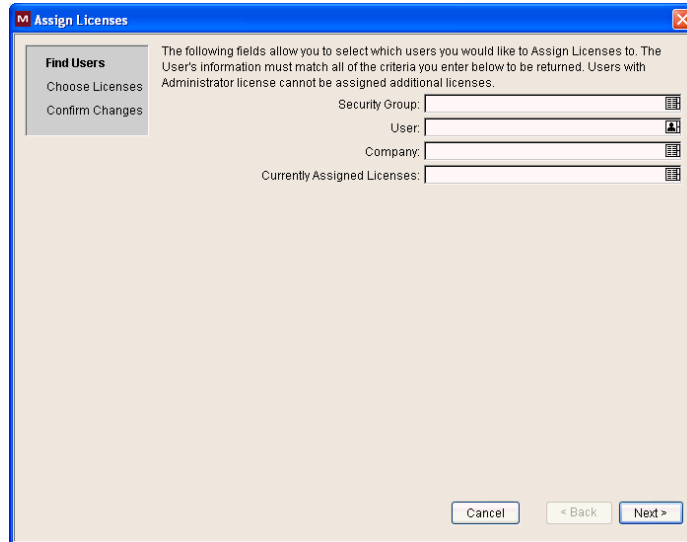
License	Expiration Date	Number Used	Number Available	Total Charge
Configuration	Jan 1, 3000	13	49967	50000
Demand Management	Jan 1, 3000	30	49970	50000
Deployment Management	Jan 1, 3000	17	49963	50000
Portfolio Management	Jan 1, 3000	6	49994	50000
Portfolio Optimization	Jan 1, 3000	n/a	n/a	n/a
Program Management	Jan 1, 3000	5	49995	50000
Project Management	Jan 1, 3000	13	49967	50000
Time Management	Jan 1, 3000	27	49973	50000
User Administration	Jan 1, 3000	5	49995	50000

Installed Extensions
No Extensions installed

Buttons: Assign Licenses, Refresh

4. Click **Assign Licenses**.

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



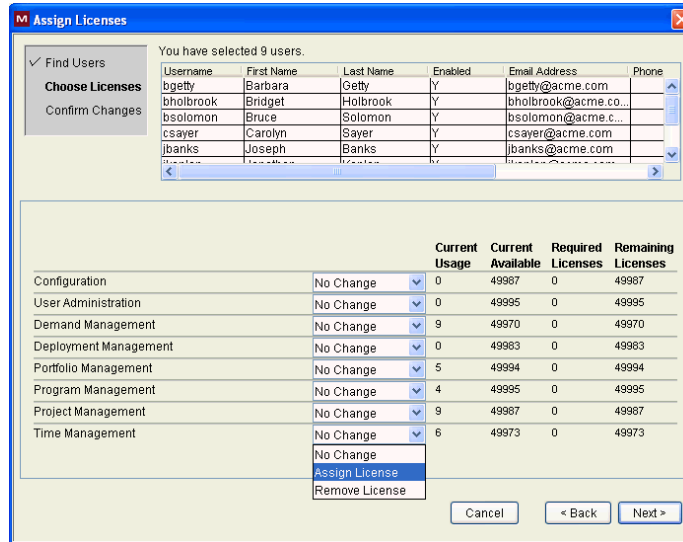
5. In one or more of the fields listed in *Table 3-1*, enter search criteria to locate the users to whom you want to assign licenses:

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

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

6. Click **Next**.

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

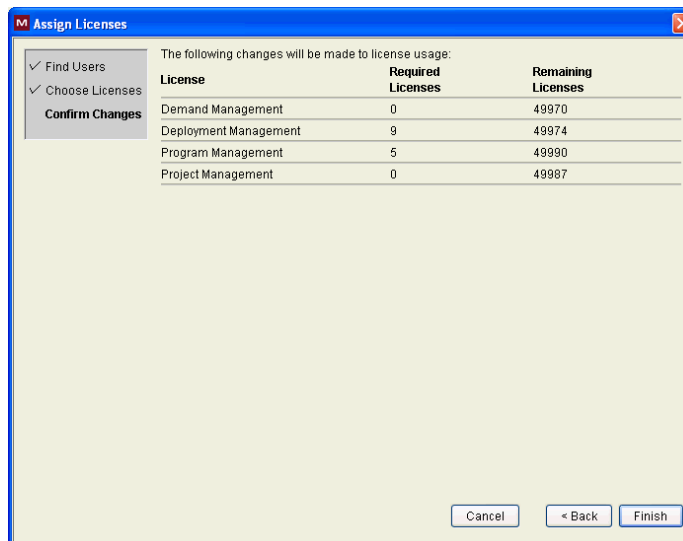


7. On the **Choose Licenses** step, review the listed users, and then select the licenses that you want to assign to them from the license fields.

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

8. Click **Next**.

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



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

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

10. Click **Finish**.



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

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

Removing Licenses Using the Assign Licenses Wizard

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

To remove licenses:

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

The Workbench opens.

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

The License Administration window opens.

4. Click **Assign Licenses**.

The Assign Licenses wizard opens.

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

Assigning Licenses Using the Open Interface

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.

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

A decorative graphic consisting of four colored squares (orange, blue, red, and a larger red square) and a large white number '4' on a red background. The word 'Chapter' is written in red above the number, and 'Request Security' is written in red below the number.

Chapter 4 Request Security

In This Chapter:

- *Overview of Request Security*
 - *Prerequisite Settings for Users and Security Groups*
 - *Licenses*
 - *Access Grants*
 - *Viewing a Request*
 - *Creating a Request*
 - *Enabling Users to Create Requests*
 - *Restricting Users from Selecting a Specific Workflow*
 - *Processing a Request*
 - *Enabling Users to Edit Fields on a Request*
 - *Enabling Users to Cancel or Delete a Request*
 - *Enabling Users to Act on a Specific Workflow Step*
 - *Viewing and Editing Fields on a Request*
 - *Field-Level Data Security Overview*
 - *Field Window: Attributes Tab*
 - *Field Window: Security Tab*
 - *Request Type Window: Status Dependencies Tab*
 - *Overriding Request Security*
-

Overview of Request Security

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

- **Request creation**

- Who can create requests
- Who can use a specific workflow
- Who can use specific request types

- **Request processing**

- Who can act on each step in the workflow

For this restriction, enable access by specifying users or security groups. Access can also be provided dynamically by having a token resolve to provide access.

- Who can view or edit certain fields in a request

For this restriction, enable view or edit access to request fields by specifying users or security groups. You can also have a token resolve to provide access dynamically.

- **Managing request resolution**

- Who can change the workflow
- Who can change each request type

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

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

Prerequisite Settings for Users and Security Groups

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

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



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

Licenses

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

For details on the functionality associated with each license, see [Licenses and User Roles on page 149](#). The following sections address how the functionality provided with each access grant depends on the license type the user has.

Access Grants

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

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

Access Grant	Description
Demand Mgmt: Edit Requests	<p>Perform basic request processing actions: create requests, edit certain requests, and delete requests that you have not submitted.</p> <ul style="list-style-type: none"> ■ Lets the user generate requests. ■ Prevents the user from changing the workflow when creating or editing a request. ■ Lets the user edit the request as specified on the User Access tab in the Request Type window. ■ Lets the user delete the request as specified on the User Access tab in the Request Type window. ■ Lets the user cancel the request as specified on the User Access tab in the Request Type window.
Demand Mgmt: Edit All Requests	<p>Perform advanced request processing actions: creating, editing, deleting, changing the request's workflow, and overriding references.</p> <ul style="list-style-type: none"> ■ User can always edit the request. ■ Override and/or remove any references on any request. ■ User can always delete or cancel a request. ■ User can change the workflow when creating and editing a request.
Demand Mgmt: Override Demand Mgmt Participant Restriction	<p>This access grant lets the user review a request, regardless of whether that user can view, as defined on the User Access tab for the request type.</p>

Screen and function access provided through access grants is cumulative. A user who belongs to three different security groups has the access to all of the user interface and functionality granted to all of the groups combined. To restrict certain screen and feature access, remove the user from any security group that has access to those areas.

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

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



Note

The Mercury IT Governance Center includes additional access grants that you can use to control access to other functions in Demand Management. For more information, see [Appendix A, Access Grants, on page 131](#).

Viewing a Request

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

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

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

The Workbench opens.

3. From the shortcut bar, select **Demand Mgmt > Request Types**.

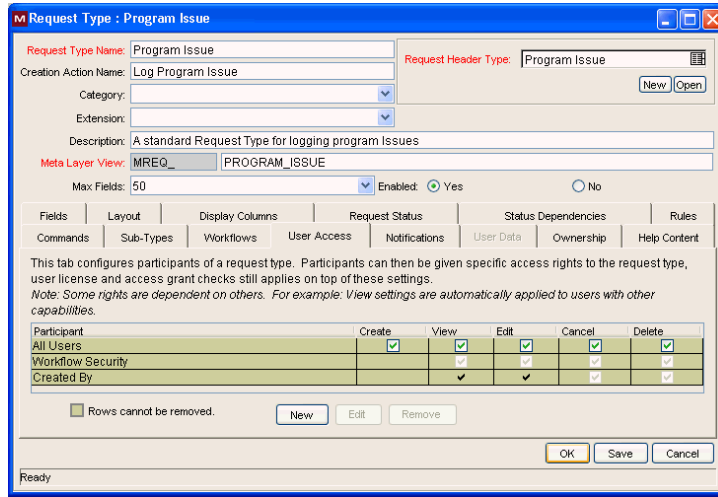
The Request Type Workbench opens.

4. Click **List**.

5. On the **Results** tab, locate, and then double-click the row that displays the request type that you want all users to be able to view.

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

- Click the **User Access** tab.



- In the **All Users** row, if the **View** checkbox is cleared, select it.
- Click **Save**.

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

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



Note

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

- Click **New**.

The Participant Security window opens.



- In the list at the top of the window, leave **Enter a Security Group Name** selected.
- In the **Security Group** field, enter the name(s) of the security group(s) that can view requests of this type.

5. Click **OK**.

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

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

To enable specific users to view a request:

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

2. Click **New**.

The Participant Security dialog box opens.



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

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

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

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

5. Click **OK**.

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

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

Creating a Request

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



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

Enabling Users to Create Requests

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

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

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

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

The Workbench opens.

3. From the shortcut bar, select **Demand Mgmt > Request Types**.

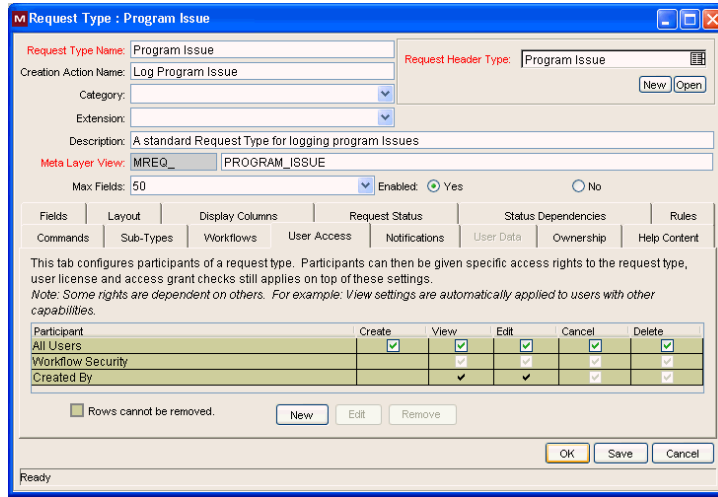
The Request Type Workbench opens.

4. Click **List**.

The **Results** tab lists all existing request types.

5. Double-click the row that displays the request type that you want all users to be able to create.

- Click the **User Access** tab.



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

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

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

The Participant Security window opens.



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

5. Click **OK**.

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

6. Click **Save**.

To enable specific users to create a request:

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

The Participant Security window opens.



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

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

6. Click **Save**.

Restricting Users from Selecting a Specific Workflow

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

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

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

The Workbench opens.

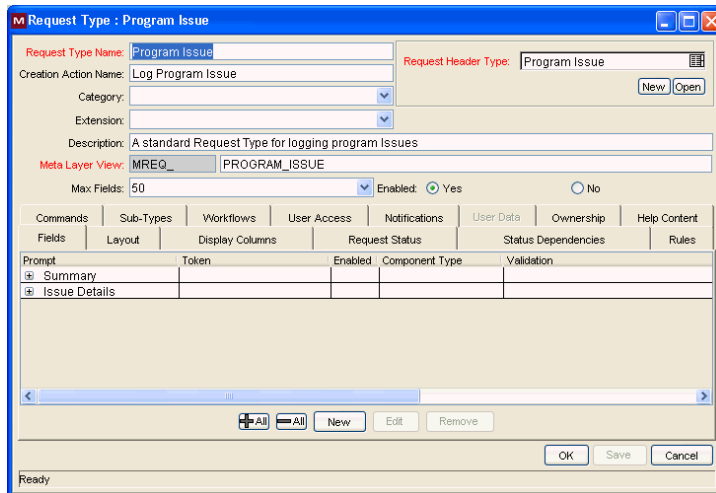
3. From the shortcut bar, select **Demand Mgmt > Request Types**.

The Request Type Workbench opens.

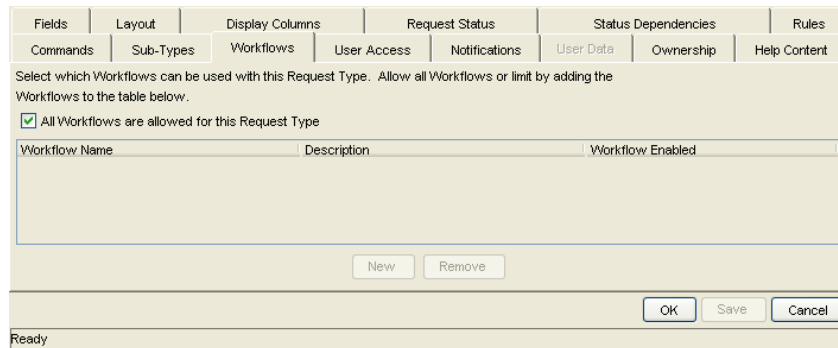
4. Click **List**.

The **Results** tab lists all existing request types.

5. Double-click the row that displays the request type for which you want to restrict applied workflows.



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



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

8. Click **New**.

The Workflow: New window opens.



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

10. Click **OK**.

The **Workflow** tab lists the selected workflows.

11. Click **Save**.

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



Note

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.

You can also specify the default request type to be used with this workflow.

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

Processing a Request

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



Note

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

Enabling Users to Edit Fields on a Request

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

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

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

The Workbench opens.

3. From the shortcut bar, select **Demand Mgmt > Request Types**.

The Request Type Workbench opens.

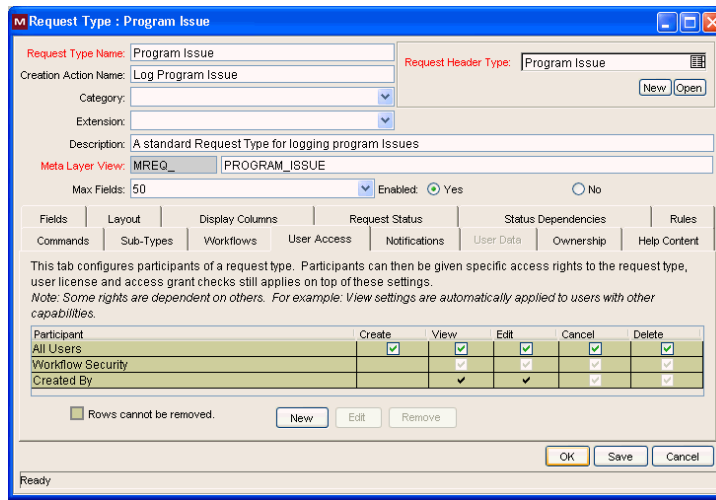
4. Click **List**.

The **Results** tab lists all existing request types.

5. Double-click the row that displays the request type for which you want to configure field editability.

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

- Click the **User Access** tab.



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

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

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



Note

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

- Click **New**.

The Participant Security dialog box opens.

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

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

- Click **Save**.

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

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

8. Click **New**.

The Participant Security dialog box opens.



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

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

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

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

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

Enabling Users to Cancel or Delete a Request

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

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

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

The Workbench opens.

3. From the shortcut bar, select **Demand Mgmt > Request Types**.

The Request Type Workbench opens.

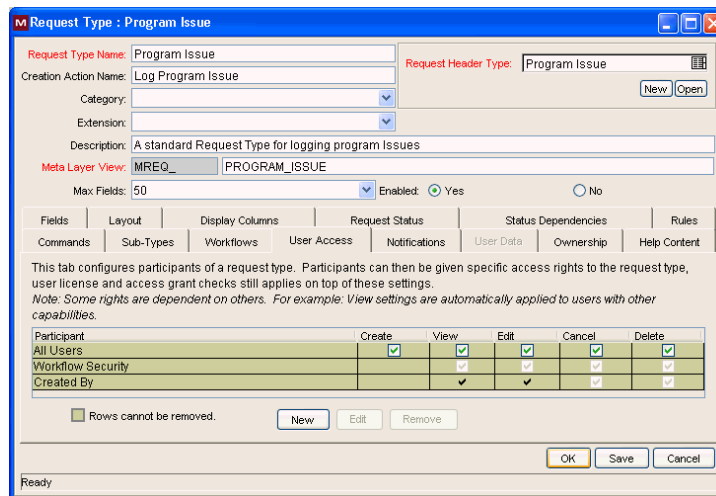
4. Click **List**.

The **Results** tab lists all existing request types.

5. Double-click the row that displays the request type you want to configure.

The Request Type window opens.

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



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

8. Click **Save**.

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

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

The Participant Security dialog box opens.



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

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

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

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

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

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

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

3. In the **Created By** row, select the **Cancel** and **Delete** checkboxes.
4. Click **Save**.

Enabling Users to Act on a Specific Workflow Step

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

To specify who can act on a specific workflow step:

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

The Workbench opens.

3. From the shortcut bar, select **Configuration > Workflows**.

The Workflow Workbench opens.

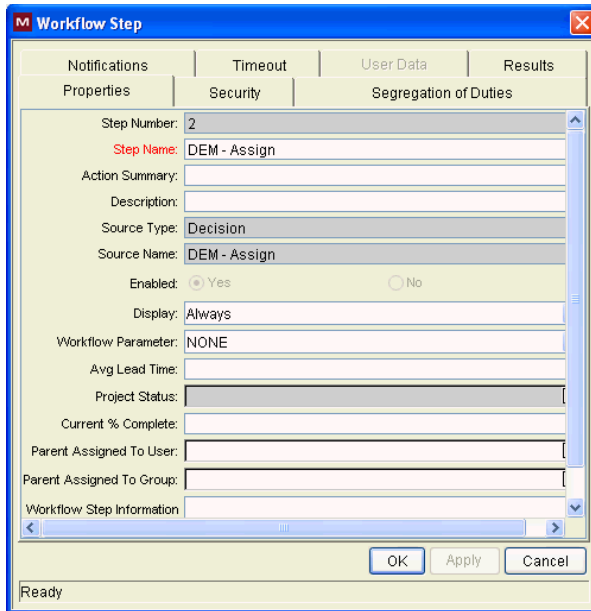
4. Click **List**.
5. On the **Results** tab, locate and open the workflow.

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

The screenshot shows the 'Workflow Step' configuration window. The 'Security' tab is active, displaying various configuration fields. The 'Step Name' is 'DEM - Assign' and the 'Source Name' is also 'DEM - Assign'. The 'Enabled' option is set to 'Yes'. The 'Display' is set to 'Always' and the 'Workflow Parameter' is 'NONE'. At the bottom, there are 'OK', 'Apply', and 'Cancel' buttons.

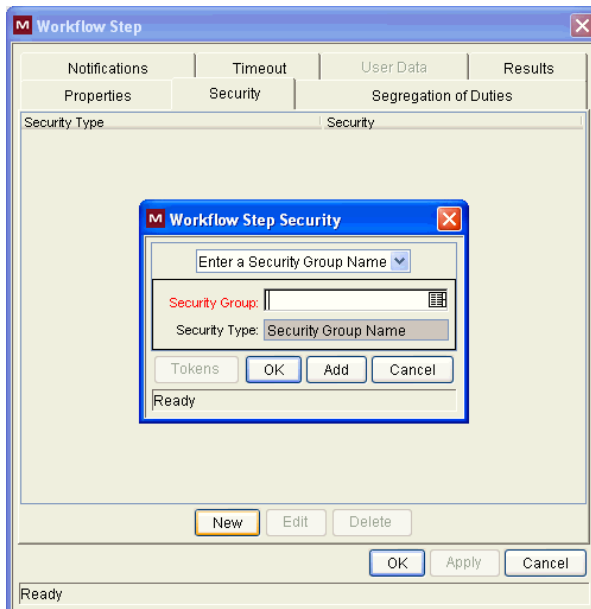
6. Double-click the step you want to configure.

The Workflow Step window opens.



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

The Workflow Step Security dialog box opens.



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

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

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

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

10. Click **OK**.

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

11. Click **OK**.



Tip

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

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

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

Viewing and Editing Fields on a Request

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



Note

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

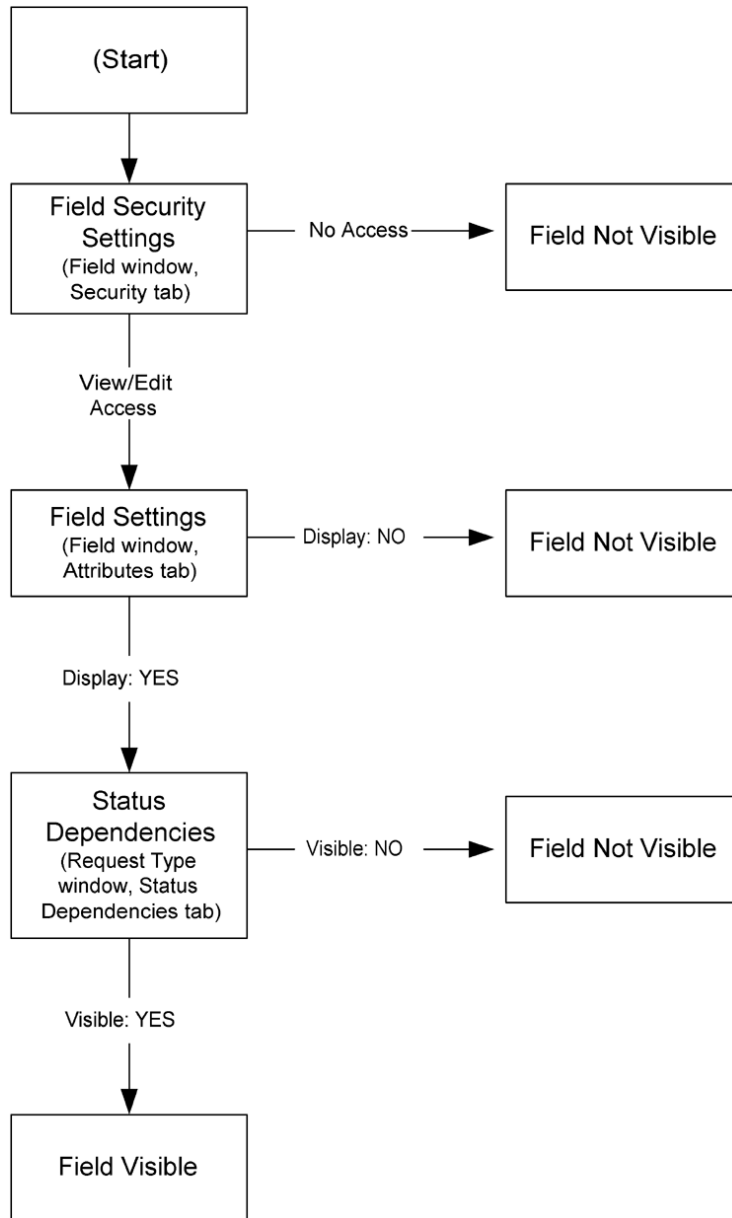
Field-Level Data Security Overview

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

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

Figure 4-1 on page 66 illustrates the settings that determine whether a field is visible to a given user.

Figure 4-1. Field visibility interactions



Field Window: Attributes Tab

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

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

1. Log on to Mercury IT Governance Center.
2. From the menu bar, select **Administration > Open Workbench**.
The Workbench opens.
3. From the shortcut bar, select **Demand Mgmt > Request Types**.
The Request Type Workbench opens.
4. Click **List**.
5. Open the request type with fields that you want to configure.
The Request Type window opens.
6. Click the **Fields** tab.
7. To view the fields associated with the request type, in the **Prompt** column, expand the listed nodes.
8. Double-click the row that displays information about the field you want to configure.

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

The screenshot shows the 'Field: Due Date' configuration window with the 'Attributes' tab selected. The window contains the following fields and controls:

- Field Prompt:** Due Date
- Token:** P_DUE_DATE
- Description:** The date the issue is expected to close
- Enabled:** Yes No
- Validation:** Date (with a list icon and 'New'/'Open' buttons)
- Component Type:** Date Field (dropdown menu)
- Multi-Select Enabled:** Yes No
- Attributes:** Default | Storage | Security (selected)
- Section Name:** Issue Details (dropdown menu)
- Display Only:** Yes No
- Transaction History:** Yes No
- Notes History:** Yes No
- Display on Search and Filter:** Yes No
- Display:** Yes No
- Search Validation:** (with a list icon and 'Open' button)
- Buttons:** OK, Apply, Cancel
- Status:** Ready

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

Field Window: Security Tab

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

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

1. Log on to Mercury IT Governance Center.
2. From the menu bar, select **Administration > Open Workbench**.
The Workbench opens.
3. From the shortcut bar, select **Demand Mgmt > Request Types**.
The Request Type Workbench opens.
4. Click **List**.
5. Open the request type with fields that you want to configure.
The Request Type window opens.
6. Click the **Fields** tab.
7. To view the fields associated with the request type, in the **Prompt** column, expand the listed nodes.

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

The Field window opens.

9. Click the **Security** tab.

10. Click **Edit**.

The Edit Field Security window opens.

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



Note

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

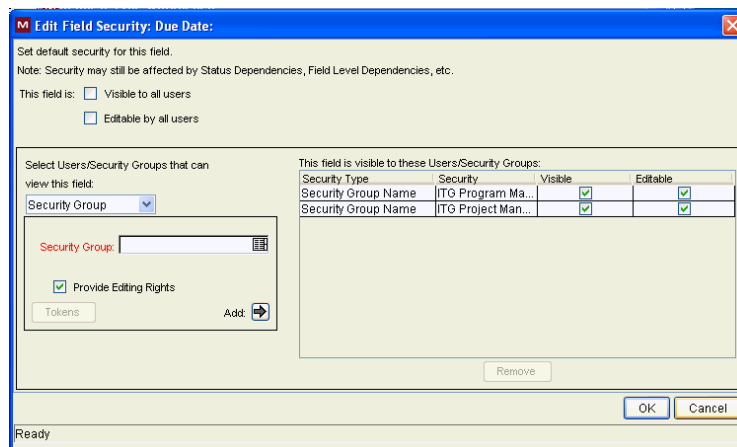
12. In the list under **Select Users/Security Groups that can view this field**, select one of the following:

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

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

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

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



15. Click **OK**.

Request Type Window: Status Dependencies Tab

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

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

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

The screenshot shows the 'Request Type: Program Issue' window with the 'Status Dependencies' tab selected. The window contains the following information:

- Request Type Name:** Program Issue
- Creation Action Name:** Log Program Issue
- Request Header Type:** Program Issue
- Category:** (dropdown menu)
- Extension:** (dropdown menu)
- Description:** A standard Request Type for logging program Issues
- Meta Layer View:** MREQ_ PROGRAM_ISSUE
- Max Fields:** 50
- Enabled:** Yes (selected)

The 'Status Dependencies' tab displays a table with the following data:

Field	Visible	Editable	Required	Reconfirm
Summary	Y	Y	[...]	
Issue Details	Y	Y		

Below the table, there are radio button controls for each status:

- Visible:** Yes (selected), No
- Editable:** Yes, No (selected)
- Required:** Yes, No (selected)
- Reconfirm:** Yes, No (selected)
- Clear:** Yes, No (selected)


Overriding Request Security

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

Table 4-2. Settings required to override request security

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

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



Chapter
5

Project and Task Security

In This Chapter:

- *Overview of Project and Task Security*
 - *Viewing Projects and Tasks*
 - *Controlling Resources on the Project*
 - *Creating Projects*
 - *Editing Project and Task Information*
 - *Updating Tasks*
 - *Overriding Project Security*
-

Overview of Project and Task Security

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



Note

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

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

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

Viewing Projects and Tasks

To allow users to view projects and tasks, assign one of the licenses and the access grant listed in [Table 5-1](#).

Table 5-1. Settings required to view projects and tasks

Setting	Value	Description
License	<ul style="list-style-type: none"> ■ Project Management ■ Portfolio Management ■ Configuration ■ Demand Management ■ Time Management 	<p>The Project Management, Portfolio Management, Configuration, and Demand Management licenses let users view project and task information in the standard interface.</p> <p>The Time Management license lets users view task status information (such as % complete) in the standard interface.</p>
Access Grants linked to the Security Group	Project Mgmt: View Projects	<p>The Project Mgmt: View Projects access grant lets users view project definitions in the standard interface.</p> <p>Note: The Project Mgmt: Edit Projects and Project Mgmt: Edit All Projects access grants also provide viewing privileges, but enable editing and processing functions.</p>

To restrict users from viewing projects and tasks, use the settings listed in *Table 5-2*.

Table 5-2. Settings to restrict a user from viewing projects and tasks

Setting	Value	Description
License	(REMOVE) Project Management	Removing the Project Management license from users prevents them from viewing any project- or task-related pages or windows in Project Management.
Access Grant	(REMOVE) Project Mgmt: View Projects; Edit Projects; Edit All Projects	Removing these access grants from users prevents them from viewing projects and tasks through Project Management.
Users who can view this project and its tasks	All Users Only participants (Project Managers, Summary Task Owners, Assigned Resources, Assigned Resource Groups, Stakeholders, and Process Participants)	Restrict who can view projects and tasks to “participants” (set in the Project Security section of the Project Settings page).
Budget, Benefit, and Cost information on the Project and Tasks can be viewed by	<ul style="list-style-type: none"> ■ All Users who can view the project and its tasks ■ Project Managers and Stakeholders ■ Project Managers, Stakeholders, Summary Task Owners and Process Participants 	

A participant can be:

- A project manager
- An assigned task resource or task owner
- A member of an assigned security group
- A program manager
- A stakeholder

Controlling Resources on the Project

Project managers can specify who can serve as a project resource. Resources can be users and groups of users.

Resources for a project come from the staffing profile attached to the project, or from the resource pools that the project manager manages. Resources who are not assigned through a staffing profile or a resource pool must be requested from other resource pools, using staffing profiles.



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

For more information on setting security for project resources and stakeholders, see the *Mercury Project Management User's Guide*.

Creating Projects

You can control which users can create projects and tasks. Any users with the licenses and access grants list in [Table 5-3](#) can create projects.

Table 5-3. Settings required to create a project (page 1 of 2)

Setting	Value	Description
License	<ul style="list-style-type: none"> ■ Project Management ■ Portfolio Management ■ Configuration ■ Demand Management 	<p>This license lets users create projects from Project Management in the standard interface.</p> <p>The Demand Management license lets a user create a project through a workflow.</p>

Table 5-3. Settings required to create a project (page 2 of 2)

Setting	Value	Description
Access Grants (only one is required)	Project Mgmt: Create Projects and Project Mgmt: Edit Projects	This access grant lets users create projects. If the user is specified as a manager on a project, this grant lets that user update the project and its subprojects.
	Project Mgmt: Create Projects and Project Mgmt: Edit All Projects	Create and edit 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. Users who have the licenses and access grants listed in [Table 5-4](#) can edit projects.

Table 5-4. Settings required to edit a project

Setting	Value	Description
License	Project Management or Configuration	Both the Project Management license and the Configuration license allow users to edit projects.
Access Grants (only one is required)	Project Mgmt: Edit Projects	Update projects and subprojects if specified as a project manager.
	Project Mgmt: Edit All Projects	Edit any project. Override (or remove) references on projects or tasks.

Updating Tasks

You can determine which users can update tasks on projects by using the licenses and access grants listed in [Table 5-5](#).

Table 5-5. Settings required to update tasks

Setting	Value	Description
License	Project Management or Configuration Time Management	Both the Project Management and Configuration licenses let users update task status information. The Time Management license lets a user update task status information on the My Tasks portlet, as well as the data on detail pages for tasks.
Access Grants	Project Mgmt: Update Tasks (Required)	If a user is specified as a resource on the project, he can update tasks.
	Project Mgmt: Edit All Projects	If a user is specified as a project participant, he can use the Update Tasks page to update multiple tasks.
	Project Mgmt: Edit Projects	If the user is specified as manager of a project or its parent, he can use the Update Tasks page to update multiple tasks.

To prevent users from updating tasks, set the following:

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

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

Overriding Project Security

Users who have the access grants listed in *Table 5-7* can view and edit any project.

Table 5-7. Settings to override request security

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

Users who have the System: Ownership Override access grant can edit Project Management configuration entities, regardless of ownership restrictions.

A decorative graphic consisting of four colored squares (orange, teal, dark red, and a larger dark red square) and a large white number '6' on a dark red background. The word 'Chapter' is written in dark red above the '6', and 'Package Security' is written in dark red below the '6'.

Chapter 6 Package Security

In This Chapter:

- *Overview of Package Security*
 - *Viewing a Package*
 - *Restricting Package Viewing to Participants*
 - *Creating a Package*
 - *Enabling Users to Create Packages*
 - *Preventing Users from Selecting a Specific Workflow*
 - *Preventing Users from Selecting a Specific Object Type*
 - *Approving Package Lines*
 - *Enabling Users to Act on a Specific Workflow Step*
 - *Deleting a Package*
 - *Overriding Package Security*
-

Overview of Package Security

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

- **Package creation**

- Who can create packages
- Who can use a specific workflow
- Who can use specific object types

- **Package processing**

- Who can approve or process each step in the workflow
- Whether you only want participants to process the packages. Participants are defined as the assigned user, the creator of the package, members of the assigned group, or any users who have access to the workflow step(s).

- **Managing deployment**

- Who can change the workflow
- Who can change each object type
- Who can change the environment and environment group definitions
- Who can change the security group definitions

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

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

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



Note

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

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

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

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

Viewing a Package

You can control which users can view a package. To enable a user to view packages, modify the settings listed in [Table 6-1](#):

Table 6-1. Settings to view packages

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

Restricting Package Viewing to Participants

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

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

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

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

Creating a Package

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

Enabling Users to Create Packages

To enable a user to create and submit packages, configure the settings listed in *Table 6-2* on page 85.

Table 6-2. Settings to enable package creation

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

Preventing Users from Selecting a Specific Workflow

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

Table 6-3. Settings to restrict workflow selection

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



Note

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

Preventing Users from Selecting a Specific Object Type

You can prevent users from selecting specific object types as they add lines to a package. *Table 6-4* contains the information you need to restrict Deployment Management object types.

Table 6-4. Settings to restrict object type selection

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

Approving Package Lines

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

Table 6-5. Settings to enable package processing

Setting	Value	Description
License	Deployment Management or Configuration	This license gives a user 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	Deployment Mgmt: Edit Packages	This access grant lets the user generate, edit, and delete packages. To edit the package, user must be its creator, an assigned user, a member of the assigned security group, or a member of the security group for the workflow step.
	Deployment Mgmt: Edit All Packages	This access grant lets the user edit or delete packages at any time.

Enabling Users to Act on a Specific Workflow Step

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

Deleting a Package

To determine who can delete a package, use the settings listed in [Table 6-6](#).

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

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

Overriding Package Security

[Table 6-7](#) lists the settings you must configure to enable a user to view, edit, and delete any package.

Table 6-7. Settings to override package security

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

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



Resource Management Security

In This Chapter:

- *Overview of Resource Management Security*
- ***Working with Resources***
 - *Viewing Resource Information*
 - *Modifying Resource Information*
- *Working with Resource Pools*
 - *Viewing Resource Pools*
 - *Creating Resource Pools*
 - *Modifying Resource Pools*
- *Working with Skills*
 - *Viewing Skills*
 - *Creating, Modifying, and Deleting Skills*
- *Working with the Organization Model*
 - *Viewing the Organization Model*
 - *Modifying Organization Definitions*
- *Working with Staffing Profiles*
 - *Viewing Staffing Profiles*
 - *Creating Staffing Profiles*
 - *Modifying Staffing Profiles*
- ***Working with Calendars***
 - *Viewing and Editing Regional Calendars*
 - *Viewing and Editing Resource Calendars*
- *Additional Protection for Resource Information*
 - *Users Who Are Assigned the Configurator License*
 - *Members of Security Groups with View or Edit Access to Cost Data*

- *Members of Security Groups with View or Edit Access to Resource Data*
 - *Users Who Have the Administrator Password*
 - *Users Who Run the Unsecured “User Detail Report”*
 - *Users Who Are Assigned the Sys Admin: Server Tools - Execute SQL Runner Access Grant*
-

Overview of Resource Management Security

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

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

■ ■ Note

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

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

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

Working with Resources

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

Viewing Resource Information

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

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

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

Modifying Resource Information

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

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

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

Working with Resource Pools

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

Figure 7-1. Configure Access for Resource Pool page

Configure Access for Resource Pool: Operational Pool A

The following users have access to view the Resource Pool for Mercury IT Governance Center. Provide additional editing access on an individual basis.

View Access			Additional Editing Access		
Username	First Name	Last Name	Edit Basic Resource Pool Information	Edit Plan	Edit Security
<input type="checkbox"/>	johnsmith	John Smith	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Give Access to User:

Viewing Resource Pools

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

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

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

Creating Resource Pools

To allow a user to create resource pools, use the settings listed in [Table 7-4](#).

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

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

Modifying Resource Pools

To allow a user to modify resource pool information, use the settings listed in [Table 7-5](#).

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

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

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

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

Figure 7-2. Configure Access for Resource Pool page

Configure Access for Resource Pool: Operational Pool A

The following users have access to view the Resource Pool for Mercury IT Governance Center. Provide additional editing access on an individual basis.

View Access			Additional Editing Access		
Username	First Name	Last Name	Edit Basic Resource Pool Information	Edit Plan	Edit Security
<input type="checkbox"/> johnsmith	John	Smith	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Give Access to User:

Working with Skills

Access to skills is controlled through access grants.

Viewing Skills

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

Creating, Modifying, and Deleting Skills

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

Working with the Organization Model

Access to the organization model is set through access grants.

Viewing the Organization Model

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

Modifying Organization Definitions

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

Table 7-6. Settings to modify organization information.

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

Working with Staffing Profiles

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

Figure 7-3. Configure Access for Staffing Profile page

Configure Access for Staffing Profile: IT Ops

The following users have access to view the Staffing Profile for Mercury IT Governance Center. Provide additional editing access on an individual basis.

View Access			Additional Editing Access			
Username	First Name	Last Name	Edit Basic Staffing Profile Information	Edit Plan and Actuals	Edit Actuals	Edit Security
<input type="checkbox"/>	johnsmith	John Smith	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Give Access to User:

Viewing Staffing Profiles

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

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

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

Creating Staffing Profiles

To allow a user to create a staffing profile, use the settings listed in [Table 7-8](#).

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

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

Modifying Staffing Profiles

To allow a user to modify staffing profile information, use the settings listed in [Table 7-9](#).

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

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

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

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

Figure 7-4. Configure Access for Staffing Profile page

Configure Access for Staffing Profile: IT Ops

The following users have access to view the Staffing Profile for Mercury IT Governance Center. Provide additional editing access on an individual basis.

View Access			Additional Editing Access			
Username	First Name	Last Name	Edit Basic Staffing Profile Information	Edit Plan and Actuals	Edit Actuals	Edit Security
<input type="checkbox"/>	johnsmith	John Smith	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Give Access to User:

Working with Calendars

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

Viewing and Editing Regional Calendars

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

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

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

Viewing and Editing Resource Calendars

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

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

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

Users must have a license for one of the following:

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

Additional Protection for Resource Information

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

Users Who Are Assigned the Configurator License

Users who have the Configuration license can create entities such as reports, and then use those entities to query the database for sensitive data. To prevent this activity, remove the Configuration license. For information about how to remove licenses from a user or set of users, see *Removing Licenses Using the Assign Licenses Wizard* on page 43.



Note

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

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

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

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

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

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

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

Users Who Have the Administrator Password

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

Users Who Run the Unsecured “User Detail Report”

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

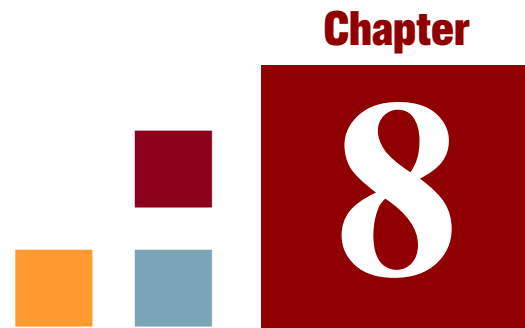


Note

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

Users Who Are Assigned the Sys Admin: Server Tools - Execute SQL Runner Access Grant

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



Cost and Budget Data Security

In This Chapter:

- *Overview of Cost and Budget Data Security*
 - ***Working with Cost Data***
 - *Viewing Cost Data*
 - *Modifying Cost Data*
 - *Working with Budgets*
 - *Viewing Budgets*
 - *Creating Budgets*
 - *Modifying Budgets*
 - *Working with Activities*
 - *Viewing Activities*
 - *Creating and Modifying Activities*
 - *Working with Regions*
 - *Working with Financial Exchange Rates and Currencies*
-

Overview of Cost and Budget Data Security

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

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

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

■ ■ Note

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

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

Working with Cost Data

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

Viewing Cost Data

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

Making Project Cost Data Visible to Users

If Financial Management is enabled for a project, you can use the **Project Security** section of the Project Settings page (see *Figure 8-1* on page 105) to specify who can view cost information. You can make cost information on the project and tasks visible to one of the following user groups:

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



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

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

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

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

Making Program Cost Data Visible to Users

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

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

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



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

Figure 8-2. Configure Access page for programs

Configure Access for Global IT Ops Initiative

Program Access

In addition to Thomas Wilcox, the Program Manager(s) of this Program, give view access to:

- No One
- All Project Managers of Projects in this Program
- All other Program Managers
- All Program Managers; and Project managers in this Program
- Only these Security Groups:

Note: Only the Program Manager(s) of this Program can delete this Program.

Cost Access

In addition to Thomas Wilcox, the Program Manager(s) of this Program, give view access to:

- No One
- All Project Managers of Projects in this Program
- All other Program Managers
- All Program Managers; and Project managers in this Program
- Only these Security Groups:

Modifying Cost Data

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

For information on how to allow users to view cost information, see [Viewing Cost Data on page 104](#).

Working with Budgets

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

Figure 8-3. Configure Access for Budget page

Configure Access for Budget: Global IT Operations

The following users have access to view the Budget for Mercury IT Governance Center. Provide additional editing access on an individual basis.

View Access			Additional Editing Access			
Username	First Name	Last Name	Edit Basic Budget Information	Edit Plan and Actuals	Edit Actuals	Edit Security
<input type="checkbox"/>	johnsmith	John Smith	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Give Access to User:

Viewing Budgets

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

Table 8-1. Settings to view budget information

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

Creating Budgets

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

Table 8-2. Settings to create budgets

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

Modifying Budgets

To allow users to modify budget information, use the settings on the Configure Access for Budget page shown in *Figure 8-4 on page 111*, which are listed in *Table 8-3*.

Table 8-3. Settings to allow users to modify budgets

Setting	Value	Description
Access Grant (only one is required)	Financial Mgmt: Edit All Budgets	Edit and delete any budget.
	Financial Mgmt: Edit Budgets	Edit budget information when the user has been granted edit access in the Configure Access for Budget page. Delete these budgets when given sufficient access in the Configure Access for Budget page for that budget.
Additional Editing Access	Edit Basic Budget Information	Used in conjunction with the Financial Mgmt: Edit Budgets access grant, lets the user edit budget header fields, user data, and notes. The user cannot change the Periods or any information in the Budget Breakdown section.
	Edit Plan and Actuals	Used in conjunction with the Financial Mgmt: Edit Budgets access grant, lets the user edit the Periods and the information in the Budget Breakdown section. Also lets the user view and edit the planning and actuals data in the Budget Breakdown table.
	Edit Actuals	Used in conjunction with the Financial Mgmt: Edit Budgets access grant, lets the user edit the Periods and the information in the Budget Breakdown section. Also lets user view and edit actuals data in the Budget Breakdown table.
	Edit Security	Used in conjunction with the Financial Mgmt: Edit Budgets access grant, lets the user edit the list of users who can use the Configure Access for Budget page (<i>Figure 8-4</i>) to modify the budgets.

Figure 8-4. Configure Access for Budget page

Configure Access for Budget: Global IT Operations

The following users have access to view the Budget for Mercury IT Governance Center. Provide additional editing access on an individual basis.

View Access			Additional Editing Access			
Username	First Name	Last Name	Edit Basic Budget Information	Edit Plan and Actuals	Edit Actuals	Edit Security
<input type="checkbox"/>	johnsmith	John Smith	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Give Access to User:

Working with Activities

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

Viewing Activities

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

Creating and Modifying Activities

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

Working with Regions

To allow users to view, create, or modify regions, assign the access grants listed in [Table 8-4](#).

Table 8-4. Access grants for working with regions

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

Working with Financial Exchange Rates and Currencies

To control who can view, create, or modify financial exchange (FX) rates, you use the same access grants that you use to control who can modify currency.

Table 8-5 lists these access grants.

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

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



Chapter
9

Dashboard Security

In This Chapter:

- *Controlling User Access to Portlets in the Dashboard*
 - *Disabling Custom Portlets*
 - *Restricting User Access*
 - *Restricting Data to Participants*
-

Controlling User Access to Portlets in the Dashboard

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



Note

For information about configuring security for Dashboard modules, see *Configuring the Standard Interface*.

Disabling Custom Portlets

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

To disable a custom portlet:

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

Configure Portlet Definition: Analyze Assignment Load

This is a built-in Portlet Definition. It cannot be deleted. Save Done Cancel

Portlet Type: Java Portlet Display Name: Analyze Assignment Load
 Name: Analyze Assignment Load Category: Resource Management
 Description: Analyze Assignment Load Portlet.
 Default Width: Wide
 Enabled: Yes No

Configure Access

User Access

Users specified below will have access to add this Portlet to their dashboards.

Require users to have one of these licenses:

Require users to have one of these privileges:

Allow access to only the following users and groups:

Security Type	Name
All Users	

Give Access to:

Administrator Access

Users specified below will have access to modify this Portlet Definition.

Security Type	Name
All Portlet Definition Administrators	

Give Access to:

Save Done Cancel

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



Note

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

- Click **Save**.

Restricting User Access

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

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

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

The screenshot shows the 'Configure Access' section of the dashboard configuration interface. It is divided into two main subsections: 'User Access' and 'Administrator Access'. Each subsection contains a table with columns for 'Security Type' and 'Name'. Below each table is a 'Give Access to:' field with a dropdown menu (currently showing 'User') and an 'Add' button. The 'User Access' section also includes fields for 'Require users to have one of these licenses' and 'Require users to have one of these privileges'. At the bottom of the form are 'Save', 'Done', and 'Cancel' buttons.

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

6. Click **Add**.

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

Configure Access

User Access

Users specified below will have access to add this Portlet to their dashboards.

Require users to have one of these licenses:

Require users to have one of these privileges: View my personal re

Allow access to only the following users and groups:

Security Type	Name
<input checked="" type="checkbox"/> Group	ITG Cost Manager
<input checked="" type="checkbox"/> Group	ITG Program Manager
<input checked="" type="checkbox"/> Group	ITG Project Manager

Give Access to:

Administrator Access

Users specified below will have access to modify this Portlet Definition.

Security Type	Name
All Portlet Definition Administrators	

Give Access to:

7. Click **Save**.

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

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

Restricting Data to Participants

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



Note

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



Chapter
10

Configuration Security

In This Chapter:

- *Overview of Configuration Security*
 - *Setting Ownership for Configuration Entities*
 - *Removing Access Grants*
-

Overview of Configuration Security

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

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

Setting Ownership for Configuration Entities

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

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

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

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

- User definitions
- Validations
- Workflows
- Workflow steps

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

For example, to set the ownership for a workflow:

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

The Workbench opens.

3. From the shortcut bar, select **Configuration > Workflows**.

The Workflow Workbench opens.

4. Click **List**.

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

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

6. Click the **Ownership** tab.

7. Click **Only groups listed below that have the Edit Workflows Access Grant**.

8. Click **Add**.

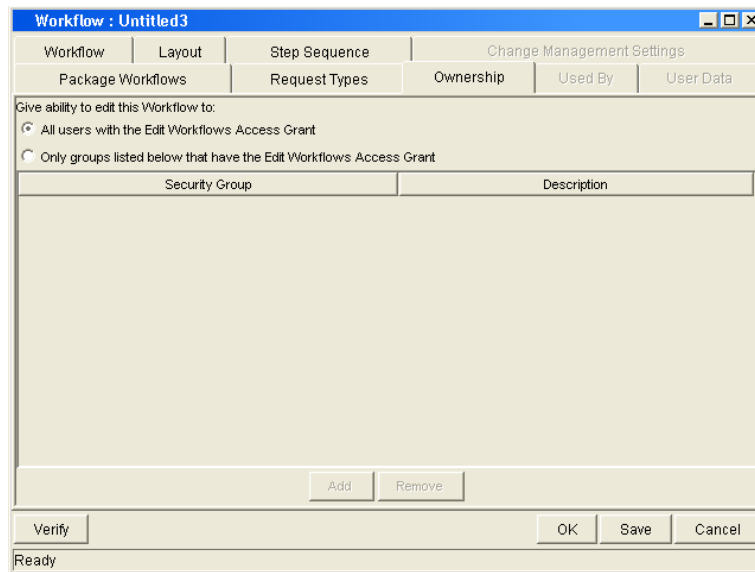
The Add Security Group window opens.

9. Select the security group.

10. Do one of the following:

- To add the current security group and continue adding security groups, click **Add**.
- To add the current security group and close the window, click **OK**.

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



11. Do one of the following:

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

■ ■ Note

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

Removing Access Grants

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

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

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



Note

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

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

Table 10-1. Access grants for editing configuration entities (page 1 of 3)

Category	Access Grant Name	Description
Config	Edit Activities	View, create, edit, or delete activities in the Dashboard.
Config	Edit Notification Templates	Create, edit, and delete notification templates in the Notification Templates Workbench.
Config	Edit Report Types	Create, edit, and delete report types in the Report Types Workbench.
Config	Edit Special Commands	Create, edit, and delete special commands in the Special 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 Validation Workbench.
Config	Edit Validations	Create, edit, and delete validations in the Validation Workbench.
Config	Edit Workflows	Create, edit, and delete workflows in the Workflows Workbench.

Table 10-1. Access grants for editing configuration entities (page 2 of 3)

Category	Access Grant Name	Description
Demand Mgmt	Edit Request Header Types	Create, edit, and delete request header types in the Request Header Types Workbench.
Demand Mgmt	Edit Request Types	Create, edit, and delete request types in the Request Types Workbench.
Deployment Mgmt	Edit All Packages	Create, edit, and delete any package.
Deployment Mgmt	Edit All Releases	Create, edit, and delete any release.
Deployment Mgmt	Edit Object Types	Create, edit, and delete object types in the Object Types Workbench.
Deployment Mgmt	Edit Packages	Create, edit, and delete packages for which the user is an assigned resource.
Deployment Mgmt	Edit Releases	Create, edit, and delete releases for which the user is an assigned resource.
Program Mgmt	Edit All Programs	Create, edit, and delete any program.
Program Mgmt	Edit Programs	Create, edit, and delete programs on which the user is an assigned resource or program manager.
Project Mgmt	Edit Project Templates	Create, edit, and delete project templates.
Project Mgmt	Edit Projects	Create projects. Update and delete projects and subprojects if 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.
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.

Table 10-1. Access grants for editing configuration entities (page 3 of 3)

Category	Access Grant Name	Description
System	Edit Portlet Definition	Create, edit, and delete portlets in the Portlets Workbench.
Time Mgmt	Edit Charge Codes	Create, edit, and delete charge codes in the Charge Codes Workbench.
Time Mgmt	Edit Override Rules	Create, edit, and delete override rules in the Override Rules Workbench.
Time Mgmt	Edit Time Sheet Policies	Create, edit, and delete policies in the Time Sheet Policies Workbench.



Chapter
11

Service Provider Functionality

In This Chapter:

- *Recommended Practice: Service Provider Functionality*
-

Recommended Practice: Service Provider Functionality

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

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

Step 1: Create a service provider user.

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

The Workbench opens.

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

The User Workbench opens.

4. Click **New User**.

The User window opens to the **User Information** tab.

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

Step 2: Create the service provider security group.

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

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

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



Note

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

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



Note

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

8. Click **OK**.

Step 3: Set ownership on the user.

1. From the Workbench shortcut bar, select **Sys Admin > Users**.
The User Workbench opens.
2. Locate and open the Restricted User 1 user record.
3. Click the **Ownership** tab.
4. Under **Give ability to edit this User to**, select **Only groups listed below that have the Edit Users access grant**.
5. Click **Add**.
The Add Security Group window opens.
6. Locate and select the Restricted Users security group.
7. Click **OK**.
8. Click **Save**.

Step 4: Set ownership on the security group.

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

Step 5: Add a server configuration parameter.

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

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



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

3. Save the `server.conf` file.
4. Restart the Mercury IT Governance Server.

Step 6: Test the functionality.

To test the functionality of the new user group:

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

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

1. After you perform steps 1 through 6, log on to Mercury IT Governance Center as Restricted User 1.
2. From the menu bar, select **Administration > Open Workbench**.
The Workbench opens.
3. From the shortcut bar, select **Sys Admin > Users**.
The User Workbench opens.
4. Click **List**.
5. On the **Results** tab, in the **Username** column, locate and click **Restricted User 1**.
6. Click **Copy**.

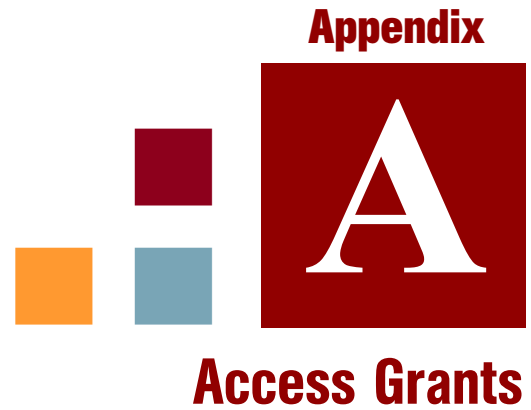
The Copy User window opens.

7. Enter a new user name and password, and then confirm the password.
8. Click **OK**.

The User Workbench prompts you to indicate whether you want to edit the user.

9. Click **No**.

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



The graphic features the word "Appendix" in a bold, dark red font at the top right. Below it is a large red square containing a white stylized letter "A". To the left of this square are three smaller squares: an orange one at the bottom left, a blue one in the middle, and a dark red one at the top right. Below the graphic, the words "Access Grants" are written in a bold, dark red font.

Appendix

Access Grants

Access grants enable certain activities within Mercury IT Governance Center. Mercury IT Governance Center comes with predefined access grants. Installing a Mercury Deployment Management Extension may introduce additional access grants. [Table A-1 on page 131](#) lists the available access grants and provides a description of each.

■ ■ Note

View access grants provide read-only access to screens and entities. Users without the View access grant cannot see certain workbenches and windows.

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

For details on specific access grants, see [Table A-1 on page 131](#).

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

Category	Access Grant Name	Description
Config	Edit Activities	Modify activities in the Activities Workbench.
Config	Edit Notification Templates	Create, update, and delete notification templates in the Notification Templates Workbench.
Config	Edit Report Types	Create, update, and delete report types in the Report Types Workbench.
Config	Edit Special Commands	Create, update, and delete special commands in the Special Commands Workbench.

Table A-1. Access grants (page 2 of 13)

Category	Access Grant Name	Description
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 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.
Config	View Workflows	View workflow definitions in the Workflows Workbench.
Demand Mgmt	Access Query Builder	Use the request query builder on the Search Requests page.
Demand Mgmt	Change Request Type	Change the request type for existing requests.
Demand Mgmt	Edit Contacts	Create and update contacts in the Contact 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.

Table A-1. Access grants (page 3 of 13)

Category	Access Grant Name	Description
Demand Mgmt	Edit Requests	<p>Perform basic request processing actions: create requests, edit certain requests, and delete requests that you have not submitted.</p> <ul style="list-style-type: none"> ■ Allows the user to generate requests. ■ User cannot change the workflow when creating or editing a request. ■ Allows the user to edit the request as specified on the User Access tab in the Request Type window. ■ Allows the user to delete the request as specified on the User Access tab in the Request Type window. ■ Allows the user to cancel the request as specified on the User Access tab in the Request Type window.
Demand Mgmt	Edit All Contacts	Edit and delete contacts using the Contact Workbench.
Demand Mgmt	Edit 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	Edit All Requests	<p>Perform advanced request processing actions: creating, editing, deleting, changing the request's workflow, and overriding references.</p> <ul style="list-style-type: none"> ■ 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 as defined on the request type's User Access tab.
Demand Mgmt	View All Contacts in Request	View all contacts in a request, even if a company is associated with the request.

Table A-1. Access grants (page 4 of 13)

Category	Access Grant Name	Description
Demand Mgmt	View Contacts	View the contact definition in the Contact Workbench.
Demand Mgmt	View Request Header Types	View request header type definitions in the Request Header Types Workbench.
Demand Mgmt	View Request Types	View the request type definition in the Request Types Workbench.
Demand Mgmt	View Requests	View request type definitions in the Request Types Workbench.
Deployment Mgmt	Edit Object Types	Create, edit, and delete object types in the Object Types Workbench.
Deployment Mgmt	Edit Packages	<p>Perform basic package processing actions: create, edit certain related packages, and delete certain packages that have not been submitted.</p> <ul style="list-style-type: none"> ■ 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.
Deployment Mgmt	Edit Releases	<p>Perform basic release processing actions in the Releases Workbench: create, edit, process, and delete certain related releases.</p> <p>A user with this grant can:</p> <ul style="list-style-type: none"> ■ View any release ■ Be designated as the release manager ■ Create releases ■ Edit or delete any release that he created ■ Act on any distribution workflow steps where he is included in the step security. ■ Edit or delete a release that he did not create (only if he is designated as the release manager in the Release Management window).
Deployment Mgmt	Edit All Packages	Edit or delete any packages.

Table A-1. Access grants (page 5 of 13)

Category	Access Grant Name	Description
Deployment Mgmt	Edit All Releases	Create, edit and delete any release using the Releases Workbench. A user with this grant can: <ul style="list-style-type: none"> ■ 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 he is specified as the release manager in the Release Management window).
Deployment Mgmt	Override Deployment Mgmt Participant Restriction	View the detailed information on a restricted package for which the user is not an active participant.
Deployment Mgmt	Submit Environment Refreshes	Create and submit an environment refresh in the Env Refresh Workbench.
Deployment Mgmt	View Environment Refreshes	View environment refresh definitions in the Env Refresh Workbench.
Deployment Mgmt	View Object Types	View object type definitions in the Object Types Workbench.
Deployment Mgmt	View Packages	View packages in the standard interface or the Package Workbench.
Deployment Mgmt	View Releases	View release definitions in the Releases Workbench. Act on any distribution workflow steps that include the user in the step security.
Environments	Edit Environments	Create, update and delete environments in the Environment Workbench.
Environments	View Environments	View environment definitions in the Environment Workbench.

Table A-1. Access grants (page 6 of 13)

Category	Access Grant Name	Description
Financial Mgmt	Approve Budgets	Change the Budget Status value on the Modify Budget page to Approved . The user must also have the Update Budgets Status grant and either the Edit Budget or Edit All Budgets grant to perform this function. Note that Approved is available in the Budget Status list only if you have this grant.
Financial Mgmt	Approve Financial Benefits	The user can set Financial Benefit Status to Approved , but nothing else. This grant is 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. This grant is supplemental to the Edit Financial Benefits or Edit All Financial Benefits access grant.
Financial Mgmt	Edit All Financial Benefits	The user can edit all financial benefit in the system.
Financial Mgmt	Edit Budgets	Edit budget information when the user has been granted edit access on the Configure Access for Budget page.
Financial Mgmt	Edit Work Plan Cost Data	Edit cost data related to tasks, projects, programs, resources and skills. The user must also have access to edit these entities.
Financial Mgmt	Edit Cost Security	Edit cost security settings for a project in the Project Settings window. Edit cost security settings for a program on the Program Security Configuration page. Note: For this grant to be relevant, the user must also be able to edit the project settings and program security.
Financial Mgmt	Edit Financial Benefits	The user can edit any financial benefit for which he is on the specified Edit list.
Financial Mgmt	Edit Cost Rate Rules	The user can create, edit, and delete cost rate rules.

Table A-1. Access grants (page 7 of 13)

Category	Access Grant Name	Description
Financial Mgmt	Edit 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 do this.
Financial Mgmt	Update Financial Benefit Status	The user can update the Financial Benefit Status, but nothing else. Supplemental to the Edit Financial Benefits or Edit All Financial Benefits access grant.
Financial Mgmt	View All Budgets	View budget information for all budgets in 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 on the Configure Access for Budget page.
Financial Mgmt	View Project, Program, and Time Sheet Cost Data	View cost data related to tasks, projects, programs, resources, and skills. The user must also have access to view these entities.
Financial Mgmt	View Cost Rate Rules	View cost rate rules on the Cost Rate Rules page.
Financial Mgmt	View Financial Benefits	The user can view any financial benefit for which he is on the specified View or Edit list.
Financial Mgmt	View Financial Exchange Rates	The user can view financial exchange rates.
PMO	Edit Programs	Update programs where the user is specified as the program manager.
PMO	Edit All Programs	Create and update any program.
PMO	View Programs	View program definitions.
Portfolio Mgmt	Configure Portfolio Management	Gives the user access to the Configure Portfolio Management page where he can set portfolio tracking and categorization metrics.

Table A-1. Access grants (page 8 of 13)

Category	Access Grant Name	Description
Portfolio Mgmt	Edit Scenario Comparison	The user can view, edit, and delete any scenario comparison for which he is on the specified Edit list, and can create new scenario comparisons.
Portfolio Mgmt	Edit All Scenario Comparisons	The user can view, edit, and delete any scenario comparisons in the system, and create new scenario comparisons.
Portfolio Mgmt	Portfolio Manager	Provides the user with access to the following additional Portfolio Management portlets and visualizations: <ul style="list-style-type: none"> ■ Portfolio by Category ■ Current Portfolio Map ■ View Current Portfolio ■ Resource by Category
Portfolio Mgmt	View Scenario Comparison	The user can view any scenario comparison for which they are on the specified View or Edit list.
Project Mgmt	Create Projects	If the user is also assigned either the Edit Projects or the Edit All Projects access grant, the user can create a project from the menu bar in the standard interface.
Project Mgmt	Edit Project Types	Create and edit project types.
Project Mgmt	Edit Projects	Create projects. Update and delete projects and subprojects if specified as the project manager.
Project Mgmt	Edit Work Plan Templates	Create and modify work plan templates.
Project Mgmt	Edit All Projects	Create, edit, and delete projects. Override (or remove) references on projects or tasks.
Project Mgmt	View All Projects	View the detailed information on a restricted project on which the user is not an active participant.
Project Mgmt	Update Tasks	Update project tasks.
Project Mgmt	View Project Types	Access and view project types.
Project Mgmt	View Projects	View project definitions.
Project Mgmt	View Work Plan Templates	View work plan templates.

Table A-1. Access grants (page 9 of 13)

Category	Access Grant Name	Description
Resource Mgmt	Create Resource Pools	Create resource pools using the standard interface. The user must also have either the Resource Mgmt: Edit Resource Pools or Resource Mgmt: Edit All Resource Pools grant.
Resource Mgmt	Create Staffing Profiles	Create staffing profiles using the standard interface. The user must also have either the Resource Mgmt: Edit Staffing Profiles or Resource Mgmt: Edit All Staffing Profiles grant.
Resource Mgmt	Edit All Resource Pools	Edit or delete any resource pool.
Resource Mgmt	Edit All Resources	Edit the resource information for any resource defined in Mercury IT Governance Center.
Resource Mgmt	Edit All Roles	Create, edit, and delete all roles 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	Allows the user to edit or delete any staffing profile in the system.
Resource Mgmt	Edit Entire Organization	Edit and delete any organization unit.
Resource Mgmt	Edit My Calendar	A user who also has the View All Resources access grant can edit his or her own calendar information.
Resource Mgmt	Edit Only Organization Units That I Manage	Edit organization unit information for units that list the current user as the manager in the View Organization Unit page. Also delete any of these organization units.
Resource Mgmt	Edit only resources that I manage	Edit resource information for resources that list the current user as the Direct Manager. A resource's Direct Manager is displayed on the View Resource page.
Resource Mgmt	Edit Regional Calendars	Create, edit, and delete regional calendars defined in Mercury IT Governance Center.

Table A-1. Access grants (page 10 of 13)

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

Table A-1. Access grants (page 11 of 13)

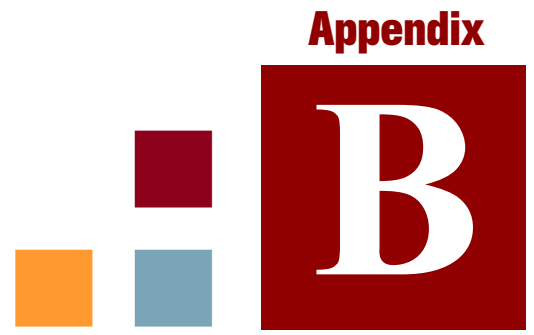
Category	Access Grant Name	Description
Resource Mgmt	View Regional Calendars	View all regional calendars defined in Mercury IT Governance Center.
Resource Mgmt	View Regions	View all regions defined in Mercury IT Governance Center.
Resource Mgmt	View Resource Pools	View resource pool information if the user has been granted view access on the Configure Access for Resource Pool page.
Resource Mgmt	View Staffing Profiles	View staffing profile information if the user has been granted view access on the Configure Access for Staffing Profile page.
Sys Admin	Configure Modules	Create, edit, and delete modules on Module Configuration in the Dashboard page. View and set the default dashboard on the Set Default Dashboard in the Dashboard page.
Sys Admin	Distribute Modules	View, publish, and distribute modules, pages and portlets to dashboards on the Distributing Modules Dashboard page.
Sys Admin	Edit Security Groups	Create, update, and delete security groups in the Security Groups Workbench. The user must also have the Edit Users access grant.
Sys Admin	Edit Users	Create, update, and delete users in the Users Workbench.
Sys Admin	Migrate Kintana Objects	Migrate configuration objects (such as workflows and request types) using the Migrators.
Sys Admin	Server Administrator	Stop the Mercury IT Governance Server, log on to the application when the server is started in restricted mode, and send messages via kWall.sh.
Sys Admin	Server Tools: Execute Admin Tools	Execute administration reports in the Admin Tools window and view the SQL Runner window in the Server Tools Workbench.
Sys Admin	Server Tools: Execute SQL Runner	Execute SQL statements in the SQL Runner window and view the Admin Tools window in the Server Tools Workbench.
Sys Admin	Synchronize Meta Layer	Perform reporting meta layer synchronizations using the Report Types Workbench.

Table A-1. Access grants (page 12 of 13)

Category	Access Grant Name	Description
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	Edit All Reports	Use the Reports Workbench to delete any submitted report.
System	Open Workbench	Open the Mercury IT Governance Center Workbench.
System	Override Document Check Out	Override document check out.
System	Override Key Fields Segmentation	View all information contained in restricted key fields. Key fields include: <ul style="list-style-type: none"> ■ 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 Deployment Management packages
System	Ownership Override	Access and edit all configuration entities even if the user is not a member of one of the entity's ownership groups.
System	Submit Reports	Submit reports in 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 if the resource is a direct report or if the time sheet has been delegated to the user.

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

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



Appendix

B

License Types

In This Appendix:

- *License Types*
 - *Deployment Management Extension Licenses*
-

License Types

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

- Product licenses

Product licenses are for 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, and the Workbench interface, depending on the product license used.

The product licenses are as follows:

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

- Configuration license

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

- User Administration license

The User Administration license is for users responsible for administering Mercury IT Governance Center users and security, as well as the application itself. It is required to configure user accounts and security groups, and to run reports related to importing new users through the Open

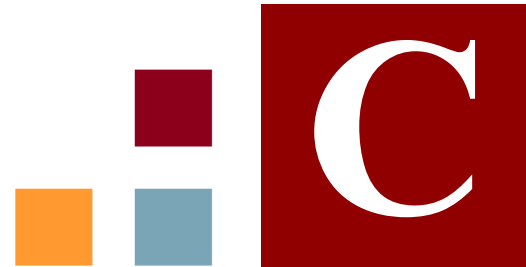
Interface. This license also gives a user access to the System Administration functionality of the Mercury IT Governance Center licensed at your site.

User access to screens and functions in Mercury IT Governance Center are controlled by a combination of license and access grants. The following sections address only the licenses required to perform specific tasks. For additional details on access grants, which are also required, see [Appendix A, *Access Grants*](#), on page 131.

Deployment Management Extension Licenses

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

Appendix



Licenses and User Roles

This appendix addresses the typical user functions and required licenses by user types and by product/license type. [Table C-1 on page 149](#) lists the licenses required by, and recommended for, different types of users. [Table C-2 on page 152](#) lists the user roles and functions based on product/license types.

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

User Type	Tasks	Required and Recommended () Licenses (Unless noted with an asterisk*, these are product licenses.)
Business User	Submit requests, monitor status of own requests, and provide user sign-off.	<ul style="list-style-type: none">■ Demand Management
Business Project Manager	Create, plan, and monitor project workplans—update tasks; assign resources; schedule, define project exception rules; set notifications; maintain project templates, manage scope changes, issues, and risk. Manage resource skills, pools, profiles, and capacity. Manage project budget and expenses. Synchronize with Microsoft Project.	<ul style="list-style-type: none">■ Demand Management■ Program Management■ Project Management■ (Time Management)

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

User Type	Tasks	Required and Recommended () Licenses (Unless noted with an asterisk*, these are product licenses.)
Business Analyst	Monitor initiative (schedule and cost) status; act on SLA exceptions; track issues; manage scope changes, issues, and risk. Manage portfolio.	<ul style="list-style-type: none"> ■ Demand Management ■ Portfolio Management ■ Program Management ■ Project Management
Business Manager	Monitor initiative (schedule, cost, earned value) status, act on SLA exceptions, prioritize portfolio.	<ul style="list-style-type: none"> ■ Demand Management ■ Portfolio Management ■ Program Management ■ Project Management
IT Management: CIOs, IT VPs, Directors, Enterprise Architects, CTOs	Monitor status of initiatives (schedule and cost), drill down on SA exceptions, control and prioritize portfolio. Monitor resource use. Manage resource capacity and IT budgets.	<ul style="list-style-type: none"> ■ Demand Management ■ Portfolio Management ■ Program Management ■ Project Management ■ (Time Management) ■ (Deployment Management)
Process and Project participants: IT Support Analyst, QA, team member, Change Control	Participate in project tasks and in request processes. Execute project tasks and update task status. Actively resolve requests—update request information, perform approvals, assign requests, prioritize requests, move requests through the workflow.	<ul style="list-style-type: none"> ■ Demand Management ■ Project Management ■ (Time Management)
Engineering Team: Developer, Infra- structure (DBA / Sysadmin / Web Admin), Release Manager, Operations	Create packages, update package information, perform approvals, schedule and execute migrations. Update tasks. Create and manage deployment releases.	<ul style="list-style-type: none"> ■ Deployment Management

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

User Type	Tasks	Required and Recommended () Licenses (Unless noted with an asterisk*, these are product licenses.)
Portfolio Manager, Program Manager, IT Controller	<p>Manage portfolio. Manage rating and prioritization of projects.</p> <p>Perform what-if portfolio scenarios.</p> <p>Manage scope changes, issues, and risk.</p> <p>Manage resource skills, pools, profiles, and capacity.</p> <p>Manage project budget and expenses.</p>	<ul style="list-style-type: none"> ■ Demand Management ■ Portfolio Management ■ Program Management ■ Project Management ■ (Time Management)
Project Manager	<p>Create, plan, and monitor project workplans—update tasks, assign resources, schedule, define project exception rules, set notifications, maintain project templates.</p> <p>Manage resource skills, pools, profiles, and capacity.</p> <p>Manage project budget and expenses.</p> <p>Synchronize with Microsoft Project (if required).</p>	<ul style="list-style-type: none"> ■ Project Management ■ (Time Management)
Mercury IT Governance Center User Administrator	<p>Common administration functions, including set up users and assign security.</p>	<ul style="list-style-type: none"> ■ Demand Management ■ User Administration License*
Mercury IT Governance Center Administrator, Process Owner / Implementer	<p>Common administration functions such as configure user-defined project information, and configure report types and Dashboard portlets.</p> <p>Configure object types, model process workflows; and configure business rules.</p>	<ul style="list-style-type: none"> ■ Demand Management ■ Configuration License*

Table C-2. User roles and functions by product license type (page 1 of 3)

Product	License Type	User Type	Primary Tasks Performed with this License Type
Dashboard	Any	All	Overall visibility of status and metrics, drill down to a specific level of detail on requests, task, projects, and packages requiring action or further review.
Demand Management	Configuration	IT Process Analyst	Configure workflows and request types.
	Project Management	Project Manager, Resource Manager	Create and manage resource pools and project resource profiles. Manage resource capacity and use. Create and manage budgets for departments, programs, and projects.
	Demand Management	Business User, Requestor	Submit requests, monitor the status of own request, and provide user sign-off.
		Analyst, IT Support Staff, Request Contact	Participate in the request processes and actively resolve requests—update request information, perform approvals, assign requests, prioritize requests, move requests through the workflow.
		Upper-level Manager, Business Analyst, Change Control Team, Project Manager, Program Manager	Monitor SLAs and act on exceptions, run reports, and perform approvals. Prioritize demand, assign requests. participate in deployment management.
Portfolio Management	Portfolio Management	Portfolio Manager, Business Analyst, Program Manager, Enterprise Architect, CTO, IT Controller	Manage IT portfolio. Explore what-if scenarios. Evaluate value and mix of current and proposed projects. Rank and rate projects. Create and manage resource pools and project resource profiles. Manage resource capacity and utilization. Create and manage budgets for departments, programs, and projects. Track and compare actuals to budgets, perform earned value analysis.
Program Management	Program Management	Program Manager	Prioritize programs and projects. Manage program and project initiation; monitor resource utilization; monitor program status, scope changes, issues, and risk. Act on exceptions.

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

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 pools 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 Manager, 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 start-end dates and periods, and approval hierarchies.

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

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

A

- access grants 48
 - described 13
 - for creating and modifying financial exchanges rates 112
 - for creating regions 111
 - for modifying regions 111
 - for viewing financial exchange rates 112
- list 131
- removing 121
- viewing regions 111

- administrator 22
- app codes 34
- App Codes tab
 - security groups 34
- approving
 - security for package lines 87
- authentication mode 21

B

- budget security 103
- budgets
 - creating 109
 - modifying 110
 - viewing 108

C

- charge code rules 35
- configuration security 118
- configuration-level restrictions 14
- cost data
 - making visible for programs 106
 - modifying 107
 - project data visibility 105
 - viewing 104
- cost security 103
- creating
 - packages, setting security for 84
 - resource pools, security for 93
 - security groups 27
 - staffing profiles 97
 - users, security for 18
- creating regions
 - access grant for 111

D

- dashboard
 - restricting data to participants 116
- deleting
 - packages, security settings for 88
- Deployment Management
 - app codes tab 34

E

entity-level restrictions 13

F

field-level restrictions 13

financial exchange rates
access grant for viewing 112

financial exchanges rates
access grant for viewing 112

financial information security 103

I

importing
users 26

L

licenses 47
and user roles 149
assigning from the User Workbench 38
assigning in batch 40
assigning using the open interface 44
described 13
managing 37
removing using the wizard 43
using the wizard 40

M

modifying regions
access grant for 111

O

organization model
changing 95
security for viewing 95
setting security for 95
ownership 118

P

package

acting on workflow step 87
security for deleting 88

package lines
setting security for approving 87

package security 81
overriding 88

packages
participant restriction 84
security for creating 84
security for selecting a specific
workflow 86
security for viewing 83
security overview 82
selecting a specific object type, security
for 86

portlets
controlling access 114
disabling 114
restricting user access 115

project security
overriding 80

projects
controlling resources 77
creating 77
editing 78
security for viewing 75

R

regions
access grant for viewing 111

request
creating 52
processing 57

request creation security
enabling users 52
workflow restrictions 55

request processing security
workflow step security 62

request security 45

requests
field attributes 67

- field level security 65, 68
- overriding security 72
- status dependencies 71
- viewing 49
- viewing and editing fields 65
- resource
 - viewing information about 91
- resource information
 - configuring 26
- resource pools
 - security for creating 93
 - security for modifying 93
 - setting security for working with 92
 - viewing 92
- resources 91
 - project security 77
 - setting security for modifying 91

S

- security
 - for creating users 18
 - for packages, overview 82
- security groups
 - app codes tab 34
 - creating 27
 - linking users to 23
 - membership controlled by Resource Management 33
 - specifying list of users 29
- skills
 - access to 94
 - security for creating 94
 - security for deleting 94
 - security for editing 94
 - security for viewing 94
- staffing profiles 96
 - creating 97
 - modifying 97
 - viewing 96

T

- task
 - editing 78
- tasks
 - security for viewing 75
 - updating 79

U

- user roles 149
- users
 - granting access 52
 - importing from a database or LDAP 26
 - linking to security groups 23
 - resource information 26
 - restricting 55
 - security for creating 18

W

- workflow
 - step security 62
- workflow step security 62
- workflow steps
 - security 62

