

Mercury IT Governance Center™

**Mercury Program Management
Configuration Guide**

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	v
List of Tables	vii
Chapter 1: Getting Started with Mercury Program Management Configuration	9
Introduction to Mercury Program Management.....	10
Overview of Program-Related Request Types	10
Overview of Program Management Configuration	14
Step One: Gather Information.....	14
Step Two: Configure Program Management Request Types	15
Step Three: Configure Program Management Workflows	15
Step Four: Add Custom User Data Fields to Program Pages.....	16
Step Five: Set Security for Program Management.....	16
Related Documents.....	17
Related Documents	17
Chapter 2: Configuring Program Management Request Types and Workflows.....	19
Configuring Program Management Request Types	20
Configuring Program Management Workflows.....	24
Configuring the Cost Roll-Up Service Interval	26
Chapter 3: Configuring User Data	27
Overview of User Data.....	28
Referring to User Data	29
Adding Custom User Fields to Programs.....	29
Configuring the Default Value for a Custom User Field	33
Configuring Default Security for a Custom User Field.....	34

More Information About Configuring User Data	38
Chapter 4: Configuring Security for Program Management	39
Program Management Security	40
Required Licenses	41
Program Management.....	41
Demand Management.....	41
Project Management.....	41
Access Grants.....	42
Security Groups	42
Creating a Security Group and Assigning It Access Grants	42
Configuring Program Management Users.....	45
Associating Security Groups with Workflows	46
Index	49

List of Figures

Figure 1-1	Field Groups window	12
Figure 3-1	User data types listed in the User Data Workbench	28

List of Tables

Table 1-1	Program Management request types and field groups.....	13
Table 1-2	Program Management request types and workflows	15
Table 4-1	Security features.....	40
Table 4-2	Program Management security group scenario.....	44
Table 4-3	Program Management security group and license scenario.....	46

Chapter

1

Getting Started with Mercury Program Management Configuration

In This Chapter:

- *Introduction to Mercury Program Management*
 - *Overview of Program-Related Request Types*
 - *Overview of Program Management Configuration*
 - *Step One: Gather Information*
 - *Step Two: Configure Program Management Request Types*
 - *Step Three: Configure Program Management Workflows*
 - *Step Four: Add Custom User Data Fields to Program Pages*
 - *Step Five: Set Security for Program Management*
 - *Related Documents*
-

Introduction to Mercury Program Management

Mercury Program Management™ gives program managers a single location from which to initiate, operate, and manage a portfolio of programs and projects. An enterprise can use it to organize and guide the delivery of a business capability through multiple projects and releases, while maintaining alignment with the overall corporate vision.

In Mercury IT Governance Center, a program is a collection of projects linked by common business objectives, and associated scope changes, risks, and issues. For example, XYZ Corporation creates a program to upgrade its customer service computer system to better meet the needs of its sales force. The Customer Service, Sales, and IT organizations create their own projects for this program. Changes and proposed changes at both the program and project level are tracked together.

Program Management users can drill down into projects and requests for detailed information. Users can view roll-ups of relevant data from projects and requests.

Program managers can:

- Oversee the milestones and deliverables of all IT projects
- Identify and mitigate risk
- Manage scope changes
- Resolve inter-project issues

Like projects, programs have associated “health” conditions and configurable exception indicators. However, while a project represents a body of work with a distinct start and finish, programs are often open-ended, and involve initial implementation as well as ongoing maintenance, upgrade, and realignment with changing organization business objectives.

Overview of Program-Related Request Types

During the life of a program, problems and concerns arise that must be addressed. Mercury IT Governance Center provides a framework that your organization can use to identify and, ultimately, resolve problems through submitted requests. The requests that users submit are tracked, rejected, completed, and reported.

Program Management includes the following request types, all of which affect programs (*Figure 1-1 on page 12*):

- **Program issue requests.** Issue requests submitted directly against a program provide a means of managing issues at the program level. These can span multiple request types. (For example, bugs and enhancements are both issues.) Each request type is processed along its assigned workflow, although the request types may have fields in common for tracking purposes.
- **Project issue requests.** Project issues introduce a framework for managing project issues. Issues can span multiple request types. These can span multiple request types. Each request type is processed along its own workflow, although the request types may have fields in common for tracking purposes.
- **Project risk requests.** Project risk requests provide a way to manage threats to a program. The process of gathering information about risks, including their probability of occurrence and potential impact, is streamlined. Each submitted risk request is processed along its assigned workflow.
- **Project scope change requests.** Project scope changes provide a way to ensure that the scope of a program and its individual projects stay manageable. The program manager can assess submitted scope change requests before rejecting them or incorporating them into the program or project scope.

Each submitted risk request is processed along its assigned workflow. Program and project scope can be controlled by ensuring that potential changes are clearly identified, aligned, and processed.

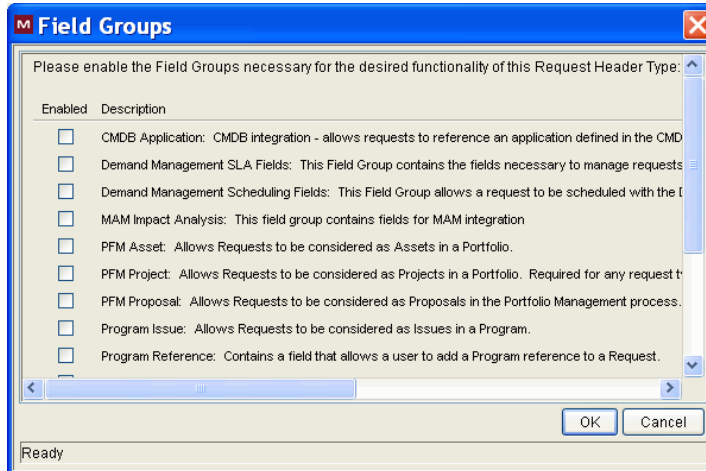
To use a given request type in Program Management, that request type must include a Program Management *field group*. A field group is a set of preconfigured fields delivered with Mercury IT Governance Center products. You can use these field groups to implement a solution quickly or to enable certain functions to act in concert in Mercury IT Governance Center.

For example, the Program Issue field group allows requests to be treated as issues in a program and activates consistent information tracking for these issues. This field group is associated with a request type (through the request header type) to enable basic Mercury Demand Management™ features such as request scheduling and analysis.

Figure 1-1 on page 12 shows the Field Groups window, which you use to select the Program Management field groups to associate with a request header

type. *Configuring Program Management Request Types and Workflows* on page 19 provides details on how to select the field groups.

Figure 1-1. Field Groups window



Each Program Management request type must be linked to its corresponding field group and to a specific Program Management workflow. Likewise, each Program Management workflow must be linked to a specific Program Management request type.

Table 1-1. Program Management request types and field groups

Request Type	Field Group	Fields
Program Issue	Program Issue: Allows requests to be treated as issues in a program.	<p>Summary</p> <ul style="list-style-type: none"> ■ Issue No. ■ Issue Status ■ Created By ■ Created On ■ Program ■ Priority ■ Assigned To ■ Description ■ Workflow ■ Contact Name ■ Request Group ■ Contact Phone ■ Department ■ Request Type ■ Contact Email ■ Application ■ Assigned Group ■ Sub-Type ■ Company ■ % Complete <p>Issue Details</p> <ul style="list-style-type: none"> ■ Date Identified ■ Due Date ■ Issue Type ■ Detailed Description ■ Proposed Solution ■ Business Function
Program Reference	Program Reference: Contains a field that lets users add a program reference to a request.	Program

Overview of Program Management Configuration

This section presents information about the high-level steps involved in configuring Program Management for your organization. [Chapter 2, *Configuring Program Management Request Types and Workflows*](#), on page 19 and [Chapter 4, *Configuring Security for Program Management*](#), on page 39 contain the detailed procedures you use to perform these steps.

Step One: Gather Information

The first step in configuring Program Management is to gather your program requirements. To deploy Program Management effectively, you must determine which program-related request types to use.

Different kinds of information are required to process each program-related request. For each field in the program-related request, collect the following information:

- **Field name.** Field names help ensure that the information captured in a request is correct and sufficient. Use the Request Type Workbench to set up a request so that it contains the fields required to gather the required information.
- **Information type.** What type of information do you need? Should the value of the field be entered as text, or will users select a value from a list? The field information type is governed by its validation, which defines the field component type, as well as what information users can enter in the field. For example, a field using a numeric text field validation accepts only numeric values.
- **Field behavior.** Configuring the behavior of a field helps to ensure that the correct information is collected. For example, to ensure that requests include specific information, you can make a field required.

You can set up fields that are populated automatically based on values in other fields. You can also set up fields that are read-only or hidden based on the access grants or the workflow step.



Note

For detailed information about how to configure request types, see the *Mercury Demand Management Configuration Guide*.

[Table 1-2 on page 15](#) lists the request types and workflows that Mercury supplies for all Program Management entities.

Table 1-2. Program Management request types and workflows

Request Type	Workflow	Definition
Program Issue	Issue Management Process	A request type used to enter issues directly against a program.
Project Issue	Issue Management Process	A request type used to enter issues into a project associated with a program.
Project Risk	Risk Management Process	A request type used to enter risk information into a project associated with a program.
Project Scope Change	Scope Change Request Process	A request type used to enter scope changes into a project associated with a program.

If these request types and workflows are adequate, no further requirements gathering is necessary.



Note

For information on how to add Program Management-related portlets to Dashboard pages, see the document *Configuring the Standard Interface*. For information on how to add the preconfigured Program Manager page to the Dashboard and modify it to suit your needs, see *Chapter 6, Program Manager Page* in the *Mercury Program Management User's Guide*.

Step Two: Configure Program Management Request Types

After you gather program requirements, configure the request header types associated with existing request types to include the required Program Management field group. For details, see *Configuring Program Management Request Types and Workflows* on page 19.



Note

Field groups are sets of preconfigured fields delivered with Mercury IT Governance Center. You can use them to implement a solution quickly or to enable certain functions simultaneously. For example, in Mercury Demand Management, the Demand Management Scheduling Fields field group enables consistent tracking of information across multiple request types.

Step Three: Configure Program Management Workflows

Configure the request header types associated with workflows to include the required Program Management field group. For details, see *Configuring Program Management Workflows* on page 24.

Step Four: Add Custom User Data Fields to Program Pages

You can define custom fields to capture additional information that standard fields on the View Program and Modify Program pages in the Dashboard do not capture. For information on how to create custom user data fields, see [Chapter 3, *Configuring User Data*, on page 27](#).

Step Five: Set Security for Program Management

Businesses often control access to certain information and business processes to protect sensitive information such as employee salaries, or to simplify business processes by hiding data that is irrelevant to specific users. Mercury IT Governance Center includes features to help control data and process security by letting you:

- Select program managers and set up security access grants for these resources
- Determine who is to report on issues, risks, and scope changes, reporter and set up security access grants for these resources
- Limit the data displayed in some fields or windows
- Specify who can view, create, edit, or process Mercury IT Governance Center entities such as requests, packages, projects, portfolios, and programs
- Specify who can view, create, or edit Mercury IT Governance Center configuration entities such as workflows, request types, object types, and security groups
- Specify who can change security settings

■ ■ Note

In addition to the security-related tasks described in this guide, the program manager can use the Control Access page to configure security for a specific program. For details on how to use the Control Access page, see the *Mercury Program Management User's Guide*.

The steps you perform to configure security groups and users for Program Management are described in [Chapter 4, *Configuring Security for Program Management*, on page 39](#).

■ ■ Note

Some business models require that specially designated security administrators set up user access grants and restrictions.

Related Documents

For additional useful information, see the following documents:

- *Mercury Program Management User's Guide*
- *Security Model Guide and Reference*
- *Mercury Demand Management Configuration Guide*
- *Mercury Deployment Management Configuration Guide*
- *Mercury-Supplied Entities Guide* (includes descriptions of all Mercury IT Governance Center portlets, request types, and workflows)

Chapter

2

Configuring Program Management Request Types and Workflows

In This Chapter:

- *Configuring Program Management Request Types*
 - *Configuring Program Management Workflows*
 - *Configuring the Cost Roll-Up Service Interval*
-

Configuring Program Management Request Types

Based on the needs of your organization, you choose and configure the request types to use in Program Management. To do this, you add field groups to the request header type for the request and attach a workflow to the request type. This section provides the steps you follow to perform these tasks.

For detailed information about requests, request types, request header types, and workflows, see the *Mercury Demand Management Configuration Guide*.



Note

To edit or create request types, you must have the Configuration license (system-level) and the Demand Mgmt: Edit Request Types access grants.

To configure a request type for Program Management:

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.

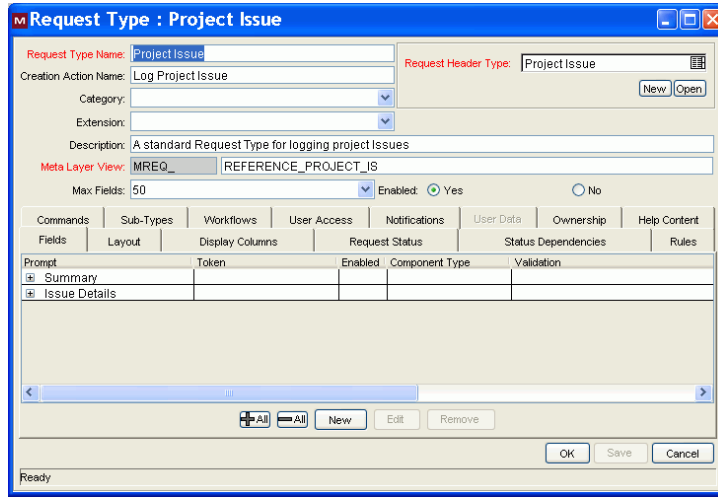
5. Open an existing request type or create a new request type.



Note

For information on how to create or open a request type, see the *Mercury Demand Management Configuration Guide*.

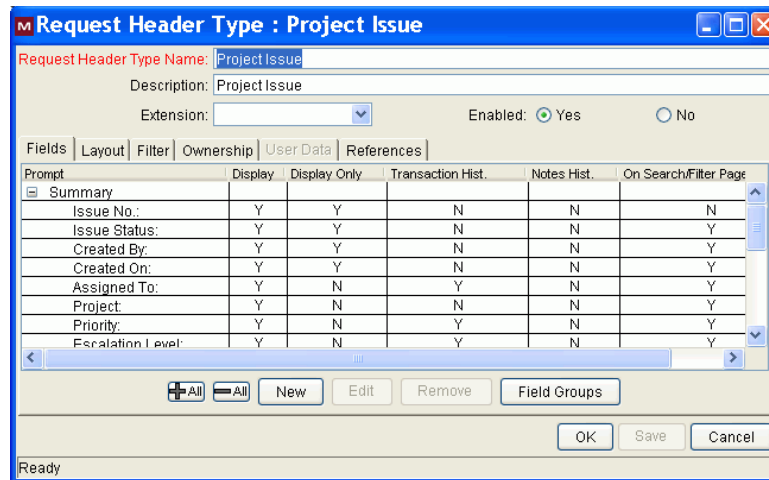
The Request Type: <Request Type Name> window opens.



6. To add a field group to the request header type:

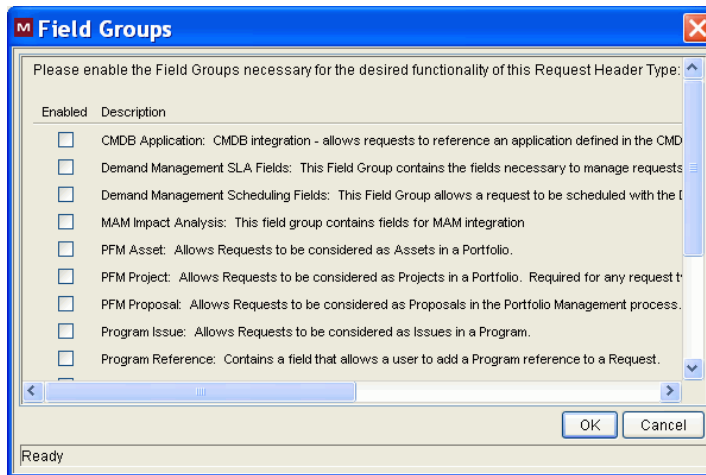
- a. In the top right of the Request Type window, under the **Request Header Type** box, click **Open**.

The Request Header Type <Request Header Type Name> window opens to the **Fields** tab.



- b. Click **Field Groups**.

The Field Groups window opens.



- c. To give the selected request header type the functionality you want it to have, select the **Enabled** checkbox for one or both Program Management field groups (**Program Issue** and **Program Reference**).



Note

Selecting the Program Issue field group allows requests to be treated as issues in a program and activates consistent information tracking for these issues. This field group is associated with a request type (through the request header type) to enable basic Mercury Demand Management features such as request scheduling and analysis.

Selecting the Program Reference field group adds a field to the request type so that users can add a program reference to requests.

- d. Click **OK**.
- e. In the Request Header Type window, click **OK**.
- f. From the Workbench shortcut bar, select **Request Types**.

The Request Type window opens.



Note

For a list of Program Management request types and the field groups associated with them, see [Table 1-1 on page 13](#).

7. To save the changes to the request type, click **Save**.
8. To add a workflow to the request type:

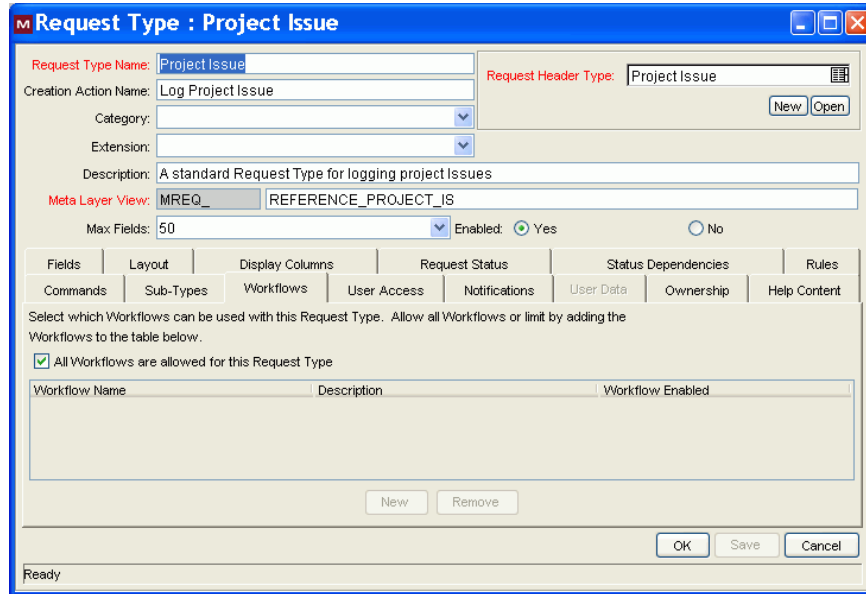


Note

For information about workflows and workflow steps, see the *Mercury Demand Management User's Guide*.

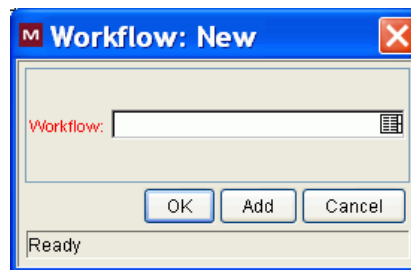
- a. In the Request Type window, click the **Workflows** tab.

By default, the **All Workflows are allowed for this Request Type** checkbox is selected.



- b. Clear the **All Workflows are allowed for this Request Type** checkbox.
- c. Click **New**.

The Workflow: New dialog box opens.



- d. In the **Workflow** box, select a workflow.
- e. Click **OK**.

The **Workflows** tab lists the selected workflow.

- f. To save the changes to the request type, click **Save**.
9. Click **OK**.

For detailed information on how to configure a request type, see the *Mercury Demand Management Configuration Guide*.

Configuring Program Management Workflows

Configuring Program Management Request Types on page 20 provided information on how to add a specific workflow to a specific Program Management request type. This section contains information on how to add a specific Program Management request type to a workflow. For information about workflows and workflow steps assigned to requests, see the *Mercury Demand Management User's Guide*.



Note

To edit request types, you must be assigned the Configuration system-level license and the Demand Mgmt: Edit Request Types access grant.

To add a request type to 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.

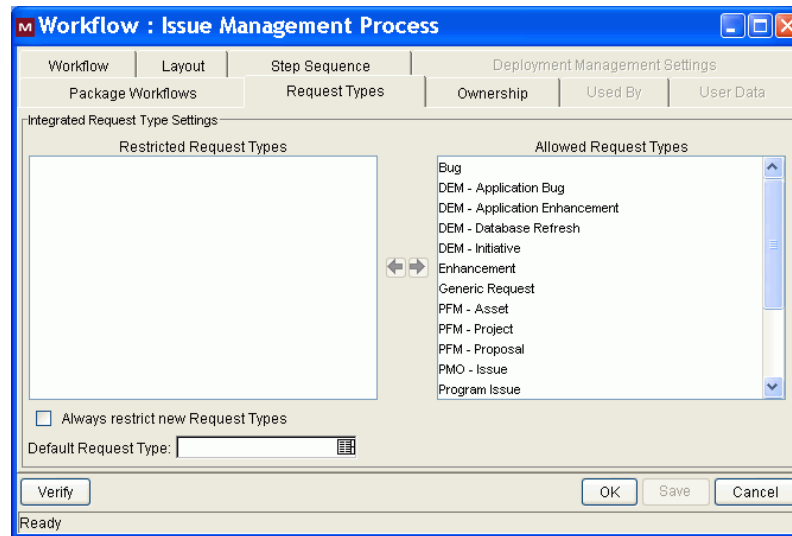
4. In the lower-right corner, click **List**.

The Workflow Workbench lists all workflow records.

5. In the **Workflow Name** column, double-click the record for the workflow that you added to the request type in [step 8 on page 22](#).

The Workflow: *<Workflow Name>* window opens.

6. Click the **Request Types** tab.



7. In the **Allowed Request Types** list, select all of the request types except the Program Management request type that you modified in *Configuring Program Management Request Types* on page 20.



Tip

To select adjacent and nonadjacent list items, use the **Shift** and **Ctrl** keys, respectively.

8. To move the selected request types to the **Restricted Request Types** list, click the left-pointing arrow.
9. Click **OK**.

For more information about workflows, see the *Mercury Demand Management Configuration Guide*.

Configuring the Cost Roll-Up Service Interval

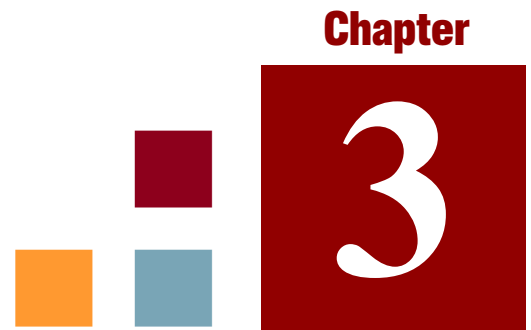
As changes are made to cost information for projects, Mercury IT Governance Center does not automatically recalculate the cost data in real time. This means that, at any given time, the rolled-up cost information displayed for a program may be out of date.

Costing information is recalculated as part of a cost rollup service that runs at a configurable interval. If a user completes an action that requires that costs be recalculated, Mercury IT Governance Center keeps a record of the updated entity to signify that a cost calculation and rollup is pending. When the cost roll-up service runs, the pending entities are loaded and cost calculations are performed and rolled up.

The server configuration parameter `com.kintana.core.server.ENABLE_COST_ROLLUP_SERVICE` determines whether the cost roll-up service is enabled. The service is enabled by default.

You can control the frequency with which the cost roll-up service runs by setting the value of the `com.kintana.core.server.COST_ROLLUP_INTERVAL` server configuration parameter. By default, the service runs every 300 seconds.

For information on how to change the value of the `COST_ROLLUP_INTERVAL` server configuration parameter, see *Appendix A* in the *System Administration Guide and Reference*.



Chapter
3

Configuring User Data

In This Chapter:

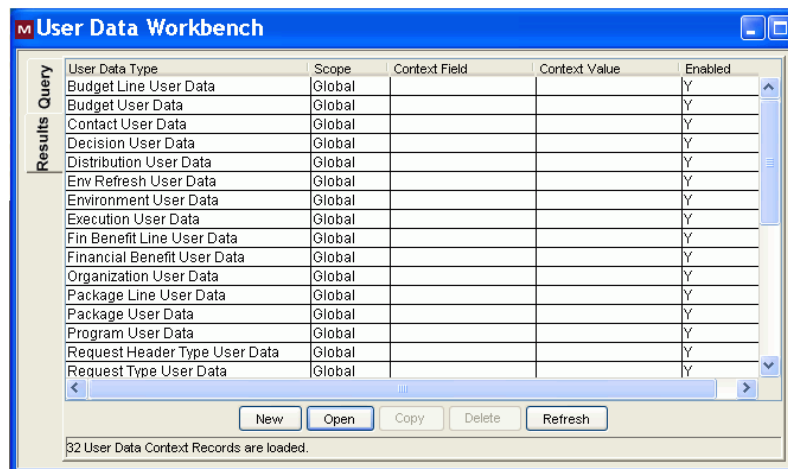
- *Overview of User Data*
 - *Referring to User Data*
 - *Adding Custom User Fields to Programs*
 - *Configuring the Default Value for a Custom User Field*
 - *Configuring Default Security for a Custom User Field*
 - *More Information About Configuring User Data*
-

Overview of User Data

Program pages in the Mercury IT Governance Dashboard™ display a set of standard fields for collecting and displaying program information. While these fields are sufficient for day-to-day processing, you can use *user data fields* to capture additional information specific to your organization. If you want to include additional fields on the View Program and Modify Program pages in the Dashboard, you can define them in the User Data Workbench.

You configure user data types from the User Data Workbench in the User Data Context window. *Figure 3-1* shows the **Results** tab in the User Data Workbench, which lists the available user data types.

Figure 3-1. User data types listed in the User Data Workbench



User Data Type	Scope	Context Field	Context Value	Enabled
Budget Line User Data	Global			Y
Budget User Data	Global			Y
Contact User Data	Global			Y
Decision User Data	Global			Y
Distribution User Data	Global			Y
Env Refresh User Data	Global			Y
Environment User Data	Global			Y
Execution User Data	Global			Y
Fin Benefit Line User Data	Global			Y
Financial Benefit User Data	Global			Y
Organization User Data	Global			Y
Package Line User Data	Global			Y
Package User Data	Global			Y
Program User Data	Global			Y
Request Header Type User Data	Global			Y
Request Type User Data	Global			Y

32 User Data Context Records are loaded.

Each user data type consists of the following components:

- The **User Data Type** column lists the user data types that Mercury IT Governance Center supplies out of the box. For programs, Mercury IT Governance Center supplies the *Program User Data* user data entity.



Note

Although you cannot create new user data types, you can define fields for an existing user data type.

- The **Scope** column indicates the scope of the user data type field. The scope value is either *global* or *context*. If the scope is global, the **User Data** tab for every designated entity contains the defined field. If the scope value is context (a context-sensitive user data type field), the defined user data field is displayed only on the **User Data** tab of entities with specific context fields and context value definitions. The scope of the Program User Data user data type is global.

- The **Context Field** column displays the label of context-sensitive fields. It is not enabled for the Program User Data type.
- The **Context Value** column lists the value (context) for context-sensitive fields. It is not enabled for the Program User Data type.

You can define up to 20 user data type fields for display on the your View Program and Modify Program pages in the Dashboard. You can configure the major attributes of each field, including its graphical presentation, validation method, and whether it is required.

Referring to User Data

After you create a user data field, you can refer to it from other parts of the product by its token name, preceded by the entity abbreviation and the user data (UD) qualifier. The token format is `[PREFIX.UD.USER_DATA_TOKEN]`. For example, if you defined a field for package user data with the token `GAP_NUMBER`, in the default format, the token would be `[PKG.UD.GAP_NUMBER]`.

Adding Custom User Fields to Programs

This section presents the steps you perform to add a custom field to your program pages:

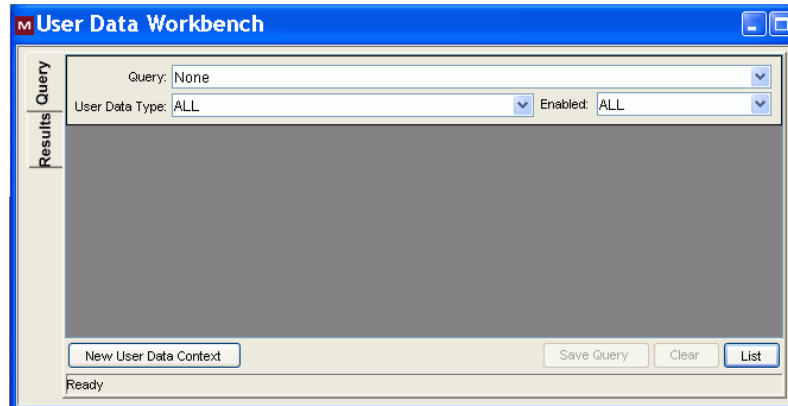
To add a custom user field to program pages:

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 > User Data**.

The User Data Workbench opens.

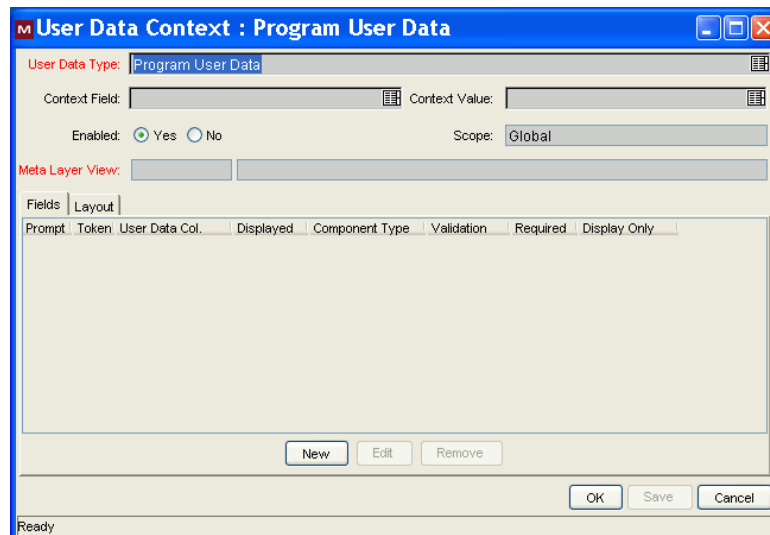


4. Click **List**.

The **Results** tab lists the available user data types.

5. In the **User Data Type** column, double-click **Program User Data**.

The User Data Context: Program User Data window opens to the **Fields** tab.

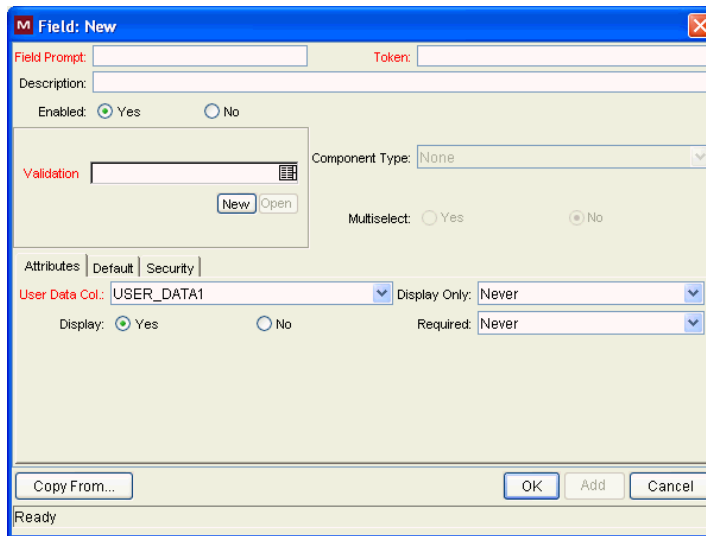


6. Click **New**.

A message warns you to exercise caution in modifying fields and prompts you to indicate whether you want to continue.

7. Click **Yes**.

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



8. Enter the following information:

- a. In the **Field Prompt** box, type the label to display for the new field.
- b. In the **Token** box, type an uppercase text string to use to identify this field.

The token name must be unique to the specific user data. An example token name is `ASSIGNED_TO_USER_ID`.

- c. In the **Description** box, you can enter text that describes what the field captures and how it is to be used.
- d. To enable the new field, leave **Enabled** selected.
- e. In the **Validation** box, enter the validation logic to use to determine the valid values for the field.

This can be a list of user-defined values, a rule that the result must be a number, and so on.

The **Component Type** field indicates the field type (list, free form text field, and so on). This read-only field is derived from the validation you selected.

- f. If the field lists selectable items, and you want users to be able to select more than one of these, select **Multiselect**.

If you select **Multiselect**, the Workbench displays a dialog box that lists limitations imposed on multiselect user fields.

g. If you selected **Multiselect**, make a note of the limitations, and then click **Yes**.

9. On the **Attributes** tab, enter the following information:

a. In the **User Data Col** list, select the internal column in which the field value is to be stored.

These values are stored in the corresponding column in the table for programs. You can store information in up to 20 columns, which means that you can create up to 20 custom fields for programs. No two fields in user data can use the same column.

b. To make the new field read-only at all times, in the **Display Only** list, select **Always**. To make the field editable at all times, select **Never**.

c. To make the field visible to users, next to **Display**, leave **Yes** selected. To hide the field, select **No**.

d. To make the field required (the user must specify a value) at all times, in the **Required** list, select **Always**. To make the field optional at all times, select **Never**.

At this point you can continue to configure the new field, save your changes and create another field, or save your changes and close the Field window.

10. Do one of the following:

■ Continue to configure the new field.

For information on how to further configure the new field, see [Configuring the Default Value for a Custom User Field on page 33](#) and [Configuring Default Security for a Custom User Field on page 34](#).

■ To save your changes and create another field, click **Apply**.

The Field window clears so that you can create another new field.

■ To save your changes and close the Field window, click **OK**, and then, in the User Data Context window, click **OK**.

Configuring the Default Value for a Custom User Field

To configure the default value for a custom user field:

1. If the Field: *<Field Name>* window is open, skip to [step 8 on page 34](#), otherwise, continue to [step 2](#).

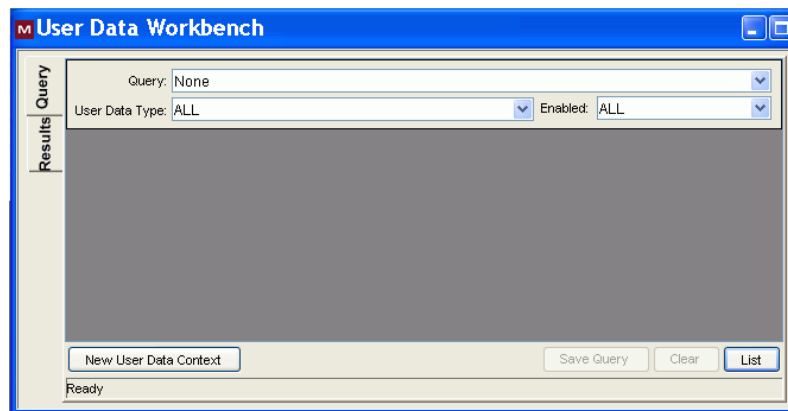
2. Log on to Mercury IT Governance Center.

3. From the menu bar, select **Administration > Open Workbench**.

The Workbench opens.

4. From the shortcut bar, select **Configuration > User Data**.

The User Data Workbench opens.



5. Click **List**.

The **Results** tab lists the available user data types.

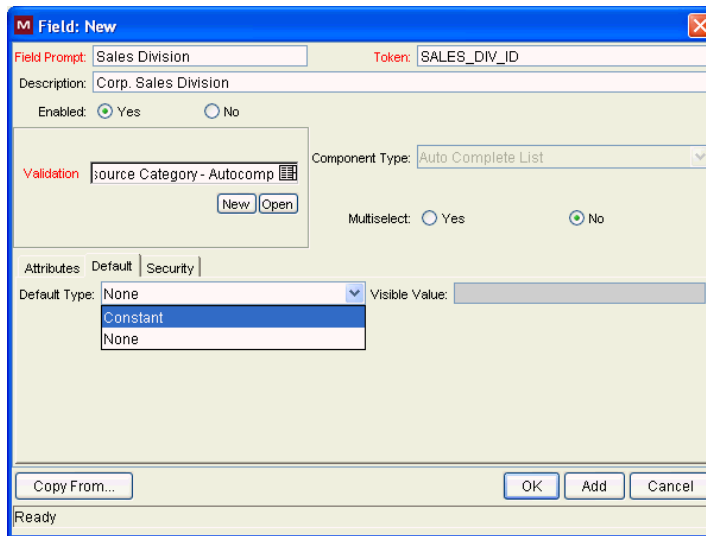
6. In the **User Data Type** column, double-click **Program User Data**.

The User Data Context: Program User Data window opens to the **Fields** tab.

7. On the **Fields** tab, double-click the row that displays the field for which you want to configure a default value(s).

The Field: *<Field Name>* window opens to the **Attributes** tab.

8. Click the **Default** tab.



9. Enter the following information:
 - a. To indicate that the field is to have a default value, in the **Default Type** list, do one of the following:
 - To specify that the field default is to be a constant value, select **Constant**.
 - To specify that the field default is to have no default, select **None**.
 - b. If you specified a constant default type, then in the **Visible Value** list, select the constant value.
10. Do one of the following:
 - Continue to configure the new custom field.
 - To save the custom field and close the Field window, click **OK**, and then, in the User Data Context window, click **OK**.

Configuring Default Security for a Custom User Field

This section provides the steps used to configure the default security setting for a custom field. Keep in mind that status dependencies and field-level dependencies can override these settings.

To configure the default security settings for a customer user field:

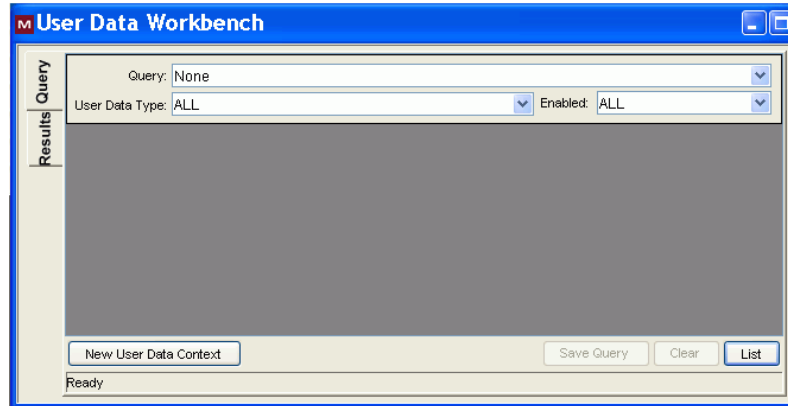
1. If the Field window is open, skip to [step 8 on page 36](#), otherwise, continue to [step 2](#).

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

The Workbench opens.

4. From the shortcut bar, select **Configuration > User Data**.

The User Data Workbench opens.



5. Click **List**.

The **Results** tab lists the available user data types.

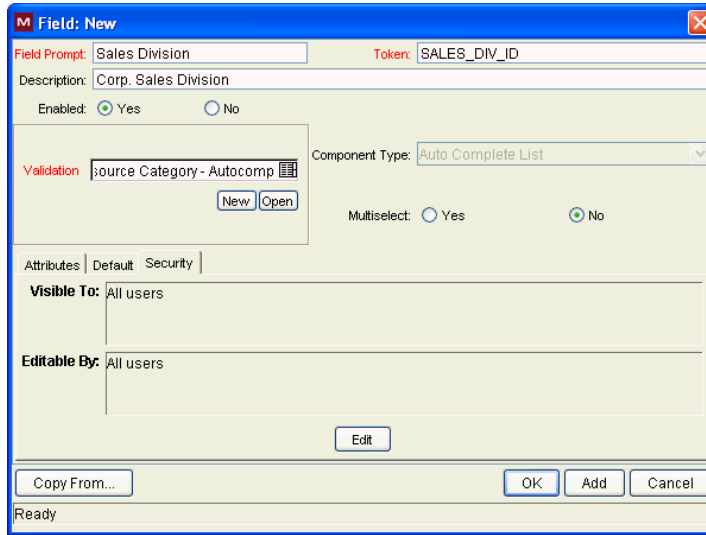
6. In the **User Data Type** column, double-click **Program User Data**.

The User Data Context: Program User Data window opens to the **Fields** tab.

7. On the **Fields** tab, double-click the row that displays the field for which you want to configure default security settings.

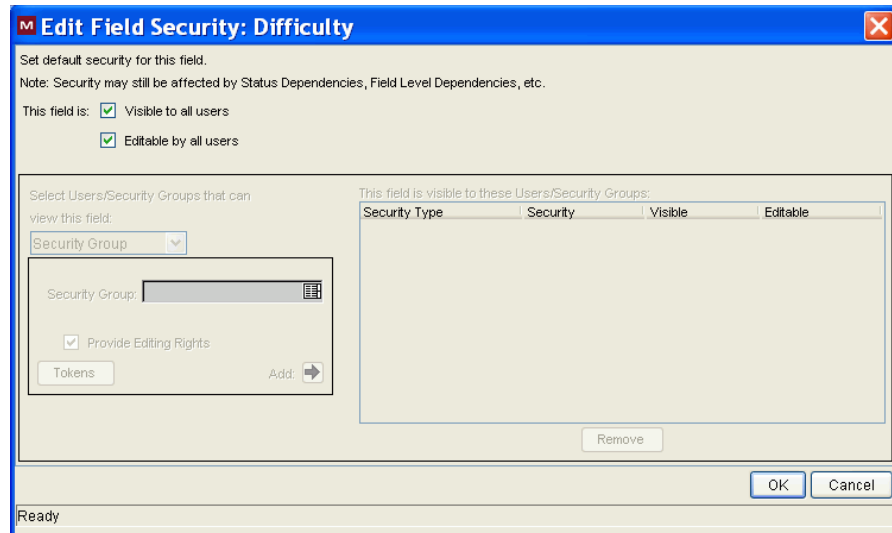
The Field window opens to the **Attributes** tab.

8. Click the **Security** tab.



- a. Click **Edit**.

The Edit Field Security window opens.



9. To specify that only certain users or groups be able to view and or edit the custom field:
 - a. Next to **This field is**, clear the **Visible to all users** and **Editable by all users** checkboxes.

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

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

Your selection determines the label displayed for the auto-complete field below the list.

c. Use the auto-complete field to select the security groups, users, standard tokens, or user-defined tokens that you want to be able to view this field.

d. To give the selected items the ability to edit the field, leave the **Provide Editing Rights** checkbox selected. To make the field read-only for your selection(s), clear the checkbox.

e. Click **Add**.

The table on the right lists your selection(s).

f. Repeat [step c](#) through [step e](#) to configure field visibility for additional users and groups.

In the table on the right, the **Visible** and **Editable** checkboxes are selected by default for all of the selected users and group.

g. In the table on the right, clear the **Visible** checkbox for the users and groups from which you want the field to be hidden.

h. In the table on the right, clear the **Editable** checkbox for the users and groups for which you want the custom field to be read-only.

10. Click **OK**.

11. In the Field window, click **OK**.

12. In the User Data Context window, click **OK**.

More Information About Configuring User Data

For information about the following topics, see the *Mercury Deployment Management Configuration Guide*:

- Copying field definitions
- Configuring user data field dependencies (detailed steps)
- Editing user data fields
- Removing fields
- Configuring user data layout

Chapter

4

Configuring Security for Program Management

In This Chapter:

- *Program Management Security*
 - *Required Licenses*
 - *Program Management*
 - *Demand Management*
 - *Project Management*
 - *Access Grants*
 - *Security Groups*
 - *Creating a Security Group and Assigning It Access Grants*
 - *Configuring Program Management Users*
 - *Associating Security Groups with Workflows*
-

Program Management Security

This chapter describes how to use licenses, access grants and security groups to give users access to Program Management information and processes. For a detailed description of Mercury IT Governance Center security, see the *Security Model Guide and Reference*.

Table 4-1 lists the settings you use to control the data and process security in Mercury IT Governance Center.

Table 4-1. Security features

Security Feature	Definition
Licenses	Each user is assigned one or more licenses that determine which set of Mercury IT Governance Center product-related screens and functions available to that user. Use the licenses in conjunction with access grants to give users access to specific fields and functions.
Access grants	Linked to users through security groups, access grants determine the windows and functions in which users can view or edit information or perform actions. Access grants also provide different levels of control over some entities and fields.
Entity-level restrictions	Use entity settings to: <ul style="list-style-type: none"> ■ Control who can create, edit, process, and delete Mercury IT Governance Center entities such as requests, packages, and projects. ■ Control which request types and object types can be used with certain workflows. You can set up these restrictions in the configuration entities (workflows, request types, and object types).
Field-level restrictions	For each custom field that you define in Mercury IT Governance Center, you can specify the conditions under which it is visible (or not) and editable (or read-only). You can also specify the users who can view or edit some fields.
Configuration-level restrictions	Use ownership groups settings to specify who can modify configuration entities. For example, to ensure that only designated users can change your Mercury IT Governance Center–controlled processes, select the users who can edit an existing workflow.

Security Groups on page 42 of this chapter provides the steps to perform to configure security groups and users for Program Management.

Required Licenses

To use Program Management, you must have the following application licenses:

- Program Management
- Demand Management
- Project Management

For information about the system-level licenses required to configure security in Mercury IT Governance Center, see the *Security Model Guide and Reference*.

Program Management

The Program Management license provides access to basic Program Management functionality and to configuration of general Program Management settings. It must be used in conjunction with Demand Management and Project Management licenses.

Demand Management

The Demand Management license provides access to all Demand Management functionality.

Project Management

The Project Management license provides access to all Project, Resource, and Financial Management functionality available through the Workbench, as well as access to advanced Mercury IT Governance Center Dashboard functions.

Access Grants

Access grants provide users (who have the required application licenses) with the permission required to access specific entities or perform specific functions within Mercury IT Governance Center.

The Program Management access grants are:

- **PMO: Edit Programs.** This access grant allows a user to modify all programs on which he is the assigned the program manager.
- **PMO: Edit All Programs.** This access grant allows users to create and modify any program.
- **PMO: View Programs.** This access grant allows users to view program definitions.

Security Groups

Using security groups in Program Management involves associating them with process (workflow) steps and potentially restricting user access to the Program Management entities—projects, requests, and budgets.

This section provides detailed instruction on how to create security groups and assign them access grants, add users to security groups, and associate the security groups with workflows (business processes).

Creating a Security Group and Assigning It Access Grants

A security group is essentially a collection of access grants. After you create and enable a security group, you can assign users to it. A user assigned to a security group assumes the access grants assigned to that security group.

Mercury IT Governance Center includes one default security group for Program Management. This security group, which is named ITG Program Manager, has all Program Management access grants assigned to it. Users that you add to this group can access and edit information for all programs.

You can define additional Program Management security groups to suit your needs.



To add access grants to a security group, you must be assigned the User Administration system-level license.

To create a security group and assign access grants to it:

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 > Security Groups**.

The Security Group Workbench opens.

4. At the lower-left part of the window, click **New**.

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

5. In the **Name** box, type a name for the security group.
6. Next to **Enabled**, click **Yes**.
7. Click **Save**.
8. Click the **Access Grants** tab.

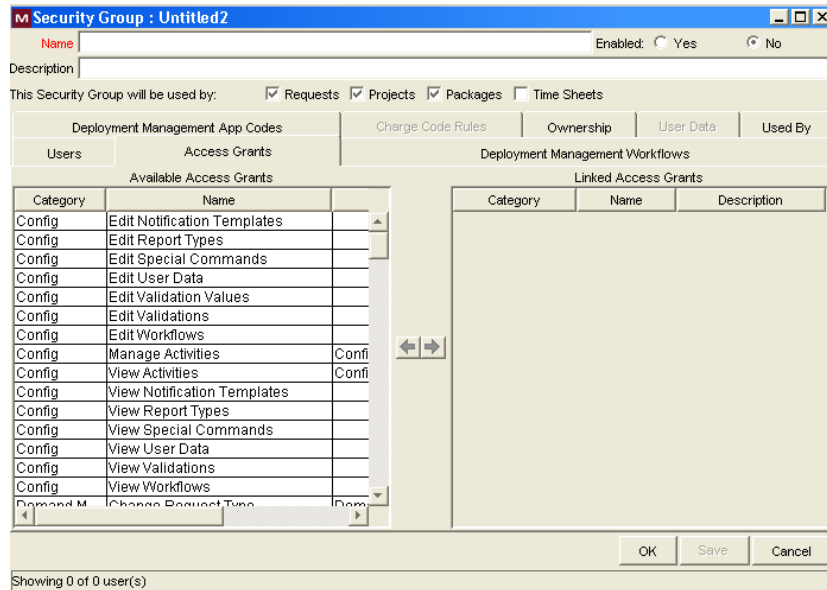
The **Available Access Grants** table lists all of the access grants that you can assign to a security group. The **Category** column lists the Mercury IT Governance Center functional area with which each grant is associated.

9. To assign access grants to your new security group:
 - a. In the **Available Access Grants** table, select one or more access grants.



You can use the **Ctrl** and **Shift** keys to select adjacent and nonadjacent items in the list.

b. Click the right-pointing arrow.



The **Linked Access Grants** table on the right lists the selected access grants, which are now associated with your security group.

10. To save the settings, click **OK**.

The Security Group Workbench lists the security group you created.

Table 4-2 lists details for the security group setup for two sets of (example) users who have different Program Management access grants assigned to them.

Table 4-2. Program Management security group scenario

Security Group	Category: Access Grant	Definition
Program Manager	<ul style="list-style-type: none"> ■ PMO: Edit Programs ■ PMO: Edit All Programs ■ PMO: View Programs 	Corporate program managers who must have full access to programs.
Admin Program Mgmt	<ul style="list-style-type: none"> ■ PMO: View Programs 	Line managers who only need to view programs.

Configuring Program Management Users

To assign access grants to a user, you add the user to a security group.

■ ■ Note

To create a user, you must have the User Administration system-level license. For information on system-level licenses, see the *Security Model Guide and Reference*.

To assign a new user to one or more security groups:

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

The Workbench opens.

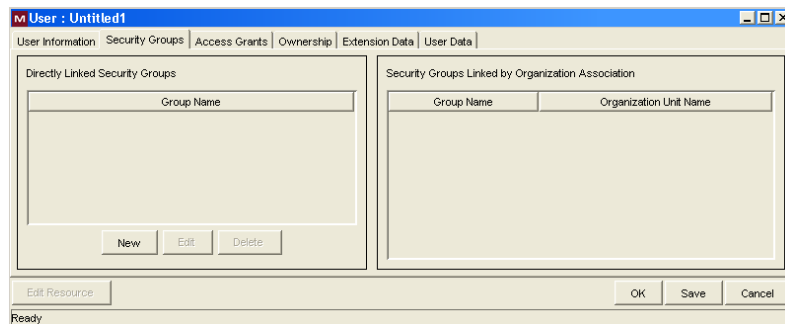
3. On the shortcut bar, select **Sys Admin > Users**.

The User Workbench opens.

4. Click **New User**.

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

5. Enter the required information (fields with labels displayed in red text) for the new user, and then click the **Security Groups** tab.



6. In the **Directly Linked Security Groups** box, click **New**.

The Security Groups dialog box opens.

7. In the **Security Groups** field, click the auto-complete button, and then select the security groups.
8. Click **OK**.
9. To save your changes, click **OK**.

Table 4-3 lists the licenses and security groups required for two sets of users who have different Program Management access grants assigned.

Table 4-3. Program Management security group and license scenario

Security Group	Licenses	Definition
Program Manager	<ul style="list-style-type: none"> ■ Program Management ■ Demand Management ■ Project Management 	Corporate program managers who require full access to programs.
Admin Program Mgmt	<ul style="list-style-type: none"> ■ Program Management ■ Demand Management ■ Project Management 	Line managers who only need to view programs.

Associating Security Groups with Workflows

Workflows represent business processes and are used to map business rules and processes to your organization. Each workflow consists of a series of workflow steps. Linked together, these workflow steps form the workflow. With the required access grants, you can edit workflows to meet your business requirements.



Note

To edit workflows, you must have the Configuration system-level license.

You can configure each workflow step so that only security groups or individual users that you specify can process it.

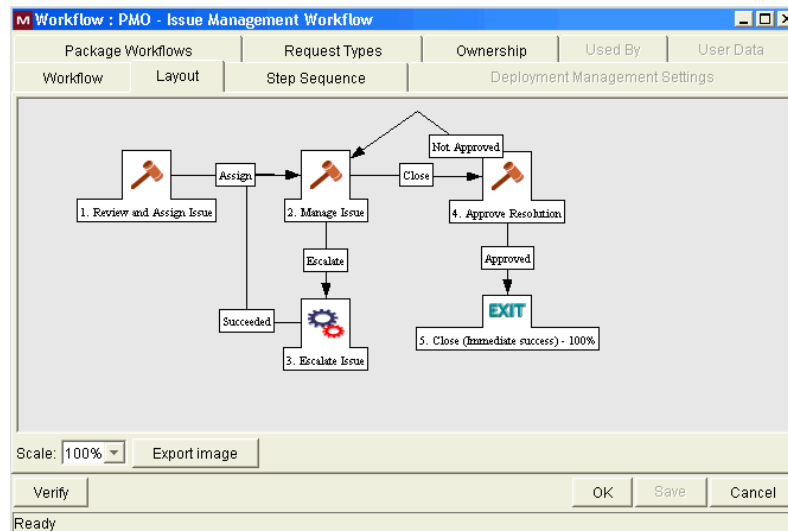
To configure an existing workflow step for a security group:

1. Open the Workbench.
2. From the Workbench shortcut bar, select **Configuration > Workflows**.

The Workflow Workbench opens.

3. Open an existing workflow.

The Workflow window opens to the **Layout** tab, which you use to configure workflow steps.



4. On the **Layout** tab, double-click a numbered workflow step.

The Workflow Step window opens to the **Properties** tab, which is used to specify general information about the workflow step.

5. Click the **Security** tab.



Note

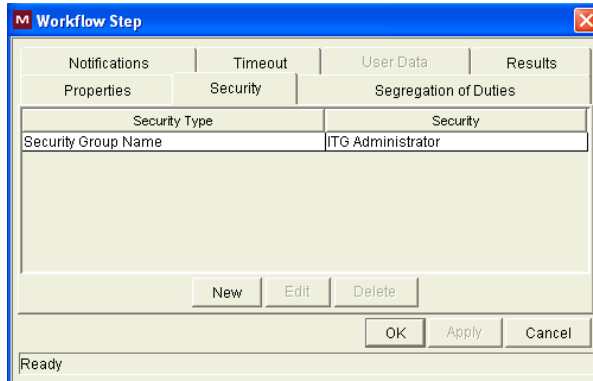
You use the **Security** tab to assign security groups and individual users to the workflow step. After you assign a security group to a workflow step, only a member of that security group can act on that step.

6. Click **New**.

The Workflow Step Security window opens.

7. In the **Security Group** box, use the auto-complete list tool to open the Validate window and select the security group or groups.
8. Click **OK**.

9. In the Workflow Step window, click **OK**.



The **Security** tab lists the security groups added to the workflow step.

10. Click **OK**.

11. To save your changes to the workflow, in the Workflow: *<Workflow Name>* window, click **OK**.

For more information on configuring workflow steps, see the *Mercury Demand Management Configuration Guide*.

A

access grants 42
 assigning to security groups 43

C

configuring
 cost roll-up service 26
 default security for custom fields 34
 Program Management 14
 Program Management workflows 15
 request types 20
 request types to use in Program Management 20
 security 40
 workflows 24
cost roll-up service
 configuring 26
COST_ROLLUP_INTERVAL parameter 26
custom fields
 configuring default security for 34
custom user fields
 configuring default values 33

E

ENABLE_COST_ROLLUP_SERVICE
 parameter 26

F

field groups
 adding to a request header type 20

I

issue requests
 programs 11
 projects within programs 11

P

Program Management
 configuring 14
 configuring request types 15, 20
 configuring workflows in 15
 creating security groups for 43
 setting security for 16
 workflows 24
programs
 adding user fields 29
 issues 11

R

related documents 17
request types
 configuring in Program Management 15
request types configuring 20

risk requests 11

S

scope change requests 11

security

- access grants 42
- configuring default for custom fields 34
- security groups 42
- security groups and workflows 46
- setting for Program Management 16
- user configuration 45

security groups

- adding users to 45
- assigning access grants to 43
- creating for Program Management 43

U

user data

- configuring default values for a custom user field 33
- overview 28
- referring to 29

W

workflows

- associating security groups with 46
- configuration 24
- configuring for Program Management 15
- Program Management 24