OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

Platform Administration

MERCURY™
BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

Platform Administration

Version 6.2

Document Release Date: July 18, 2006

MERCURY™

Mercury Business Availability Center, Version 6.2
Platform Administration

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

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

If you have any comments or suggestions regarding this document, please send them by e-mail to documentation@mercury.com.

AMLIB_PLATAD6.2/01

Table of Contents

PART I: SETUP AND MAINTENANCE

PART II: DATA COLLECTION

PART III: ALERTS MANAGEMENT

PART IV: SCHEDULED REPORTS

PART V: USERS AND PERMISSIONS

PART VI: PERSONAL SETTINGS

PART VII: REPORT ADMINISTRATION

PART VIII: AUTHENTICATION

Welcome to Platform Administration

This guide provides detailed instructions on how to configure and administer the Mercury Business Availability Center platform.

How This Guide Is Organized

The guide contains the following parts:

Part I Setup and Maintenance

Describes how to download components, manage licenses, upgrade the platform and Service Level Management data, administrate the profile and management databases, enable data purging, configure the infrastructure settings, view the audit log, and configure MMS Import.

Part II Data Collection

Describes how to configure the settings and resources related to data collection, including upgrading and removing data collectors; scheduling downtime and events; filtering and removing transactions, locations, and groups; setting the order for transactions to run; adding and updating definitions of user-defined samples; setting filters for report data; and recording scripts for Client Monitors.

Part III Alerts Management

Describes the process of creating and maintaining alerts, recipients, and alert dependencies.

Part IV Scheduled Reports

Describes how to define and schedule user-defined reports.

Part V Users and Permissions

Describes how to create and manage users and user groups, as well as the permissions that apply to them across the platform's resources.

Part VI Personal Settings

Describes the customizations to set per user, including refresh interval, time zone, menus, and default pages.

Part VII Report Administration

Describes how to generate a report automatically and how to view, in a reports log, the errors that occurred when generating a report and all activities carried out on a report: creating a new report, generating a report, modifying the report filter(s), drilling down in reports, and so forth.

Part VIII Authentication

Describes how to configure Mercury Business Availability Center to work with authentication strategies.

Who Should Read This Guide

This guide is intended for the following users of Mercury Business Availability Center:

- Mercury Business Availability Center administrators
- Mercury Business Availability Center platform administrators

Readers of this guide should be knowledgeable about enterprise system administration and highly knowledgeable about Mercury Business Availability Center.

Getting More Information

For information on using and updating the Mercury Application Management Documentation Library, reference information on additional documentation resources, typographical conventions used in the Documentation Library, and quick reference information on deploying, administering, and using Mercury Business Availability Center, refer to *Getting Started with Mercury Business Availability Center*.

Part I

Setup and Maintenance

1

Downloads and Licenses

Once the servers for Mercury Business Availability Center are installed, there are several components that must be downloaded. These components include tools for monitoring your enterprise and recording business processes. Mercury Business Availability Center also includes a flexible licensing feature enabling you to update your own license information.

Downloads

You download components from the Downloads page, accessed from the Setup and Maintenance tab in Platform Administration. To view and download components from the Downloads page, after installing Mercury Business Availability Center, you must install the data collector setup file. For details, see “Installing Components Setup Files for a Windows Platform” or “Installing Components Setup Files for a Solaris Platform” in *Deploying Servers*.

Note: If there is a component you want to download that does not appear on the Downloads page because it was not selected during data collector setup file installation, you can access the setup file for any available download on the Mercury Business Availability Center Data Collector CD. For details, see "Installing Components Setup Files for a Windows Platform" or "Installing Components Setup Files for a Solaris Platform" in *Deploying Servers*.

Depending on the options selected during data collector setup file installation, any of the following components may be available for download:

- Mercury Business Process Monitor for Windows 2000/2003/XP, or Solaris
- Discovery Probe for Windows 2000/2003/XP
- Mercury SiteScope for Windows 2000/2003/XP, or Solaris
- Mercury SiteScope Service Pack for Windows 2000/2003/XP, or Solaris (to use SiteScope with Mercury Business Availability Center version 6.2, you must download SiteScope version 8.2)
- Mercury Virtual User Generator
- Mercury Client Monitor
- Mercury Real User Monitor Engine for Windows or Solaris
- Mercury Real User Monitor Probe
- Mercury Dashboard Ticker (for details about this application, see "Dashboard Ticker" in *Using Dashboard*)

To download and install a component:

1. Select **Setup and Maintenance** > **Downloads** from the Platform Administration page in the Administration Console. The Downloads page opens.
2. Click the component you want to download.
3. Save the component's setup file to your computer.

4 To install the component, double-click its setup file.

- For details on installing Mercury Business Process Monitor for Windows 2000/2003/XP, or Solaris, see "About Business Process Monitor Deployment" in *Business Process Monitor Administration*.
- For details on installing Mercury SiteScope for Windows 2000/2003/XP, or Solaris, see "Introducing and Deploying SiteScope" in *SiteScope Administration*.
- For details on installing Mercury Virtual User Generator, start the installation process and follow the on-screen instructions.
- For details on installing Client Monitor, see "Installing Client Monitor" in *Client Monitor Administration*.
- For details on installing Mercury Real User Monitor Engine, see "Installing the Real User Monitor Engine" in *Real User Monitor Administration*.
- For details on installing Mercury Real User Monitor Probes, see "Installing the Real User Monitor Probe" in *Real User Monitor Administration*.
- For details on installing Mercury Dashboard Ticker start the installation process and follow the on-screen instructions (for details, see "Dashboard Ticker" in *Using Dashboard*).

License Management

Note to Mercury Managed Services customers: Mercury Operations administers these pages and the interface is hidden from your view.

To run monitors and transactions, as well as use Service Level Management, J2EE, .Net, Business Availability Center for Siebel, and Client Monitor, you must have a valid license key.

The Mercury Business Availability Center license enables you to simultaneously run a predetermined number of monitors and transactions for a specified period of time. The number of monitors and transactions that you can run simultaneously and the license key expiration date depend on the license your organization has purchased from Mercury Interactive. You provide the license key during installation.

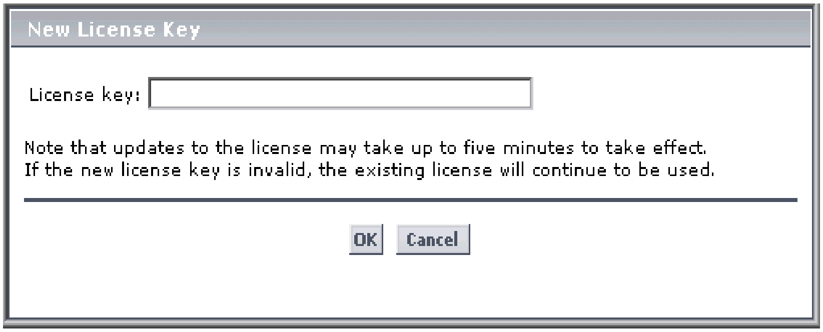
Mercury Business Availability Center applications that require an additional license are not displayed in the About Mercury Business Availability Center dialog box unless a valid license exists.

You can review the status of your maintenance number and license key by selecting **Help** > **About Mercury Business Availability Center**. The About Mercury Business Availability Center dialog box opens and displays your current license information. You can update your maintenance number and license key in the License Management page available from the Setup and Maintenance tab in Platform Administration.

Note: Mercury Business Availability Center posts a license expiration reminder on the login page of the Web site seven days before license expiration.

To update your license key or maintenance number in Windows:

1. In Platform Administration, select **Setup and Maintenance** > **License Management** to open the License Management page.
2. Click **New Maintenance Number** or **New License Key**. The relevant dialog box opens.



New License Key

License key:

Note that updates to the license may take up to five minutes to take effect.
If the new license key is invalid, the existing license will continue to be used.

3. Type the new or updated number for the license key or the maintenance number in the appropriate box.
4. Click **OK**.

To update your license key or maintenance number in Solaris:

Note: The initial license key and maintenance number are installed during the installation process. Do not use Platform Administration to install them.

---

1. Log in to Solaris as user **root**.
2. Go to directory <**Mercury Business Availability Center root directory**>**/scripts**.
3. Run the script **create_license.sh** with the parameters <**Management database user name**> <**Management database password**> <**database tns name**>. For example,

```
./create_license.sh TopazMng11 topaz spenser
```

To view your current license information in License Management:

In Platform Administration, select **Setup and Maintenance** > **License Management** to open the License Management page.

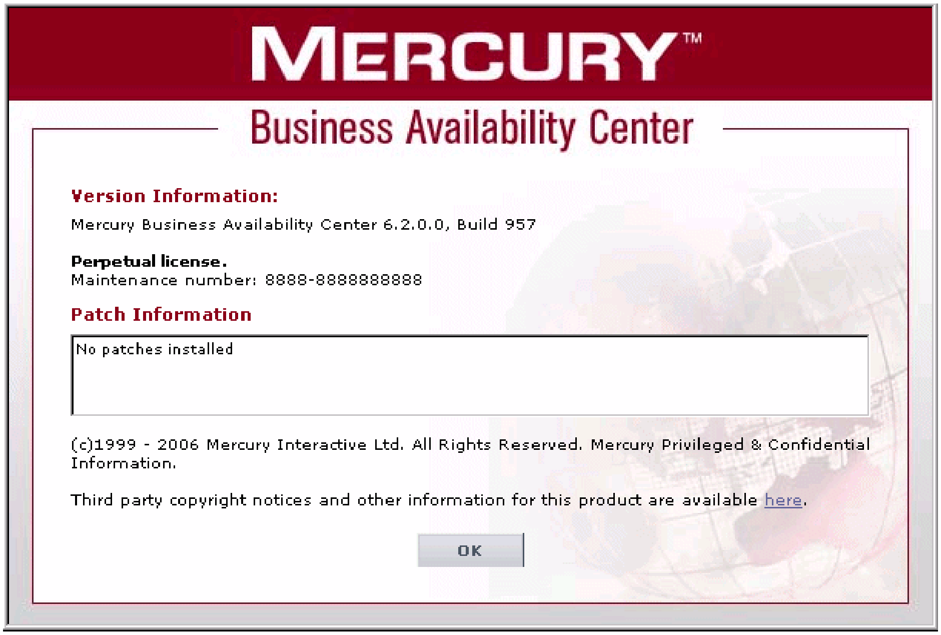
The following information is displayed:

- General License Properties area including:
  - current license key
  - current maintenance number
  - license type
  - license expiration date
- Business Process Monitor and Client Monitor areas both include:
  - maximum number of transactions allowed to run simultaneously under the current license key
  - number of transactions currently running in all profiles
  - total number of transactions currently in the database
- Applications area including:

- validity of Dashboard license
- validity of Service Level Management license
- validity of End User Management license
- validity of Real User Monitor license
- validity of System Availability Management license
- validity of Diagnostics license
- validity of Business Availability Center for Citrix license
- validity of Business Availability Center for SAP license
- validity of Automatic Discovery license

To open the About Mercury Business Availability Center dialog box:

Click **Help** > **About Mercury Business Availability Center**.



Version Information:

Mercury Business Availability Center 6.2.0.0, Build 957

Perpetual license.
Maintenance number: 8888-8888888888

Patch Information

No patches installed

(c)1999 - 2006 Mercury Interactive Ltd. All Rights Reserved. Mercury Privileged & Confidential Information.

Third party copyright notices and other information for this product are available here.

2

Upgrading Mercury Business Availability Center

Upgrade Documentation

Note to Mercury Managed Services customers: Mercury Operations administers these pages and the interface is hidden from your view.

For more information on the entire upgrade procedure, refer to the upgrade guide relevant to your upgrade path. The following upgrade guides are available:

- Upgrading Mercury Business Availability Center Version 4.5 to Version 6.2
- Upgrading Mercury Business Availability Center Version 5.x to Version 6.2
- Upgrading Mercury Business Availability Center Version 6.1.x to Version 6.2

You can access these guides in PDF format (make sure you have Acrobat Reader 4.0 or later installed on the machine) from the following locations:

- From the **Deployment_Documentation** directory on the **Mercury Business Availability Center 6.2 Setup** CD-ROM.
- From the **Documentation\pdfs** directory on the **Mercury Business Availability Center 6.2 Documentation and Utilities** CD-ROM.
- From the Mercury Business Availability Center Documentation Portal area on support.mercury.com.

Configuration Upgrade

Part of the upgrade process requires manually upgrading certain stored data to the new version. This is done from the Configuration Upgrade page. The Configuration Upgrade page also enables you to complete the upgrade.

The configuration upgrade must be performed at a particular stage of the upgrade procedure.

Important: Do not upgrade your data or click the **Finish Upgrade** button until you have completed all the prior upgrade steps, as described in the Upgrade documentation. For details on accessing the documentation, see "Upgrade Documentation" on page 11.

Views Upgrade

Part of the upgrade process requires upgrading custom Dashboard views to Mercury Business Availability Center 6.2 views. This is done from the Views Upgrade page.

The views upgrade must be performed at a particular stage of the upgrade procedure.

Important: Do not upgrade your views until you have completed all the prior upgrade steps, as described in the Upgrade documentation. For details on accessing the documentation, see “Upgrade Documentation” on page 11.

Service Level Management SLAs Upgrade

For details on the upgrade procedure for Service Level Management SLAs, see “Upgrading Service Level Management to Mercury Business Availability Center 6.2” in *Application Administration*.

3

Database Administration

You can maintain and administer the databases Mercury Business Availability Center uses to store profile and monitoring data.You can create and manage profile databases directly from the Administration Console. You can also enable the Purging Manager to purge the data in the database periodically according to your organization’s needs.

Database Management

Note to Mercury Managed Services customers: Mercury Operations administers these pages and the interface is hidden from your view.

Before you create profiles, you must configure the database(s) into which you want profile data saved. A profile database can store data for multiple profiles, as well as from any type of profile (Business Process Monitor, Client Monitor, SiteScope). You can either create one database for all profile data or create dedicated databases (for example, for each profile type).

Note: The term **database** is used to refer to a database in MS SQL Server and a user schema in Oracle Server.

Mercury Business Availability Center supports two database types:

- **Microsoft SQL Server.** This database runs on Windows operating systems only – for details, see page 17.
- **Oracle Server.** This database runs on Windows or Solaris operating systems – for details, see page 21.

The Database Management page, accessed from the Setup and Maintenance tab in Platform Administration, enables you to perform the following database management tasks:

- **create a new database.** Mercury Business Availability Center automatically creates a new database and populates it with profile tables.
- **add profile tables to an existing, empty database.** Mercury Business Availability Center connects to an empty database that was manually created on your database server, and populates it with profile tables.
- **connect to an existing database populated with profile tables.** Mercury Business Availability Center connects to a profile database that was either manually created and populated with profile tables, or previously defined in Platform Administration.

To deploy profile databases on MS SQL Server or Oracle Server for your organization's particular environment, follow the instructions in "Databases Used in Mercury Business Availability Center" in *Preparing the Database Environment*. It is recommended that you review the relevant portions of *Preparing the Database Environment* before performing profile database management tasks.

Configuring a Profile Database on MS SQL Server

You configure one or more profile databases on your MS SQL Server. Before you begin, make sure that you have the following connection parameters to the database server:

- **Server name.** The name of the machine on which MS SQL Server is installed.
- **Database user name and password.** The user name and password of a user with administrative rights on MS SQL Server (if using SQL server authentication).
- **Server port.** The MS SQL Server's TCP/IP port. The default port, 1433, is automatically displayed.

If required, consult with your organization's database administrator to obtain this information.

Note: It is recommended that you configure MS SQL Server databases manually, and then connect to them in the Database Management page. For details on manually configuring MS SQL Server databases, see "Overview of MS SQL Server Deployment" in *Preparing the Database Environment*.

To configure a profile database on MS SQL Server:

1 In Platform Administration, select **Setup and Maintenance** > **Database Management**. The Database Management page opens.

2 In the database type list, select **MS SQL**, and click **Add**.

Note: If you are configuring a database for training or demonstration purposes, you can select MSDE. The remaining steps in the procedure are identical.

The Profile Database Properties - MS SQL Server page opens.

3 Select or clear the **Create database and/or tables** check box as required:

- ➤ To create a new database, or connect to an existing, empty database, and populate it with profile tables, select the check box.
- ➤ To connect to an existing database already populated with profile tables, clear the check box.

4 Select or clear the **Make this my default profile database (required for custom data types)** check box as required.

This setting is required if you are collecting Real User Monitor, Mercury Diagnostics (if installed), or persistent custom data. For details about custom data, see "Working with Measurement Filters" on page 131. There can be only one default profile database. If a default profile database already exists, selecting this check box overwrites the existing database.

5 In the **Server name** box, enter the name of the machine on which MS SQL Server is installed.

6 In the **Database name** box, enter:

- a descriptive name for the database, if you are configuring a new database
- the name of the existing database, if you are connecting to a database that was previously created

7 If the MS SQL Server's TCP/IP port is configured to work on a different port from the default port (1433), enter it in the **Port** box.

8 Select the type of authentication the MS SQL server is using:

- **Windows authentication.** The user name and password that was used to run the Mercury Business Availability Center service on the current machine is used.
- **SQL server authentication.** In the **User name** and **User password** boxes, enter the user name and password of a user with administrative rights on MS SQL Server.

9 Click **Apply**. Mercury Business Availability Center configures or connects to the database, as instructed, adds it to the database table on the Database Management page, and displays the message: Operation Successful.

Database creation can take several minutes.

10 To configure additional profile databases on MS SQL Server, repeat steps 2-9.

Managing Profile Databases on MS SQL Server

You perform the following tasks, as required, to manage the profile databases configured on your MS SQL Server:

- **Edit database connection parameters.** You can change the type of authentication used, modify the user name and password that is used to connect to profile database on MS SQL Server (for SQL server authentication), if those parameters are changed on the database server, and change the port number used for connecting to the MS SQL Server machine.For details, see page 20.
- **Remove database connection.** You can disconnect a profile database from the Mercury Business Availability Center system. For details, see page 21.

Note: Disconnecting a database removes its reference from the Management database, but does not physically remove the database from the MS SQL Server machine. To delete a database from your MS SQL Server machine, follow the instructions provided in your MS SQL Server documentation.

To edit database properties:

1. On the Database Management page, click the **Edit Database Properties** button beside the MS SQL Server database whose properties you want to edit. The Profile Database Properties - MS SQL Server page opens.
2. Select or clear the **Make this my default profile database (required for custom data types)** check box as required.

   This setting is required if you are collecting Real User Monitor, .Net, J2EE (if installed), or persistent custom data. For details about custom data, see "Working with Measurement Filters" on page 131. There can be only one default profile database. If a default profile database already exists, selecting this check box overwrites the existing database.
3. Change the type of authentication as required.
4. Modify the user name and password as required.

   The existing password appears as a series of asterisks. To edit this field, highlight the current password value and enter the new value.
5. Change the port number as required.
6. Click **Apply** to save the settings and return to the Database Management page.

   Click **Cancel** to return to the Database Management page without saving any changes.

To disconnect a database from the Mercury Business Availability Center system:

1 On the Database Management page, click the **Disconnect Database** button beside the MS SQL Server database that you want to disconnect. The Profile Database Properties - MS SQL Server page opens.

2 Click **Disconnect**. The database is disconnected and removed from the table on the Database Management page.

Click **Cancel** to return to the Database Management page without disconnecting the database.

Creating a User Schema on Oracle Server

You configure one or more profile user schemas on your Oracle Server. Before you begin, ensure that:

- Oracle Client is installed on the server machines and that the **tnsnames.ora** file contains the correct connection parameters to the Oracle Server.
- You have created a dedicated default tablespace for profile user schemas (and a dedicated temporary tablespace, if required).
- You are using a secure network connection if you do not want to submit database administrator connection parameters over a non-secure connection. If you do not want to submit database administrator connection parameters via your Web browser at all, you can manually create profile user schemas and then connect to them from the Database Management page.

In addition, before you begin, make sure that you have the following connection parameters to the database server:

- **Host name.** The name of the machine on which Oracle Server is installed.
- **SID.** The Oracle instance name that uniquely identifies the instance of the Oracle database being used, if different from the default value, **orcl**.
- **Port.** The Oracle listener port, if different from the default value, **1521**.
- **Database administrator user name and password.** The name and password of a user with administrative permissions on Oracle Server.

- **Default tablespace.** The name of the dedicated default tablespace you created for profile user schemas (for details on creating a dedicated tablespace, see "Overview of Oracle Server Deployment" in *Preparing the Database Environment*). If you did not create, and do not require, a dedicated default tablespace, specify an alternative tablespace. The default Oracle tablespace is called **users**.
- **Temporary tablespace.** The name of the dedicated temporary tablespace you created for profile user schemas. If you did not create, and do not require, a dedicated temporary tablespace, specify an alternative tablespace. The default Oracle temporary tablespace is called **temp**.
- **TNS name.** The TNS name of the Oracle Client, as specified in the **tnsnames.ora** file on the core server machine.

  If required, consult with your organization's database administrator to obtain this information.

Note: It is recommended that you configure Oracle Server user schemas manually, and then connect to them in the Database Management page. For details on manually configuring Oracle Server user schemas, see "Overview of Oracle Server Deployment" in *Preparing the Database Environment*.

To configure a profile user schema on Oracle Server:

1. In Platform Administration, select **Setup and Maintenance** > **Database Management**. The Database Management page opens.
2. In the database type list, select **Oracle**, and click **Add**.

   The Profile User Schema Properties - Oracle Server page opens.
3. Select or clear the **Create database and/or tables** check box as required:
   - To create a new user schema, or connect to an existing, empty user schema, and populate it with profile tables, select the check box.
   - To connect to an existing user schema already populated with profile tables, clear the check box.

Note: Clearing the **Create database and/or tables** check box disables the database administrator connection parameter, tablespace, and TNS name fields on the page, and instructs the platform to ignore the information in these fields when connecting to the Oracle Server machine.

4 Select or clear the **Make this my default profile database (required for custom data types)** check box as required.

This setting is required if you are collecting Real User Monitor, .Net, J2EE (if installed), or persistent custom data. For details about custom data, see “Working with Measurement Filters” on page 131. There can be only one default profile database. If a default profile database already exists, selecting this check box overwrites the existing database.

5 In the **Host name** box, enter the name of the machine on which Oracle Server is installed.

6 In the **SID** box, enter the required Oracle instance name, or accept the default value.

7 In the **Port** box, enter the required Oracle listener port, or accept the default value.

8 In the **New user schema name** box, enter:

- ➤ a descriptive name for the user schema, if you are configuring a new user schema
- ➤ the name of the existing user schema, if you are connecting to a user schema that was previously created

Note: You must specify a unique user schema name for each user schema you create for Mercury Business Availability Center on Oracle Server.

9 In the **TNS name** box, enter the TNS name of the Oracle Client, as specified in the tnsnames.ora file on the core server machine.

10 In the **New user schema password** box, enter:

- a password that enables access to the user schema, if you are configuring a new user schema
- the password of the existing user schema, if you are connecting to a user schema that was previously created

11 In the **Retype password** box, retype the user schema password that you entered in step 10.

If you cleared the **Create database and/or tables** check box in step 3, skip to step 15.

If you selected the **Create database and/or tables** check box in step 3, continue with step 12.

12 In the **Database administrator username** and **Database administrator password** boxes, enter the name and password of a user with administrative permissions on Oracle Server.

13 In the **Default tablespace** box, enter the name of the default tablespace designated for use with profile user schemas.

14 In the **Temporary tablespace** box, enter the name of the temporary tablespace designated for use with profile user schemas, if different from the default value, **temp**.

15 Click **Apply**. Mercury Business Availability Center configures or connects to the user schema, as instructed, adds it to the database table on the Database Management page, and displays the message: Operation Succeeded.

Note: User schema creation can take several minutes. The browser might time out before the creation process is completed. However, the creation process continues on the server side. If a time out occurs before you get a confirmation message, you can verify that the user schema was successfully created by checking that the user schema name appears in the database list on the Database Management page.

---

16 To configure additional profile user schemas on Oracle Server, repeat steps 2-15.

Managing Profile User Schemas on Oracle Server

You perform the following tasks, as required, to manage the profile user schemas configured on your Oracle Server:

- **Edit database connection parameters.** You can modify the password that Mercury Business Availability Center uses to connect to the profile user schema on Oracle Server, and change the port number used to connect to the Oracle Server machine. For details, see page 25.
- **Remove database connections.** You can disconnect a profile user schema from the system. For details, see page 26.

Note: Disconnecting a user schema removes its reference from the management database, but does not physically remove the user schema from the Oracle Server machine. To delete a user schema from your Oracle Server machine, follow the instructions provided in your Oracle Server documentation.

To edit user schema properties:

1. On the Database Management page, click the **Edit Database Properties** button beside the Oracle Server user schema whose properties you want to edit. The Profile User Schema Properties - Oracle Server page opens.
2. Select or clear the **Make this my default profile database (required for custom data types)** check box as required:

   This setting is required if you are collecting Real User Monitor, .Net, J2EE (if installed), or persistent custom data. For details about custom data, see "Working with Measurement Filters" on page 131. There can be only one default profile database. If a default profile database already exists, selecting this check box overwrites the existing database.
3. Modify the user schema password as required.

   The existing password appears as a series of asterisks. To edit this field, highlight the current password value and enter the new value.
4. Change the port number as required.

5 Click **Apply** to save the settings and return to the Database Management page.

Click **Cancel** to return to the Database Management page without saving any changes.

To disconnect a user schema from Mercury Business Availability Center:

1 On the Database Management page, click the **Disconnect Database** button beside the Oracle Server user schema that you want to disconnect. The Profile User Schema Properties - Oracle Server page opens.

2 Click **Disconnect**. Mercury Business Availability Center disconnects the user schema and removes it from the table on the Database Management page.

Click **Cancel** to return to the Database Management page without disconnecting the database.

Purging Historical Data from Profile Databases

Note to Mercury Managed Services customers: Mercury Operations administers these pages and the interface is hidden from your view.

The data collection tables in the profile databases can grow to a very large size, and thus need occasional purging. You use the Purging Manager to instruct the platform to automatically remove historical data from profile databases.

The Purging Manager can be used with profile databases located on the following database servers:

- any Oracle Server version supported by Mercury Business Availability Center
- MS SQL Server 2000 Standard and Enterprise editions (MS SQL Server 7.0 and MSDE are not supported)

For details on advanced purging capabilities, see “Data Partitioning and Purging” in *Preparing the Database Environment*.

Once enabled, the Purging Manager removes data according to the time period listed for the database table. These time periods specify how long the data is saved in the profile database table. After the time period set for each table, the Purging Manager purges aggregated data.

Mercury Business Availability Center includes default time periods for keeping the data in each database table. You can also use the Purging Manager to set a specific time period—per table—for removing data. If you do not modify the default time period and the Purging Manager is enabled, data is removed according to the default range listed for each table.

This section covers the following topics:

- Enabling and Disabling the Purging Manager – for details, see page 27
- Modifying the Default Time Range Configurations – for details, see page 28
- Guidelines and Tips for Using the Purging Manager – for details, see page 30

Enabling and Disabling the Purging Manager

By default the Purging Manager is disabled. You can enable the Purging Manager to instruct Mercury Business Availability Center to begin the process of data removal. Once enabled, the Purging Manager runs every hour and checks whether it has work (whether there is data to remove or purge). The Purging Manager removes data only after the data has been aggregated.

Note: When working with an Oracle database, it is strongly recommended that you set **PARTITION_VIEW_ENABLED** parameter in the Oracle initialization file to **True**. For details on purging data from an Oracle database, see “Creating Oracle Tablespaces When Using the Purging Manager” in *Preparing the Database Environment*.

To enable the Purging Manager:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Data Purging**. The Purging Manager page opens.
2. Click **Enable** to enable the Purging Manager.

To disable the Purging Manager:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Data Purging**. The Purging Manager page opens.
2. Click **Disable** to disable the Purging Manager.

Modifying the Default Time Range Configurations

If required, you can modify the default time period configurations per table. You can make those modifications to the database tables globally, for all profile databases, or per profile database.

Note: Another parameter that can affect the purging process is the EPM parameter. For details on working with this parameter, see “Calculating Purging Manager Parameter Values” in *Preparing the Database Environment*.

To modify the Purging Manager settings:

1. In Platform Administration, select **Setup and Maintenance** > **Data Purging**. The Purging Manager page opens.
2. Select whether you want your changes to affect the selected table in all the profile databases in your platform, that is globally, or per individual profile database.
   - ➤ To change the time range for purging data in a table for all profile databases, select the **Global Settings** tab.
   - ➤ To change the time range for purging data in a table per profile database, select the **Database-Specific Settings** tab and select the profile database from the drop-down list at the top of the section.

Note: Once you modify tables for a specific profile (under the Database-Specific Settings tab), any changes made globally (under the Global Settings tab) do not affect the tables for that profile. Any additional changes to purging settings for that database must be made from the Database-Specific Settings tab.

It is recommended that you select the Global Settings tab unless there is a table in a specific profile database for which you must configure a different purging time period.

3. Select the check box next to all the database tables for which you want to change the purging time range to the same time period.

   All database tables are listed by the data collector from which the data was gathered. There is also a table for Service Level Management data that is not considered raw data. Choose from the following data types:

   - Business Logic Engine
   - Business Process Monitor
   - Diagnostics
   - Real User Monitor
   - Service Level Management
   - SiteScope
   - UDX (custom data)
   - WebTrace

4. Set the new time range for keeping data in the selected database tables by selecting the number and the time unit in the appropriate **Keep data for** boxes.

5. Click **Apply**.

6. Repeat steps 3 through 5 for additional time periods you want to set, selecting the database tables that are purged for that time period.

   Configuration changes automatically take effect at the beginning of the next Purging Manager cycle.

Guidelines and Tips for Using the Purging Manager

- Prior to purging, the Purging Manager performs an additional check to ensure that raw data is not purged before it has been aggregated and reported to Mercury Business Availability Center. If a particular profile database's data is scheduled for purging but it's raw data has not yet been aggregated, the Purging Manager does not purge the data according to its schedule. The Purging Manager automatically purges the data on it's next hourly run only after the data has been aggregated. For example, if data was scheduled to be purged on Sunday at 8:00 but its data was only aggregated on Sunday at 10:00, the Purging Manager checks the data at 8:00, does not purge the data, and automatically purges the data on its next hourly run only after Sunday at 10:00 once the data has been aggregated.
- If you find that data is not being purged according to the schedules set in the Purging Manager and your profile databases are growing too large, check that the aggregator is running properly and view the Purging Manager logs located in **<Mercury Business Availability Center server root directory>/log/pmanager.log**.

  Mercury Business Availability Center displays raw data only in the following contexts: SiteScope Warning Summary and SiteScope Error Summary reports, transaction breakdown data used in trend reports, Service Level Management reports, and Excel Reports that use raw data.

  Because aggregated data is not used in these reports, if the raw data for a specific time period has been removed from the profile database using the Purging Manager, those reports do not contain any data when generated for that time period.
- Keep in mind the following principle, which the default configuration uses: the length of time that raw data is kept is shorter than the length of time that one-hour chunks of aggregated data are kept, which is shorter than the length of time that one-day chunks of aggregated data are kept.

- Any changes made under the Global Setting tab affect the default time periods for new profile databases created in the system. If a new profile database is created after you have made modifications to the time periods under the Global Settings tab, data is kept in the tables of that new profile database for the time periods now listed under Global Settings for all tables.

Removing Unwanted Data from the Profile Database

Note to Mercury Managed Services customers: This section is not relevant to Mercury Managed Services customers.

The Data Marking utility enables Mercury Business Availability Center users with superuser security privileges to mark specific sets of data in profile databases as unwanted. The utility does not physically remove marked data from the database, however it renders it unusable in reports and applications by assigning the marked data a status of “unavailable” in the database. During installation, Mercury Business Availability Center installs the Data Marking utility to the Core Server.

After you mark a specific set of data from a given time period as unwanted, Mercury Business Availability Center reruns the aggregation process on remaining raw data for the relevant time period so that reports using aggregated data display only the relevant data. The Data Marking utility also enables you to reaggregate a defined set of data without marking it as unavailable. For details, see “Enabling the Reaggregation-Only Option” on page 35.

Currently, the Data Marking utility enables removal of unwanted Business Process Monitor, Client Monitor, and SiteScope data.

The Data Marking utility supports partitions. Thus, users running the Purging Manager can also use the Data Marking utility.

This section covers the following topics:

- Working with the Data Marking Utility – for details, see page 32
- Enabling the Reaggregation-Only Option – for details, see page 35
- Troubleshooting Data Marking Utility Errors – for details, see page 36
- Data Marking Utility Limitations – for details, see page 37

Working with the Data Marking Utility

The Data Marking utility enables you to select sets of data for removal by profile or by location for Business Process Monitor and Client Monitor data, and by SiteScope target machine for SiteScope data.

- Business Process Monitor and Client Monitor data:
  - **Profile view.** In the Profile view, you select a Business Process Monitor or Client Monitor profile and then one or more transactions or locations for which you want to mark data for removal. This view is helpful if you want to remove data collected for specific transactions, for example, transactions that ran during unexpected system downtime.
  - **Location view.** In the Location view, you select a location and then one or more Business Process Monitor or Client Monitor profiles for which you want to mark data for removal. This view is helpful if you want to remove data collected from a specific location, for example, a location at which the installed Business Process Monitor machine was experiencing technical problems for a period of time.
- SiteScope data:
  - **SiteScope view.** In SiteScope view, you select a SiteScope target machine for which you want to mark data for removal. The SiteScope target is the machine which the SiteScope is monitoring. The SiteScope target list includes all machines being monitored by all the SiteScopes for which profiles are running within your Mercury Business Availability Center platform. The target machine is listed with the name of the profile running the SiteScope in parentheses. If a target machine is monitored by more than one SiteScope, then the target machine is listed more than once with the different profile names in parenthesis.

After selecting the above criteria, you specify a time range over which to mark data as unwanted.

Before executing the data marking run, you can review the number of data rows that will be affected using the **Get Info** button. After a data marking run is completed, use the **Get Info** button after a run to view the number of data rows still unmarked within the selected time period and filter criteria.

After the utility marks the specified data as unavailable, Mercury Business Availability Center automatically reaggregates the remaining raw data for the selected time period.

To mark data as unwanted:

1. On the Core Server, double-click the <**Mercury Business Availability Center Core Server root directory**>**\tools\dataMarking\dataMarking.bat** file. A Command Prompt window opens, followed by the Data Marking utility login dialog box.
2. Enter the username and password of a Mercury Business Availability Center user with administrator or superuser privileges.
3. Click **OK** to open the main Data Marking utility screen.
4. Select either **Profiles** or **Locations** in the **View by** box.
5. Choose the required filter criteria:
   - In the **Profile View**, select a profile as well as one or more transactions and one or more locations.
   - In the **Location View**, select a location as well as one or more profiles.
   - In the **SiteScope View**, select a target machine.
6. Choose the **Mark data as obsolete** check box.
7. In the **Start Time** section, select a starting date and time.
8. In the **Duration** section, select the period of time, starting from the specified start time, for which the utility will mark data as unavailable. You can set a maximum duration of up to 6 hours and 59 minutes for each data marking run. This value can be customized; for details, see “Customizing Data Marking Utility Configurations” on page 34.

9 Click the **Get Info** button before a run to view the number of data rows to be marked.

10 Click **Start**, and confirm that you want to begin. The Data Marking utility starts its run. The utility displays the progress of the data marking and the reaggregation of remaining raw data for the specified time period.

11 When the run is completed, a status message is displayed.

In certain cases, not all data rows defined by the filter criteria may have been marked (for examples of such cases, see “Data Marking Utility Limitations” on page 37). Click the **Get Info** button to view the number of data rows still unmarked within the selected time period and filter criteria. If necessary, rerun the Data Marking utility with the same set of filters to mark the missed rows.

Customizing Data Marking Utility Configurations

You can configure the maximum duration for each data marking run. The current default is 6 hours and 59 minutes.

To configure the maximum duration:

1 Open the **<Mercury Business Availability Center Core Server root directory>\tools\dataMarking\dataMarking.bat** file in a text editor.

2 Add the **-DmaximumDuration=xx** property to the command line, where xx represents the maximum duration in hours.

For example, to change the maximum duration to 23 hours and 59 minutes, replace:

```
%TOPAZ_HOME%\JRE\bin\java -Dtopaz.home=%TOPAZ_HOME% -jar
datamarking.jar
```

with:

```
%TOPAZ_HOME%\JRE\bin\java -Dtopaz.home=%TOPAZ_HOME% -
DmaximumDuration=24 -jar datamarking.jar
```

3 Save and close the file.

Restoring Marked Data

The Data Marking utility also includes an un-mark feature that enables you to reverse the data marking action and clear data that has been marked as unavailable so that the data is made available again. Re-aggregation is automatically initiated once data has been un-marked.

To un-mark data that has been marked as unavailable:

1. Define the set of data you want to make available again, as described in “Working with the Data Marking Utility” on page 32.
2. In step 6, choose the **Mark data as valid** check box.
3. Follow the rest of the data marking procedure from step 7 through step 11.

Enabling the Reaggregation-Only Option

By default, the Data Marking utility always runs the data marking process, followed by the reaggregation process. If required, you can enable a feature that allows you to instruct Mercury Business Availability Center to run only reaggregation. This might be required if data marking passed successfully but reaggregation failed. Alternatively, you can use this feature to reaggregate a defined set of data without marking it as unavailable (for example, if data was aggregated and then late-arriving data was inserted into the raw data tables in the database).

To enable the reaggregation-only option:

1. Open the file **dataMarking.bat** in a text editor.
2. Change the line:

   ```
   %TOPAZ_HOME%\JRE\bin\java -Dtopaz.home=%TOPAZ_HOME% -jar datamarking.jar
   ```

   to

   ```
   %TOPAZ_HOME%\JRE\bin\java -Dtopaz.home=%TOPAZ_HOME% -DadvancedMode=true -jar datamarking.jar
   ```

3. Save the file. The next time you open the Data Marking utility, the **Advanced** button appears.

   After you enable this feature, you can instruct the Data Marking utility to only run the data reaggregation process when clicking the **Start** button.

To run data reaggregation only:

1. Define the set of data you want to reaggregate, as described in “Working with the Data Marking Utility” on page 32.
2. Click the **Advanced** button. The Advanced window opens.
3. Select the **Run reaggregation only** check box.
4. Select the categories of data for the reaggregation and click **OK** to confirm selection.
5. Click **Start**.

Troubleshooting Data Marking Utility Errors

Various types of errors might occur while using the Data Marking utility. Generally, when an error occurs, the utility displays the following error message:

```
The Data Marking utility must shut down due to an internal error. For details see:
<Mercury Business Availability Center Core Server root
directory>\log\datamarking.log
```

Reasons for which the utility might display this error include:

- failure to connect to the database server or profile database
- failure to complete the data marking process, for example, due to communication error between the Aggregation Server and database
- failure of Mercury Business Availability Center to successfully reaggregate raw data for the defined data set

In case of error, check the **datamarking.log** file for error information.

Data Marking Utility Limitations

- The utility does not support the removal of late arriving data. For example, if a set of data for a specific time period is marked for removal, and later Mercury Business Availability Center receives data from that time period (which arrived late due to a Business Process Monitor temporarily being unable to connect to the Core Server), the late arriving data will be available for use in reports. Use the **Get Info** button to check for late arriving data. If zero rows are not displayed, run the utility again, if required, to remove the data that arrived late.

- The utility does not support removal of data arriving during the data marking process. For example, if a set of data for a specific time period is marked for removal, and during that same time period (while the utility is running), data arrives and enters the profile database, the rows of newly arrived data are not marked for removal, and are therefore not removed. In this case, after the utility finishes running, use the **Get Info** button to determine whether all rows of data were removed for the selected time period. If zero rows are not displayed, run the utility again, if required, to remove the data that arrived during the run. This is a rare scenario as typically you would mark data for a previous time period, not for a time period that ends in the future.

- While the utility is running, and removing data, reports that are generated for that time period may not show accurate results. As such, it is recommended to run the utility during off-peak hours of Mercury Business Availability Center usage.

- Do not run more than one instance of the Data Marking utility at one time as this can affect the reaggregation process.

- Do not mark data sets for time periods that include purged data (data that has been removed using the Purging Manager) as this can affect the reaggregation process.

4

Mercury Universal CMDB Management

When a management database is created for Mercury Business Availability Center, the CMDB is included by default. You can create a new CMDB and direct Mercury Business Availability Center to work with it.

Managing the Database for CMDB

Note to Mercury Managed Services customers: Mercury Operations administers these pages and the interface is hidden from your view.

The Mercury Universal CMDB (Configuration Management Database) is the central repository for the configuration information that is gathered from the various Mercury Business Availability Center and third-party applications and tools.

The CMDB contains all the configuration items (CIs) and relationships created in Mercury Business Availability Center, whether created automatically from the discovery process or source adapters, or manually using the IT Universe editor. The CIs and relationships together represent a model of the IT universe in which your business functions.

CMDB is automatically created as part of the Mercury Business Availability Center management database. If you want to use a CMDB that is different from the default (for example, if you have over one million CIs, or if the CMDB is being shared with Mercury Application Mapping) you create a new CMDB and configure Mercury Business Availability Center to use the new CMDB, instead of the default one. For details on sharing the Mercury Universal CMDB, see “Sharing the Mercury Universal CMDB Environment” in *Working with the CMDB*.

Warning: When you create and work with a new CMDB, no data is copied from the old CMDB to the new one, therefore you can create and use a new CMDB only for a new Mercury Business Availability Center installation, before the system is used in a live environment.

Note: Each CMDB created contains the same basic, default classes and views.

Mercury Business Availability Center supports two database types:

- **Microsoft SQL Server.** This database runs on Windows operating systems only – for details, see page 41.
- **Oracle Server.** This database runs on Windows or Solaris operating systems – for details, see page 44.

Note: The term **database** is used to refer to a database in MS SQL Server and a user schema in Oracle Server.

The CMDB Database Management page, accessed from the Setup and Maintenance tab in Platform Administration, enables you to perform the following database management tasks:

- **create a new CMDB.** Mercury Business Availability Center automatically creates a new CMDB and populates it with tables.
- **connect to an existing CMDB populated with tables.** Mercury Business Availability Center connects to a CMDB that was either manually created and populated with CMDB tables, or previously defined in Platform Administration.

To deploy CMDB on MS SQL Server or Oracle Server for your organization's particular environment, follow the instructions in "Databases Used in Mercury Business Availability Center" in *Preparing the Database Environment*. It is recommended that you review the relevant portions of *Preparing the Database Environment* before performing CMDB management tasks.

Configuring CMDB on MS SQL Server

Before you begin, make sure that you have the following connection parameters to the database server:

- **Server name.** The name of the machine on which MS SQL Server is installed.
- **Database user name and password**. The user name and password of a user with administrative rights on MS SQL Server (if using SQL server authentication).
- **Server port.** The MS SQL Server's TCP/IP port. The default port, 1433, is automatically displayed.

If required, consult with your organization's database administrator to obtain this information.

Note: It is recommended that you create an MS SQL Server database and add the CMDB schema manually, and then connect to it in the CMDB Database Management page. For details on manually creating an MS SQL Server database and adding the CMDB schema, see "Creating and Configuring MS SQL Server Databases" in *Preparing the Database Environment*.

To configure CMDB on MS SQL Server:

1 In **Admin** > **Platform** > **Setup and Maintenance,** choose **Manage Database for CMDB**. The CMDB Database Management page opens.

2 In the database type list, select **MS SQL**, and click **Add**.

The CMDB Database Management page opens.

3 Select or clear the **Create database and/or tables** check box as required:

- ➤ To create a new database and populate it with CMDB tables, select the check box.
- ➤ To connect to an existing database already populated with CMDB tables, clear the check box.

4 In the **Server name** box, enter the name of the machine on which MS SQL Server is installed.

5 In the **Database name** box, enter:

- ➤ a descriptive name for the database, if you are configuring a new database
- ➤ the name of the existing database, if you are connecting to a database that was previously created

6 If the MS SQL Server's TCP/IP port is configured to work on a different port from the default port (1433), enter it in the **Port** box.

7 Select the type of authentication the MS SQL server is using:

- ➤ **Windows authentication.** The user name and password that was used to run the Mercury Business Availability Center service on the current machine will be used.

- **SQL server authentication.** In the **User name** and **User password** boxes, type the user name and password of a user with administrative rights on MS SQL Server.

8. Click **Apply**. Mercury Business Availability Center configures or connects to the database, as instructed, adds it to the database table on the CMDB Database Management page, and displays the message: Operation Successful.

   Database creation can take several minutes.

Managing CMDB on MS SQL Server

You perform the following tasks, as required, to manage CMDB configured on your MS SQL Server:

- **Edit database connection parameters.** You can change the type of authentication used, modify the user name and password that is used to connect to CMDB on MS SQL Server (for SQL server authentication), if those parameters are changed on the database server, and change the port number used for connecting to the MS SQL Server machine. For details, see page 43.
- **Remove database connection.** You can disconnect a CMDB from the Mercury Business Availability Center system. For details, see page 44.

Note: Disconnecting a database removes its reference from the Management database, but does not physically remove the database from the MS SQL Server machine. To delete a database from your MS SQL Server machine, follow the instructions provided in your MS SQL Server documentation.

To edit database properties:

1. On the CMDB Database Management page, click the **Edit Database Properties** button beside the MS SQL Server CMDB whose properties you want to edit. The CMDB Database Management page opens.
2. Change the type of authentication as required.
3. Modify the user name and password as required.

The existing password appears as a series of asterisks. To edit this field, highlight the current password value and enter the new value.

4. Change the port number as required.
5. Click **Apply** to save the settings and return to the Database Management page.

   Click **Cancel** to return to the CMDB Database Management page without saving any changes.

To disconnect a database from the Mercury Business Availability Center system:

1. On the CMDB Database Management page, click the **Disconnect Database** button beside the MS SQL Server database that you want to disconnect. The CMDB Database Management page opens.
2. Click **Disconnect**. The database is disconnected and removed from the table on the Database Management page.

   Click **Cancel** to return to the CMDB Database Management page without disconnecting the database.

Creating a User Schema on Oracle Server

Before you begin, ensure that:

- Oracle Client is installed on the server machines and that the **tnsnames.ora** file contains the correct connection parameters to the Oracle Server.
- You have created a dedicated default tablespace for the CMDB schema (and a dedicated temporary tablespace, if required).
- You are using a secure network connection if you do not want to submit database administrator connection parameters over a non-secure connection. If you do not want to submit database administrator connection parameters via your Web browser at all, you can manually create the CMDB schema and then connect to them from the Database Management page.

In addition, before you begin, make sure that you have the following connection parameters to the database server:

- **Host name.** The name of the machine on which Oracle Server is installed.
- **SID.** The Oracle instance name that uniquely identifies the instance of the Oracle database being used, if different from the default value, **orcl**.
- **Port.** The Oracle listener port, if different from the default value, **1521**.
- **Database administrator user name and password.** The name and password of a user with administrative permissions on Oracle Server.
- **Default tablespace.** The name of the dedicated default tablespace you created for the CMDB schema (for details on creating a dedicated tablespace, see "Overview of Oracle Server Deployment" in *Preparing the Database Environment*). If you did not create, and do not require, a dedicated default tablespace, specify an alternative tablespace (the default Oracle tablespace is called **users**).
- **Temporary tablespace.** The name of the dedicated temporary tablespace you created for the CMDB schema. If you did not create, and do not require, a dedicated temporary tablespace, specify an alternative tablespace (the default Oracle temporary tablespace is called **temp**).
- **TNS name.** The TNS name of the Oracle Client, as specified in the tnsnames.ora file on the core server machine.

  If required, consult with your organization's database administrator to obtain this information.

Note: It is recommended that you create an Oracle Server tablespace and add the CMDB user schema manually, and then connect to it in the CMDB Database Management page. For details on manually creating an Oracle Server tablespace and adding the CMDB user schema manually, see "Setting Up the Mercury Business Availability Center Database Environment" in *Preparing the Database Environment*.

To configure a CMDB user schema on Oracle Server:

1. In **Admin** > **Platform** > **Setup and Maintenance,** choose **Manage Database for CMDB**. The CMDB Database Management page opens.

2. In the database type list, select **Oracle**, and click **Add**.

   The CMDB Database Management page opens.

3. Select or clear the **Create database and/or tables** check box as required:

   - To create a new user schema and populate it with CMDB tables, select the check box.

   - To connect to an existing user schema already populated with CMDB tables, clear the check box.

4. In the **Host name** box, type the name of the machine on which Oracle Server is installed.

5. In the **SID** box, type the required Oracle instance name, or accept the default value.

6. In the **Port** box, type the required Oracle listener port, or accept the default value.

7. In the **New user schema name** box, type:

   - a descriptive name for the user schema, if you are configuring a new user schema

   - the name of the existing user schema, if you are connecting to a user schema that was previously created

   ---

   Note: You must specify a unique user schema name for each user schema you create for Mercury Business Availability Center on Oracle Server.

   ---

8. In the **New user schema password** box, type:

   - a password that will enable access to the user schema, if you are configuring a new user schema

   - the password of the existing user schema, if you are connecting to a user schema that was previously created

9 In the **Retype password** box, retype the user schema password that you entered in step 8.

10 In the **TNS name** box, type the TNS name of the Oracle Client, as specified in the **tnsnames.ora** file on the core server machine.

11 In the **Database administrator username** and **Database administrator password** boxes, type the name and password of a user with administrative permissions on Oracle Server.

12 In the **Default tablespace** box, type the name of the default tablespace designated for use with the CMDB schema.

13 In the **Temporary tablespace** box, type the name of the temporary tablespace designated for use with the CMDB schema, if different from the default value, **temp**.

14 Click **Apply**. Mercury Business Availability Center configures or connects to the user schema, as instructed, adds it to the database table on the CMDB Database Management page, and displays the message: Operation Succeeded.

Note: User schema creation can take several minutes. The browser might time out before the creation process is completed. However, the creation process continues on the server side. If a time out occurs before you get a confirmation message, you can verify that the user schema was successfully created by checking that the user schema name appears in the database list on the CMDB Database Management page.

Managing CMDB User Schemas on Oracle Server

You perform the following tasks, as required, to manage the CMDB user schemas configured on your Oracle Server:

➤ **Edit database connection parameters.** You can modify the password that Mercury Business Availability Center uses to connect to the CMDB user schema on Oracle Server, and change the port number used to connect to the Oracle Server machine. For details, see page 48.

➤ **Remove database connections.** You can disconnect a CMDB user schema from the system. For details, see page 48.

Note: Disconnecting a user schema removes its reference from the management database, but does not physically remove the user schema from the Oracle Server machine. To delete a user schema from your Oracle Server machine, follow the instructions provided in your Oracle Server documentation.

To edit CMDB user schema properties:

1 On the CMDB Database Management page, click the **Edit Database Properties** button beside the Oracle Server user schema whose properties you want to edit. The CMDB Database Management page opens.

2 Modify the user schema password as required.

The existing password appears as a series of asterisks. To edit this field, highlight the current password value and enter the new value.

3 Change the port number as required.

4 Click **Apply** to save the settings and return to the CMDB Database Management page.

Click **Cancel** to return to the CMDB Database Management page without saving any changes.

To disconnect a CMDB user schema from Mercury Business Availability Center:

1 On the CMDB Database Management page, click the **Disconnect Database** button beside the Oracle Server user schema that you want to disconnect. The CMDB Database Management page opens.

2 Click **Disconnect**. Mercury Business Availability Center disconnects the user schema and removes it from the table on the CMDB Database Management page.

Click **Cancel** to return to the CMDB Database Management page without disconnecting the database.

Redirecting Mercury Business Availability Center to Work with a New CMDB

After you create a new CMDB, you redirect Mercury Business Availability Center to work with the new CMDB instead of the default one.

To redirect Mercury Business Availability Center to work with a new CMDB:

1. In **Admin** > **Platform** > **Setup and Maintenance,** choose **Manage Database for CMDB**. The CMDB Database Management page opens.
2. On the CMDB Database Management page, click the **Change CMDB** button beside the new CMDB to which you want to redirect Mercury Business Availability Center.
3. Restart the Mercury Business Availability Center Data Processing Server (or Modeling Data Processing Server in an enterprise deployment).

Note: Redirecting Mercury Business Availability Center to a different CMDB does not copy any data from the old CMDB to the new one.

5

Managing System Health

Note to Mercury Managed Services customers: Mercury Operations administers these pages and the interface is hidden from your view.

The System Health page enables high-level Mercury Business Availability Center administrators to manage the workload of the Data Processing Servers and the services they are running by setting up Automatic Failover or manually reassigning services among servers in response to resource issues or for maintenance purposes.

Working with the System Health Page

The System Health page enables high-level Mercury Business Availability Center administrators to monitor the load on the Data Processing Servers in the Mercury Business Availability Center server architecture and manage the Data Processing Servers—by setting up Automatic Failover or by manually reassigning services from one server to another —to prevent downtime due to insufficient resources on a particular machine or due to required server machine maintenance.

Administrators can also view static information about the machines on which the Centers Servers and Core Servers are running.

Note:

- For complete details on setting up a high availability deployment of Mercury Business Availability Center servers, as well as descriptions of all services that run on the Data Processing Server, see "High Availability for Mercury Business Availability Center" in *Deploying Servers*.
- Reassigning services from one server to another can also be done using the JMX Console. It is recommended that the JMX Console only be used to reassign services that cannot be reassigned via the System Health page. For details, see "Manually Reassigning Services" in *Deploying Servers*.

Permissions Required to Access the System Health Page

The System Health page can be accessed by users with Superuser or Administrator permissions.

System Health Page Layout

The System Health page can be viewed by selecting **Admin** > **Platform** > **Setup and Maintenance** > **System Health**. The System Health page is divided into three panes:

- **Servers.** The Servers pane is located on the top left of the page and lists:
  - in the All tab, the names and types of all the installed servers
  - in the Data Processing tab, the names of all the Data Processing Servers, the service configuration for each, and the status of the worst monitored server resource
- **Services.** The Services pane is located on the top right of the page and displays the statuses of all the monitored server resources for the server currently selected in the Servers pane.
- **Management.** The Management pane is located across the bottom of the page and displays the status of tasks that are running or were run during the course of the current Web session.

Understanding Service Reassignment

In typical enterprise environments, the Data Processing Server is split into three standalone servers:

- Modeling Data Processing Server
- Online Data Processing Server
- Offline Data Processing Server

Each server is installed on a separate machine. Each server might also be installed on one or more backup machines.

Note: Because Mercury Business Availability Center allows only one active Data Processing Server of each type at any given time, the servers cannot be load balanced.

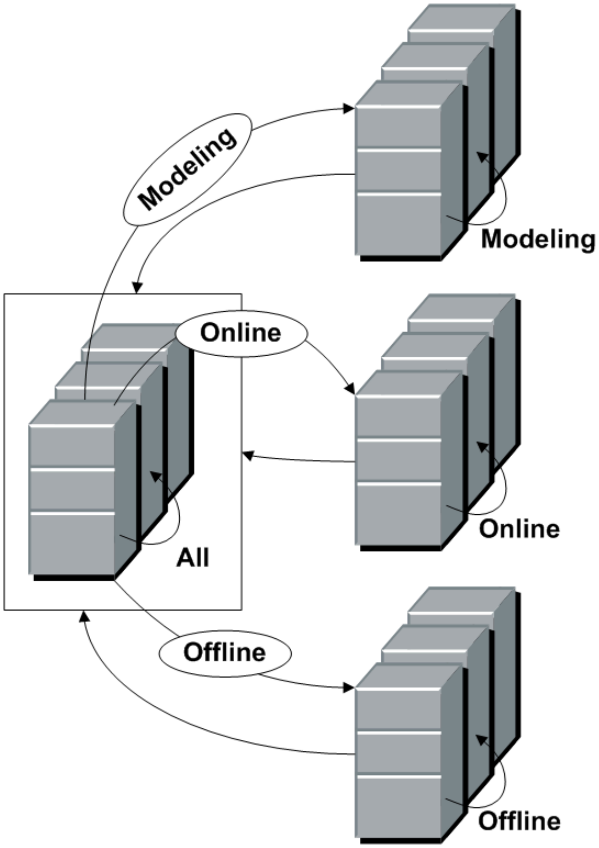
If a certain Data Processing Server machine is not functioning properly or requires downtime for servicing, administrators can manually reassign the services running on that machine to a different Data Processing Server machine. Administrators can also preconfigure a specific Data Processing Server to automatically fail over to a specific backup machine.

Important: Before manually reassigning services to another server or configuring a server as a backup server for Automatic Failover, ensure that the Mercury Business Availability Center service is running on that server.

When a service is reassigned via the System Health interface from an active Data Processing Server to a different Data Processing Server, for example a backup server, Mercury Business Availability Center modifies the setting in the management database that defines the active Data Processing Server. The newly defined server setting in the management database is read by the high availability controller running on the Data Processing Servers. At that point, a process begins whereby Mercury Business Availability Center stops using the services on the previously active server and begins using the services on the newly active server. This process can take up to several minutes, during which time the system is in downtime.

There are several theoretical scenarios for reassigning services among machines, to manage resource issues or enable server administration. The arrows in the below diagram and the table that follows it illustrate these scenarios by indicating the paths along which services can be reassigned.

Flow Diagram



Flow Table

	To Full Data Processing Server	To Modeling Data Processing Server	To Online Data Processing Server	To Offline Data Processing Server
From Full Data Processing Server	✓	✓	✓	✓
From Modeling Data Processing Server	✓	✓	X	X
From Online Data Processing Server	✓	X	✓	X
From Offline Data Processing Server	✓	X	X	✓

Monitoring System Resources on the System Health Page

High-level Mercury Business Availability Center administrators can use the System Health page to monitor system resource status to identify potential resource issues and take action before the system is adversely affected.

This section includes the following topics:

➤ “Viewing Server Architecture” on page 57

➤ “Viewing Data Processing Server Configuration” on page 57

➤ “Viewing Data Processing Server Properties” on page 57

➤ “Understanding Data Processing Server Resource Status” on page 58

Viewing Server Architecture

From the All tab in the Servers pane, you can view the names of all the servers that are deployed in the Mercury Business Availability Center server architecture, and their type (Centers, Core, or Data Processing).

Viewing Data Processing Server Configuration

From the Data Processing tab in the Servers pane, you can view the names of all the Data Processing Servers that are deployed in the Mercury Business Availability Center server architecture, and their configuration (All services, Modeling, Online, Offline). For details on Data Processing Server configurations, see “Services Assigned to each of the Data Processing Servers” in *Deploying Servers*.

In addition, the status of the worst-performing monitored resource is displayed in the Worst Resource column. For details on resource status, see “Understanding Data Processing Server Resource Status” on page 58.

Viewing Data Processing Server Properties

When a specific server is selected from the Data Processing tab in the Servers pane, you can view properties for that server by clicking the Show Properties button in the Services pane. The Properties dialog box displays the following properties:

- **Name.** The server name.
- **IP.** The server IP address.
- **Backup server for this server.** If a backup server is configured for the server, the name of the backup server is displayed. Note that this information is displayed even if Automatic Failover has been disabled.
- **This server is a backup for servers.** If the server is configured as a backup server, the names of the severs the server is backing up are displayed. Note that this information is displayed even if Automatic Failover has been disabled.

Understanding Data Processing Server Resource Status

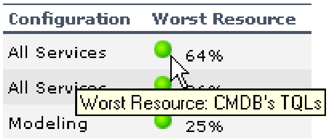
The resource status information that is displayed on the System Health page is based on capacity limit and threshold settings that are preconfigured by Mercury. These settings can be viewed in the Infrastructure Settings Manager (select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, and select **System Health**).

Warning: Do not modify Capacity Limit settings as doing so can adversely affect the performance of Mercury Business Availability Center. If your organization requires modification of these settings, it should be done in coordination with your Mercury representative.

Types of Resource Status Information

Two types of resource status information are displayed:

- **percentage of capacity limit.** Represents the actual usage of the resource relative to its configured capacity limit. In the example below, the CMDB's TQLs are at 64% of capacity (in this case, 77 TQLs out of a limit of 120).



Configuration	Worst Resource
All Services	● 64%
All Servi	●
Modeling	● 25%

Worst Resource: CMDB's TQLs

- **threshold representation of the percentage of capacity limit.** Uses a color-coded icon to express the percentage of the capacity limit , based on the following ranges:

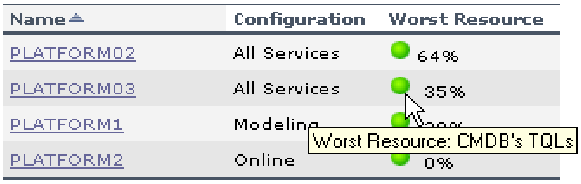
Range	Color Code
<=70% of capacity limit	Green
>70% but <=90% of capacity limit	Yellow

Range	**Color Code**
> 90% of capacity limit	Red
No data/No services running	Gray

Resource Status Information in the Servers Pane

In the Servers pane, you can see the following resource status information:

- for each active server in the list, the percentage of capacity limit and its threshold representation, in the Worst Resource column, indicating the status of the worst-performing resource among all the resources being monitored on that server.
- a tooltip with resource details. Place your mouse pointer over a threshold icon to view information on the specific resource whose status is being reported.



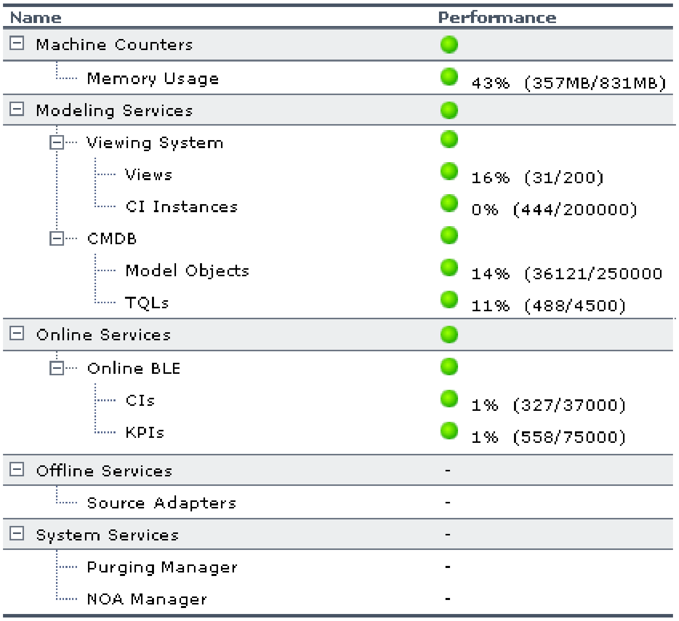
Name ▲	Configuration	Worst Resource
PLATFORM02	All Services	● 64%
PLATFORM03	All Services	● 35%
PLATFORM1	Modeling	● [illegible]
PLATFORM2	Online	● 0%

Worst Resource: CMDB's TQLs

Note: The offline server configuration does not report any resource status information as there are currently no monitored resources for the Offline Data Processing Server.

Resource Status Information in the Services Pane

In the Services pane, you can see a detailed display of all monitored server resources for the server selected in the Servers pane.



Name	Performance
⊟ Machine Counters	●
Memory Usage	● 43% (357MB/831MB)
⊟ Modeling Services	●
⊟ Viewing System	●
Views	● 16% (31/200)
CI Instances	● 0% (444/200000)
⊟ CMDB	●
Model Objects	● 14% (36121/250000
TQLs	● 11% (488/4500)
⊟ Online Services	●
⊟ Online BLE	●
CIs	● 1% (327/37000)
KPIs	● 1% (558/75000)
⊟ Offline Services	-
Source Adapters	-
⊟ System Services	-
Purging Manager	-
NOA Manager	-

- ➤ The **Name** column displays, per resource group, the services and their monitored resources.
- ➤ The **Performance** column displays:
  - ➤ for each resource group, a threshold icon indicating the status of the resource group, based on the worst child rule (the parent node inherits the status of its worst child)
  - ➤ for each service, a threshold icon indicating the status of the service, based on the worst child rule (the parent node inherits the status of its worst child)

- for each monitored resource, a threshold icon and accompanying percentage indicating the status of the resource, and the numerical representation of the percentage, based on the preset capacity limit for the resource. Note that the capacity limits differ depending on the specific deployment architecture. For example the capacity limit for CMDB TQLs is lower in a three-server deployment (the CMDB service runs on a Data Processing Server running all services) than it is in a five-server deployment (the CMDB service runs on a dedicated Modeling Data Processing Server).

The table below describes the different resource groups, services, and monitored resources whose status can be monitored from the System Health page. Note that the offline server configuration—which includes offline services and system services—does not report any resource status information as there are currently no monitored resources for the Offline Data Processing Server.

Resource Group	**Service**	**Monitored Resource**	**Description**
Machine Counters (all servers)		Memory Usage	The percentage of memory usage by the **mercury_as** process. In addition, the absolute memory usage and total memory capacity values are displayed. These are taken from the server's operating system.

Resource Group	Service	Monitored Resource	Description
Modeling Services (Modeling Data Processing Server)	**Viewing System**	CI Instances	The number of configuration item (CI) instances in service views that the server can handle simultaneously
		Views	The number of service views that the server can handle simultaneously
	CMDB	Model Objects	The number of CMDB model objects (CIs, KPIs, and so forth) that the server can handle simultaneously
		TQLs	The number of Topology Query Language (TQL) queries that the server can handle simultaneously
Online Services (Online Data Processing Server)	**Online BLE**	CIs	The number of configuration items (CIs) with associated KPIs that the server can handle simultaneously
		KPIs	The number of Key Performance Indicator (KPI) objects that the server can handle simultaneously
Offline Services (Offline Data Processing Server)	**Source Adapters**	*Resource not monitored. If service is running, the "-" character appears. If service is not running, it does not appear in the table.*	Service responsible for adding data collector entities to the CMDB

Resource Group	**Service**	**Monitored Resource**	**Description**
System Services (Offline Data Processing Server)	**Purging Manager**	*Resource not monitored. If service is running, the "-" character appears. If service is not running, it does not appear in the table.*	Service that handles data purging and partitioning
	NOA Manager	*Resource not monitored. If service is running, the "-" character appears. If service is not running, it does not appear in the table.*	Service that validates and synchronizes new tasks for the offline aggregator on an hourly or daily basis

Configuring Service Reassignment

High-level Mercury Business Availability Center administrators can use the System Health page to:

- configure Automatic Failover for the Data Processing Server. For details, see "Configuring Automatic Failover for the Data Processing Server" on page 64.
- manually reassign services to accommodate the need for server machine maintenance. For details, see "Procedure for Manually Reassigning Services" on page 69.

Configuring Automatic Failover for the Data Processing Server

The process of automatically moving services from a primary server to another server is called Automatic Failover.

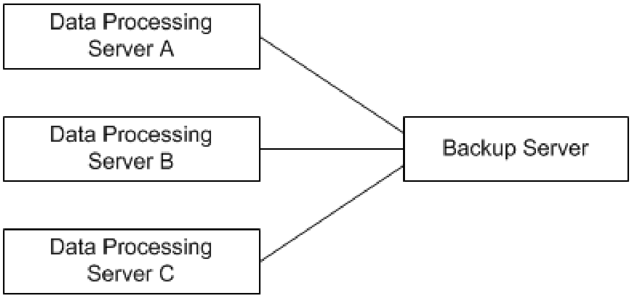
This section includes the following topics:

- "Notes and Limitations" on page 64
- "Automatic Failover Configuration" on page 66
- "Removing Automatic Failover" on page 68

Notes and Limitations

- Automatic Failover is only supported in Data Processing Servers.
- By default, Automatic Failover is not enabled.
- A primary server does not have a default backup server. A backup server must be explicitly defined. If no backup server is defined, Automatic Failover does not try to locate a suitable backup server, even if one is available.
- Each server can have only one backup server.

- Several primary servers can be assigned to the same backup server. Keep in mind, however, that if several primary servers fail simultaneously, the backup server may also fail if it exceeds its performance capacity.



- The backup server cannot have a defined backup server.
- After a primary fails and its services move to a backup, the primary, after it restarts, acts as a backup to the backup server for its original services.

  For diagram above, when Data Processing Server A fails, its services automatically move to Backup Server. When it returns online, it acts as a backup for its services which are now running on the Backup Server. Data Processing Server A, however, is not defined as a backup for Backup Server.

- The Source Adapters service (also known as the CDM service) on the Offline Data Processing Server uses the **<Mercury Business Availability Center root directory>\CMDB** directory. The CMDB directory must be moved to a separate machine for high availability purposes (that is, configured as a shared directory) to enable success of the Automatic Failover mechanism when backing up the Offline Data Processing Server. For details on configuring the CMDB directory as a shared directory, see “High Availability for the CMDB Directory” in *Deploying Servers*.
- The backup server must have the same operating system as the Data Processing server it backs up. In other words, the active server and its backup server must both be either Solaris or Windows.
- The active server and its backup server must both have the same version of Mercury Business Availability Center.

- The Mercury Business Availability Center service must be running on the backup server so that it can poll the database intermittently to know when it receives service assignments.
- If, after enabling Automatic Failover and configuring backup servers, you then disable Automatic Failover, the backup server assignments remain visible in the System Health page.
- When a designated backup server becomes the active server (starts running the services of the server it was backing up), an asterisk (*) appears beside the server name in the Servers pane. When the server ceases to act as a backup server (no longer runs the services of the server it was backing up), the asterisk is removed.

Automatic Failover Configuration

Automatic Failover for a Data Processing Server to a backup server must be configured. It is not enabled by default.

There are two steps in enabling the Automatic Failover mechanism:

- enable Automatic Failover of primary servers
- configure the backup server for primary servers

To enable Automatic Failover of primary servers:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **High Availability Controller**, and locate **Automatic Failover Enabled** entry in the High Availability Controller - General Properties table.
2. Click the edit button for **Automatic Failover Enabled.** The Automatic Failover Enabled dialog box opens.
3. Select **true** and click **Save**. The change takes effect immediately.

Note: It is recommended to keep the **Keep Alive Timeout (minutes)** default value of **20.** A lower value may give a false failure alert.

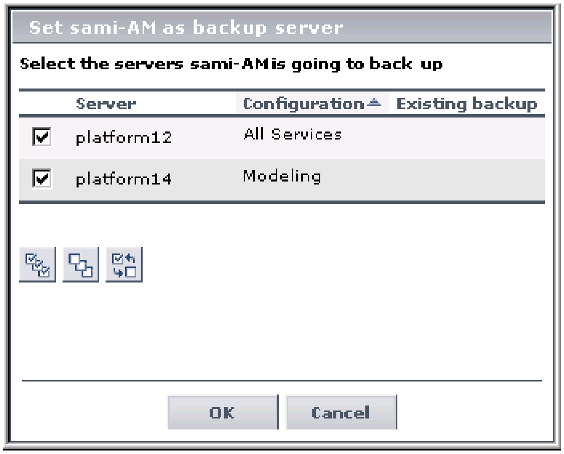
To configure the backup server for primary servers:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **System Health**.
2. In the Servers pane, choose the Data Processing tab. Click the server to be the backup server. Information about the selected server is displayed in the Services pane.
3. In the Services pane, click the Set as Backup Server button to define the server as a backup server. The Set as Backup Server dialog box opens with a list of Data Processing Servers.

   For each listed server, the following information is displayed:

   - **Server.** The server name.
   - **Configuration.** The server configuration (All services, Modeling, Online, or Offline)
   - **Existing backup.** Lists the backup server currently defined for the servers in the Server list.

4. Select the primary servers that the backup server is to back up and click **OK** to save your selections.



Set sami-AM as backup server

Select the servers sami-AM is going to back up

	Server	Configuration	Existing backup
☑	platform12	All Services	
☑	platform14	Modeling	

When a primary server exceeds the **Keep Alive Timeout** with no response, Automatic Failover automatically reassigns the services to the predefined backup server. The primary server automatically shuts down its services in order to prevent duplicate services from running. During the period of time that the backup server is running services,

---

Note: While Automatic Failover is moving services, a brief period of high CPU usage on the backup server may occur while those services start. CPU usage returns to normal once all services are running.

When the primary server becomes operational, you must manually reassign services to it from the backup server. For details on manually reassigning services, see “Procedure for Manually Reassigning Services” on page 69.

Removing Automatic Failover

Follow the procedure below to stop a server from being a backup server for some or all of the servers it is backing up.

To stop a server from being a backup server:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **System Health**.
2. In the Servers pane, choose the Data Processing tab. Click the server that you no longer want to serve as a backup server. Information about the selected server is displayed in the Services pane.
3. In the Services pane, click the Set as Backup Server button to open the Set as Backup Server dialog box.
4. Clear the check boxes beside some or all of the listed servers, as required.
5. Click **OK** to save the settings.

Procedure for Manually Reassigning Services

When there is a need to manually reassign services from one machine to another (for example, due to a resource issue on a given machine, or due to required server maintenance, or to reassign services to a primary server after its services were automatically moved to a backup server using the Automatic Failover mechanism), follow the below procedure to create and apply server reassignment tasks.

Note: The Source Adapters service (also known as the CDM service) on the Offline Data Processing Server uses the **<Mercury Business Availability Center root directory>\CMDB** directory. If the CMDB directory has not been moved to a separate machine for high availability purposes (that is, configured as a shared directory), when the Offline Data Processing Server services are manually reassigned to a different server, the CDM service will not function properly until the CMDB directory is manually copied to the new Offline Data Processing Server. For details on configuring the CMDB directory as a shared directory, see “High Availability for the CMDB Directory” in *Deploying Servers*.

To reassign services:

1. In the Servers pane, select the server whose services you want to reassign.
2. In the Services pane (right pane), click the **Move services as group** button to view the **Move services** context menu.

3 Select one of the below options. The Move Services dialog box opens.

- ➤ **Move all services.** Select to move all services from the server to a different server.
- ➤ **Move modeling services.** Select to move modeling services from the server to a different server.
- ➤ **Move offline services.** Select to move offline services from the server to a different server.
- ➤ **Move online services.** Select to move online services from the server to a different server.
- ➤ **Move system services.** Select to move system services from the server to a different server.

4 In the Move Services dialog box, select the server to which you want to reassign the selected group of services. Only servers to which the services can be moved are listed.

5 Click **OK** to move the services.

6 Monitor the status of the running tasks from the Status tab.

The Status tab displays all tasks currently running, or that have completed running during the current Web session.

Limitation: If a task does not complete (that is, the reassigned services do not start successfully), the Status tab will continue to display a status message indicating that the task is in progress. Successful reassignment can be verified in the System Health log file, **systemConsole.log**, if the log file is configured to record messages at the INFO level. For details on the log file, see “Log File” on page 71.

System Health Logging and Troubleshooting

Use the following information to troubleshoot issues, as required.

System Health Logging

All server reassignments performed via the System Health page are written to the Audit Log. In addition messages are written to a log file.

Audit Log

All services reassignments are written to the Audit Log (**Admin** > **Platform** > **Setup and Maintenance** > **Audit Log**).

To view the history of services reassignments, in the Audit Log select the **System Console** context. If required, use the up and down arrows to scroll through the entries.

Log File

Log messages are written to the log file <**Mercury Business Availability Center root directory**>**\log\systemConsole.log**. The type of messages is dependent on the level of logging enabled. By default, only errors are written to this log. For details on changing log level, see "Changing Log Levels" in *Reference Information*.

System Health Troubleshooting

Problem: Mercury Business Availability Center servers installed and running in a distributed architecture appear as unavailable in the Servers pane.

Problem Cause: To determine server availability, Mercury Business Availability Center pings the servers according to the name registered in the SERVERS table in the database. In certain environments, the host machine performing the ping requires the target machine's IP (and not its machine name) but does not know the IP. Thus the ping fails and the machine is reported as unavailable.

Solution: Map the names of all Mercury Business Availability Center server machines (Centers, Core, and Data Processing) to their corresponding IPs in the **C:\windows\system32\drivers\etc\hosts** file (path may vary depending on Windows installation) on the Centers Server machine. If there are multiple Centers Server machines and/or Centers Server machines behind a load balancer, perform the above procedure on all machines. Note that the left column is for IP addresses and the right column is for machine names.

6

Infrastructure Settings

Note to Mercury Managed Services customers: Mercury Operations administers these pages and the interface is hidden from the view of customers, apart from customer super users.

You can configure Mercury Business Availability Center settings to meet your organization's specifications for the platform and its applications. You configure most Infrastructure Settings directly within the Administration Console.

Understanding the Infrastructure Settings Manager

Mercury Business Availability Center enables you to define and configure many variables and xml files that determine how the platform and its applications run. Most of the configuration is done in the Infrastructure Settings Manager, which consolidates the settings taken from various files on the servers onto one accessible page in Platform Administration. For details on settings that are configured directly in files, see “Infrastructure Configurations Not Performed in the Infrastructure Settings Manager” on page 77.

Note: Many of the settings in the Infrastructure Settings Manager should not be modified without first consulting Mercury Customer Support or your Mercury Services representative. Modifying certain settings can adversely affect the performance of Mercury Business Availability Center.

Throughout the documentation, there are descriptions of specific settings that are related to documented tasks. In these cases, edit the settings according to the instructions given within the description or the procedure.

In the Infrastructure Settings Manager, you can select different contexts from which to view variables and/or XML format files. These are split into two groups:

Applications

This list includes those contexts that determine how the various applications running within Mercury Business Availability Center behave. These include:

- Dashboard Application
- End User/System Availability Management
- Service Level Management

Foundations

This list includes those contexts that determine how the different areas of the Mercury Business Availability Center foundation run.

- Alerting
- Auto Correlation
- Business Availability Center Interface
- CMDB
- Connection Pool
- Data Engine Open API
- Generic Data Engine
- Generic Data Engine Open API
- LDAP Authentication
- Monitor Administration
- NTP Time
- Offline Aggregator
- Offline Business Logic Engine
- Online Business Logic Engine
- Platform Administration
- Production Analysis
- Reporting
- SAP
- Scheduled Reports
- Security
- SiteScope Events
- Snapshot Converter (HTML, SAP, QTP, Citrix)
- Sources Configuration
- System Console
- Third-Party Components
- Vertical
- View Explorer

Editing Infrastructure Settings

You edit infrastructure settings within the Setup and Maintenance tab of Platform Administration.

To edit infrastructure variable values:

1 In Platform Administration, select **Setup and Maintenance** > **Infrastructure Settings.** The Infrastructure Settings Manager page opens.

2 Select the context for viewing the variables or XML format files you want to edit:

➤ **Applications.** Select if you are editing variables for one of the Mercury Business Availability Center applications. For a detailed list, see “Applications” on page 74.

➤ **Foundations.** Select if you are editing variables for the Mercury Business Availability Center foundation. For a detailed list, see “Foundations” on page 74.

➤ **All.** Select to view all the variables and xml files for both Applications and Foundations.

3 Locate the variable you want to edit within the relevant context table and click the edit button next to the currently defined value. A dialog box opens displaying the variables value as an editable field.

4 Edit and save the new value using one of the following options:

➤ To change the value, edit the value directly in the value field and click **Save**.

➤ To set the value back to the platform’s default value, click **Default** and then **Save**.

Infrastructure Configurations Not Performed in the Infrastructure Settings Manager

The following infrastructure configuration procedures are not performed in the Infrastructure Settings Manager:

- Disabling Automatic Adjustment of Daylight Savings Time in Mercury Business Availability Center – for details, see below
- Modifying the Ping Time Interval – for details, see page 78
- Modifying the Location and Expiration of Temporary Image Files – for details, see page 79

Disabling Automatic Adjustment of Daylight Savings Time in Mercury Business Availability Center

When running Mercury Business Availability Center servers on Windows NT or Windows 2000 machines, it might be necessary to modify the way the machines and Mercury Business Availability Center handle the changeover to Daylight Saving Time (DST). It might also be necessary to modify the way DST is handled on the database server machine(s) on which Mercury Business Availability Center databases are located.

Note: If you are running Mercury Business Availability Center servers or databases on a Solaris platform, it is not necessary to modify settings.

DST Handling on Server Machines

It might be necessary to disable—on the machines running Mercury Business Availability Center servers—the operating system setting that automatically adjusts the machine clock for Daylight Saving Time (DST), and instead to manually adjust the machine clock when DST begins. This might be required when Mercury Business Availability Center servers are located in a geographic region where the exact date that DST begins differs from season to season, in multiple geographic regions whose dates of changeover to DST differ, or in multiple geographic regions some of which do not use DST.

DST Handling on Database Server Machines

It might be necessary to always leave the machine clock on the database server machine(s) on which the databases are located in Standard time (by disabling the operating system setting that automatically adjusts the machine clock for DST, and not adjusting the time manually for DST). This might be required when users are located in multiple geographic regions whose dates of changeover to DST differ from each other and/or that of the region where the database server is located.

If you choose to always leave the machine clock on the database server in Standard time, you must modify a setting in Mercury Business Availability Center so that Mercury Business Availability Center and the database server remain synchronized during DST.

To modify DST handling for Mercury Business Availability Center databases:

1. On the Centers Server machine, open the file **<Centers Server root directory>\conf\topaz.config** in a text editor.
2. Search for the line:

   ```
   ## Daylight saving time fix
   ```
3. Delete the comment marker (#) from the line:

   ```
   daylightsaving.database.adapts=true
   ```
4. Save the **topaz.config** file, and restart the Mercury Business Availability Center service on the Centers Server machine.

   If, in the future, you re-enable the operating system setting that automatically adjusts the machine clock's time zone for DST, add back the comment marker to the above line.

Modifying the Ping Time Interval

You can modify the time interval after which the Mercury Business Availability Center Web site pings the server to refresh a session.

To modify the ping time interval:

1. Open the file **<Centers Server root directory>\conf\settings\website.xml** in a text editor.

2 Search for the parameter: **user.session.ping.timeinterval**.

3 Change the value (120, by default) for the ping time interval. Note that this value must be less than half of the value specified for the session timeout period (the previous value defined in the file).

4 Restart the Mercury Business Availability Center service on the Centers Server machine.

If you have multiple Centers Server machines, repeat this procedure on all the machines.

Modifying the Location and Expiration of Temporary Image Files

When you generate a report in Mercury Business Availability Center applications, or when Mercury Business Availability Center automatically generates a report to send via the scheduled report mechanism, images (for example, of graphs) are created. Mercury Business Availability Center saves these images, for a limited period of time, in temporary directories on the Centers Server machine(s) on which the images are generated.

You can modify the following settings related to these images:

- the path to the directory in which the temporary image files are stored – for details see page 79
- the length of time that Mercury Business Availability Center keeps temporary image files before removing them – for details see page 85
- the directories from which temporary images are removed – for details see page 88

You modify temporary image file settings in the **<Centers Server root directory>\conf\topaz.config** file.

Modifying the Directory in Which Temporary Image Files Are Stored

You can modify the path to the directory where Mercury Business Availability Center stores generated images used in scheduled reports and Analytics. For example, you might want to save generated images to a different disk partition, hard drive, or machine that has a greater storage capacity than the partition/drive/machine on which the Centers Server machine is installed.

In certain cases, you might be required to modify the path to the directory in which images are stored. For example, if Mercury Business Availability Center reports are accessing the Centers Server machine via a virtual IP—typical when there are multiple Centers Server machines running behind a load balancer in the Mercury Business Availability Center architecture—since the load balancer could send requests to any of the Centers Server machines, the image files need to be in a common location that is configured on all the Centers Server machines and shared among them. For more details, see "Accessing Temp Directory with Multiple Centers Server Machines" on page 81.

To support a shared location for temporary images in a Windows environment, the following configuration is recommended:

- All Centers Servers—and the machine on which the shared image directory is defined, if different from the Centers Servers—should be on the same Windows domain.
- The IIS virtual directory should be configured to use the credentials of an account that is a member of the domain users group.
- The account for the virtual directory should be given read/write permissions on the shared image directory.

Note: If your server configuration requires placing servers on different Windows domain configurations, contact Mercury Customer Support.

To support a shared location for temporary images in a Solaris environment, the following configuration is recommended:

- The shared directory must be mounted with read/write access from other machines.
- The Mercury Business Availability Center user account must have read/write access on the shared directory.

To modify the path to the directory holding temporary image files:

1. Open the file **<Centers Server root directory>\conf\topaz.config** in a text editor.
2. Search for the parameter **images.save.directory.offline**.
3. Remove the comment marker (#) from the line that begins **#images.save.directory.offline=** and modify the value to specify the required path.

Note: In Windows environments, use UNC path syntax (\\\\server\\path) when defining the path. In a Solaris environment, use forward slashes (/) and not backslashes (\) when defining the path.

---

4. Save the **topaz.config** file.
5. Restart the Mercury Business Availability Center service on the Centers Server machine.
6. Repeat the above procedure on all Centers Server machines.
7. Map the newly defined physical directory containing the images to a virtual directory in the Web server on all Centers Server machines. For details, see the next section.

Accessing Temp Directory with Multiple Centers Server Machines

If you define a custom path to temporary images (as defined in the **images.save.directory.offline** parameter), you must map the physical directory containing the images to a virtual directory in the Web server on all Centers Server machines.

To configure the virtual directory in IIS:

1 Rename the default physical directory containing the temporary scheduled report images on the Centers Server machine.

For example, rename:

```
<Centers Server root
directory>\AppServer\webapps\site.war\Imgs\chartTemp\offline
```

to

```
<Centers Server root
directory>\AppServer\webapps\site.war\Imgs\chartTemp\old_offline
```

2 In the IIS Internet Services Manager on the Centers Server machine, move to **Default Web site** > **Topaz** > **Imgs** > **ChartTemp**.

The renamed offline directory appears in the right frame.

3 In the right frame, right-click and select **New** > **Virtual Directory**. The Virtual Directory Creation Wizard opens. Click **Next**.

4 In the Virtual Directory Alias dialog box, type offline in the Alias box to create the new virtual directory. Click **Next**.

5 In the Web Site Content Directory dialog box, type or browse to the path of the physical directory containing the temporary images (the path defined in the **images.save.directory.offline** parameter). Click **Next**.

6 If the physical directory containing the temporary images resides on the local machine, in the Access Permissions dialog box, specify Read and Write permissions.

If the physical directory containing the temporary images resides on a machine on the network, in the User Name and Password dialog box, enter a user name and password of a user with permissions to access that machine.

7 Click **Next** and **Finish** to complete Virtual Directory creation.

8 Restart the Mercury Business Availability Center service on the Centers Server machine.

9 Repeat the above procedure on all Centers Server machines.

To configure the virtual directory on Apache HTTP Web Server:

1. Rename the default physical directory containing the temporary scheduled report images on the Centers Server machine.

   For example, rename:

   <Centers Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\offline

   to

   <Centers Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\old_offline

2. Open the Apache configuration file <**Centers Server root directory**\WebServer\conf\httpd.conf with a text editor.

3. Map a virtual directory named **offline** to the physical location of the common directory by adding the following line to the file:

   ```
   Alias /Imgs/chartTemp/offline <shared_temp_image_directory>
   ```

   where <shared_temp_image_directory> represents the path to the physical directory containing the temporary scheduled report images (the path defined in the **images.save.directory.offline** parameter).

4. Save the file.

5. Restart the Mercury Business Availability Center service on the Centers Server machine.

6. Repeat the above procedure on all Centers Server machines.

To configure the virtual directory on Sun Java System Web Server:

1. Rename the default physical directory containing the temporary scheduled report images on the Centers Server machine.

   For example, rename:

   <Centers Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\offline

   to

   <Centers Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\old_offline

2. Open the Sun Java System Web Server configuration file <**Sun Java System Web Server installation directory\server\<server_nam>\config\obj.conf** with a text editor.

3. Add the following line inside the <Object name=default> directive (but before the line **NameTrans fn="pfx2dir" from="/Imgs" dir="ProductDir/Site Imgs/"**, if it exists, and before the line **NameTrans fn=document-root root="$docroot"**):

   NameTrans fn="pfx2dir" from=”/topaz/Imgs/chartTemp/offline" dir="<shared_temp_image_directory>"

   where <shared_temp_image_directory> represents the path to the physical directory containing the temporary scheduled report images (the path defined in the **images.save.directory.offline** parameter).

4. Save the file.

5. Restart the Sun Java System Web Server on the Centers Server machine.

6. Repeat the above procedure on all Centers Server machines.

Modifying the Length of Time that Mercury Business Availability Center Keeps Temporary Image Files

You can modify settings that control how long Mercury Business Availability Center keeps temporary image files generated by the Centers Server machine, before removing them from the defined temporary directories. You can modify settings for the following directories in the <**Mercury Business Availability Center Centers Server root directory**>**conf****topaz.config** file:

Directory Setting	Description
remove.files.0.path=../../AppServer/webapps/site.war/Imgs/chartTemp/offline	Path to images created when generating scheduled reports and Analytics reports
remove.files.1.path=../../AppServer/webapps/site.war/Imgs/chartTemp/online	Path to images created when generating reports in Mercury Business Availability Center applications
remove.files.3.path=../../AppServer/webapps/site.war/snapshots	Path to images created by the Snapshot on Error mechanism and viewed in Error Summary reports

For the above temporary image directories, you can modify the following settings:

- **remove.files.directory.number=<number of directories>**

  Specifies the total number of directories for which you are defining settings.

- **remove.files.<num_of_path>.path=<path to directory>**

  Specifies the path to the directory that contains the files you want to remove. For the default directories that remove temporary image files, these values must match the **images.save.directory.online** and **images.save.directory.offline** parameters, also defined in the topaz.config file.

Note: In Windows environments, use UNC path syntax (\\\\server\\path) when defining the path. In Solaris environments, use forward slashes (/) only when defining the path.

- **remove.files.<num_of_path>.expirationTime=<file expiration time in sec>**

  Specifies the time, in seconds, that Mercury Business Availability Center leaves a file in the specified directory. For example, if you specify "3600" (the number of seconds in 1 hour), files older than one hour are removed.

  Leave this setting empty if you want Mercury Business Availability Center to only use maximum size criteria (see below).

- **remove.files.<num_of_path>.maxSize=<maximum size of directory in KB>**

  Specifies the total size to which the defined directory can grow before Mercury Business Availability Center removes files. For example, if you specify "100000" (100 MB), when the directory exceeds 100 MB, the oldest files are removed in order to reduce the directory size to 100 MB.

  If you also define a value in the **remove.files.<num_of_path>.expirationTime** parameter, Mercury Business Availability Center first removes expired files. Then Mercury Business Availability Center removes additional files if the maximum directory size limit is still exceeded, deleting the oldest files first. If no files have passed their expiration time, Mercury Business Availability Center only removes files based on the maximum directory size criteria.

  This parameter is used in conjunction with the **remove.files.<num_of_defined_path>.deletePercents** parameter (see below), which instructs Mercury Business Availability Center to remove the specified percentage of files, in addition to the files removed using the **remove.files.<num_of_path>.maxSize** parameter.

  Leave this and the **remove.files.<num_of_defined_path>.deletePercents** settings empty if you want Mercury Business Availability Center to only use the expiration time criterion.

- **remove.files.<num_of_path>.deletePercents=<percent to remove>**

  Specifies the additional amount by which Mercury Business Availability Center reduces directory size—expressed as a percentage of the maximum allowed directory size—after directory size has been initially reduced according to the **remove.files.<num_of_path>.maxSize** parameter. Mercury Business Availability Center deletes the oldest files first.

  Leave this and the **remove.files.<num_of_path>.maxSize** settings empty if you want Mercury Business Availability Center to only use the expiration time criterion.

- **remove.files.<num_of_path>.sleepTime=<thread sleep time in sec>**

  Specifies how often Mercury Business Availability Center runs the mechanism that performs the defined work.

Example

Mercury Business Availability Center is instructed to perform the following work once every 30 minutes: Mercury Business Availability Center first checks whether there are files older than 1 hour and, if so, deletes them. Then Mercury Business Availability Center checks whether the total directory size is greater than 250 MB, and if so it reduces directory size to 250 MB by removing the oldest files. Finally, Mercury Business Availability Center reduces the total directory size by 50% by removing the oldest files. As a result, Mercury Business Availability Center leaves files totaling 125 MB in the directory.

```
# remove files older than 1 hour (3600 sec.)
remove.files.0.expirationTime=3600
# reduce folder size to 250 MB
remove.files.0.maxSize=250000
# remove an additional 50% of max. folder size (125 MB)
remove.files.0.deletePercents=50
# perform work once every 30 min. (1800 sec)
remove.files.0.sleepTime=1800
```

Note: You can configure the file removal mechanism to remove files from any defined directory. You define the parameters and increment the index. For example, to clean out a temp directory, you would specify **6** instead of **5** for the number of directories in the **remove.files.directory.number** parameter; then you would define the directory's path and settings using the index value **4** (since 0-4 are already being used by the default settings) in the **num_of_path** section of the parameter. Do not use this mechanism to remove files without first consulting with your Mercury Customer Support representative.

To modify the default settings:

1. Open the file <**Mercury Business Availability Center Centers Server root directory**>**\conf\topaz.config** in a text editor.

   Tip: Before modifying the values, back up the file or comment out (using #) the default lines so that the default values are available as a reference.

2. Modify the settings as required.
3. Save the **topaz.config** file.
4. Restart the Mercury Business Availability Center service on the Centers Server machine.
5. Repeat the above procedure on all Centers Server machines.

Specifying the Directories from Which Temporary Image Files Are Removed

By default, temporary images files are removed from the root path of the specified directory. However, you can also configure Mercury Business Availability Center to remove temporary image files from the subdirectories of the specified path.

To configure Mercury Business Availability Center to remove temporary images files from subdirectories:

1. Open the file <**Centers Server root directory**>\conf\topaz.config in a text editor.
2. Insert the following line after the specified path's other settings (described in the previous section):

   ```
   remove.files.<num_of_path>.removeRecursively=yes
   ```

3. Save the **topaz.config** file.
4. Restart the Mercury Business Availability Center service on the Centers Server machine.
5. Repeat the above procedure on all Centers Server machines.

7

Audit Log

Mercury Business Availability Center enables you to view a log of all the actions performed by different users accessing the platform.

Understanding the Audit Log

You use the audit log to keep track of different actions performed by users in the system. You can track according to the following contexts in the audit log:

- **Alert Administration.** Displays actions related to adding, modifying, deleting, enabling and disabling alerts, as well as registering and unregistering alert recipients.
- **CI Status Alert Administration.** Displays actions related to creating alert schemes for a configuration item (CI) status alert.
- **Customer Package Management.** For Mercury Managed Services only. Displays actions related to modifying package information such as: package location information, package host information for Client Monitor, general package properties, Business Process Monitor package properties, SiteScope package properties or Client Monitor package properties.
- **Dashboard Administration.** Displays actions related to configurations made in the Dashboard Administration

- **Data Collector Maintenance.** Displays actions related to removing or upgrading Business Process Monitors and SiteScopes, and removing, upgrading, or uninstalling Client Monitors.
- **Database Management.** Displays actions related to creating, deleting, and modifying users and passwords for profile databases, as well as modifying the status of the Purging Manager.
- **Deleted Entities.** Displays actions related to adding and deleting data collectors from Monitor Administration. These are Business Process profiles, Client Monitor profiles, Real User Monitor engines, and SiteScope monitors.
- **Downtime/Event Scheduling.** Displays actions related to creating and modifying downtime and scheduled events.
- **Infrastructure Settings.** Displays actions related to modifying any of the infrastructure settings.
- **IT World (IT Universe) Configuration.** Displays actions, including editing, updating, and removing CIs and relationship, performed in the IT Universe Manager application.
- **Monitor Administration (Business Process Monitor).** Displays actions related to profile management and configuration, including starting and stopping profiles, adding and deleting transaction monitors, modifying scheduling, defining and modifying hosts, adding and deleting WebTrace addresses, and modifying transaction thresholds.
- **Monitor Administration (Client Monitor).** Displays actions related to profile management and configuration, including starting and stopping profiles, adding and deleting transaction monitors, modifying scheduling, defining and modifying hosts, adding and deleting traceroute addresses, and modifying transaction thresholds.
- **Monitor Administration (Real User Monitor).** Displays actions related to Real User Monitor management and configuration, including the addition and deletion of Real User Monitor probes, servers, and host groups, and the configuration and deletion of pages, transactions, and end users.
- **Monitor Administration (SiteScope).** Displays actions related to profile management and configuration, including starting and stopping profiles, adding and deleting monitors, modifying monitors and groups, editing preferences, and configuring alerts.

- **Notification Template Administration.** Displays actions related to modifying open ticket information, ticket settings, closed tickets, ticket templates, and subscription information: notification types (locations or general messages), and recipients.
- **Permissions Management.** Displays all actions related to assigning permissions, roles, and permissions operations for resources onto users and user groups.
- **Recipient Administration.** Displays actions related to modifying information about the recipients of audit logs.
- **Scheduled Report Administration.** Displays actions related to modifying the reporting method and schedule of reported events.
- **Script Repository.** For Mercury Managed Services only. Displays actions related to modifying the type of verification of Business Process Monitor scripts, and verification subscription information.
- **Service Level Management Configuration.** Displays actions related to service level agreements performed in the Service Level Management application. For a list of the audited actions, see "Using the Audit Log" on page 94.
- **SLA Status Alert Administration.** Displays actions related to creating, modifying, or deleting SLA alerts.
- **System Console.** Displays all services reassignments performed in the System Health interface to resolve system resource issues.
- **User Defined Reports.** For Mercury Managed Services only. Displays actions related to the creation and modification of custom reports.
- **User/Group Management.** Displays actions related to adding, modifying, and deleting users and user groups.
- **View Manager.** Displays actions related to KPIs such as adding a KPI, editing a KPI, and deleting a KPI. Additionally, it displays actions related to changing the "Save KPI data over time for this CI" and the "Monitor changes" options.

Using Filters in the Audit Log

When you select one of the above categories from the Context list, the following information is displayed in the Audit Log table:

- **Modification Date.** Displays the date of the listed action
- **Modified By**. Displays the user who performed the listed action
- **Actions.** Displays a detailed description of the action

Using the Audit Log

You access the audit log from the Audit Log page, available from the Setup and Maintenance menu of Platform Administration.

To use the audit log:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Audit Log.** The Audit Log page opens.
2. Select a context using the **Context** filter.
3. Where relevant, select a profile from the list. Mercury Business Availability Center updates the table with the relevant information.
4. If desired, click the **Auditing Filters** link and specify filter criteria. The following filters are available:

    - **User.** Specify a user in the system to view actions performed by only that user.
    - **Containing text.** Specify a text string that the action must contain to be displayed.
    - **Start after** and **End before.** Specify a starting and ending time period to view actions for only that period. Click the **more** button to open the Calendar dialog box where you can select a date.

    Click **OK**. Mercury Business Availability Center updates the table with the relevant information.

5. If required, use the **Previous Page** and **Next Page** arrows to move through the audit log.

8

System Tickets for Mercury Managed Services

Note: The System Ticket page is available only to Mercury Managed Services customers.

System Tickets for Mercury Managed Services allows you to view open tickets for your locations, view archived tickets to search for previous problems, and select the type of notification you want to receive about your locations.

About System Tickets

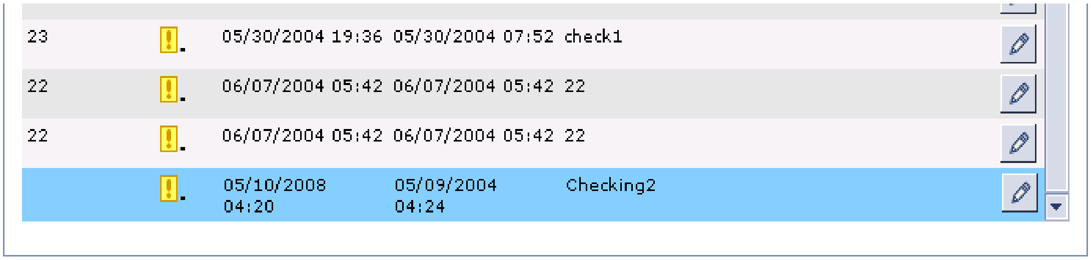
Mercury Managed Services operators use tickets to communicate with Mercury Managed Services customers when the customer’s system encounters problems or to inform the customer about scheduled maintenance for one or more locations in the customer package.

Understanding System Tickets

System Tickets uses special icons to display a ticket's severity:

Icon status	Description
i	Informational
!	Minor
!	Critical

System Tickets that are related to scheduled maintenance are highlighted with a blue background.



23	!	05/30/2004 19:36	05/30/2004 07:52	check1
22	!	06/07/2004 05:42	06/07/2004 05:42	22
22	!	06/07/2004 05:42	06/07/2004 05:42	22
	!	05/10/2008 04:20	05/09/2004 04:24	Checking2

Scheduled maintenance usually consists in installing a patch or performing maintenance on the Mercury Managed Services servers.

Viewing Open Tickets

Mercury Managed Services customers work with a package that was defined according to their license. The package includes a number of pre-defined locations. The System Tickets page displays information only about the tickets that occur at the customer's own locations.

You can view all the open tickets and their severity.

To view the open tickets:

1 In Platform Administration, click **Setup and Maintenance** > **System Tickets** to open the **System Tickets** area with the **Open Tickets** tab selected.

2 Select the type of ticket you want to display in the **Ticket Type** list. The type can be: **Location Ticket** or **General Maintenance Ticket**.

   The following information is displayed:

   ➤ **SR#.** The service request number.

   ➤ **Severity.** The severity can be: informational, minor, or critical (for more details, see "Understanding System Tickets" on page 96).

   ➤ **Start time.** The starting time of the ticket.

   ➤ **Last update.** The date and time of the last update to the ticket.

   ➤ **Details.** The ticket description.

Note: Scheduled events are highlighted with a blue background. For more details, see "Understanding System Tickets" on page 96.

Viewing Archived Tickets

You use the archive to view the tickets that were closed by the Mercury Managed Services operator or to search for previous problems.

When the Mercury Managed Services operator changes the status of a ticket to closed, the ticket is automatically moved from the Open Tickets tab to the Archive tab. The Mercury Managed Services operator can also move the ticket back from the Archive tab to the Open Tickets tab by changing the status back to open.

To view the ticket archive:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **System Tickets** to open the **System Tickets** area. Click the **Archive** tab.

2 Select the type of ticket you want to display in the **Ticket Type** box.

For more details about the displayed information, see "Viewing Open Tickets" on page 96.

3. Use the arrows to scroll the log.

Modifying Recipient Settings

Mercury Managed Services customers can set specific recipients to whom specific types of tickets should be sent.

You can view, specify, or modify the recipients to whom specific types of tickets should be sent.

Viewing, Specifying, or Modifying the Settings

You can specify whether you want the recipient to receive information about the customer's location tickets, general messages tickets, or both.

To view, specify, or modify the settings:

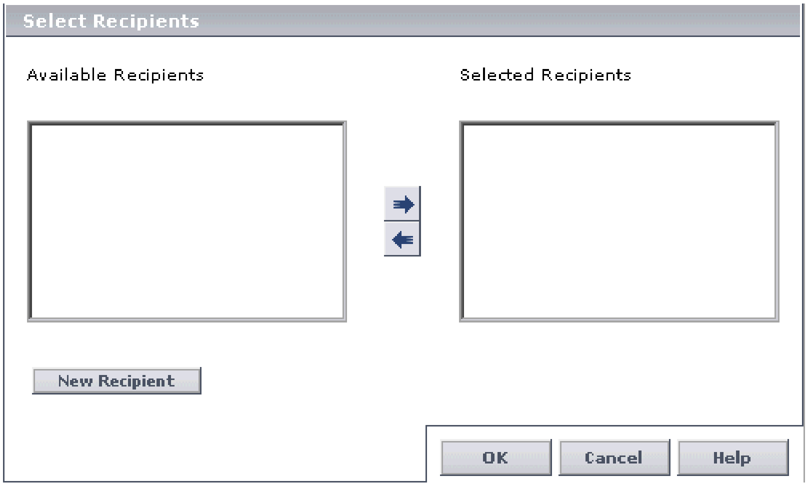
1. In Platform Administration, click **Setup and Maintenance** > **System Tickets** to open the **System Tickets** area. Click the **Settings** tab.
2. Select **Locations** to have the recipients listed in the recipient box receive all location tickets related to the customer with whom they are associated.
3. Select **General Messages** to have the recipients listed in the recipient box receive all general message tickets related to the customer with whom they are associated.
4. Click **Recipients** to select recipients to be listed in the recipient box. For more details, see "Assigning Recipients" on page 99.
5. Click **Save** to save the settings.

Assigning Recipients

You can select or clear the recipients that will receive the type of ticket information defined above from among the customer existing recipients.

To select or clear recipients:

1 In the **Settings** tab, click **Recipient** to open the **Select Recipients** area.



2 Select the required recipients in the **Available Recipients** box.

3 Click the left-to-right arrow to move the selected recipient to the **Selected Recipients** box, or vice-versa to remove recipients from the **Selected Recipients** box.

4 Click **New Recipient** to create new recipients. For more details, see “Configuring and Selecting Recipients” on page 181.

5 Click **OK** to save the recipient settings.

Part II

Data Collection

9

Data Collector Maintenance

Note to Mercury Managed Services customers: Mercury Operations administers these pages and the interface is hidden from your view. The Client Monitor tab in the Data Collector Maintenance page is available to customer superusers, but without host management operations (that is, without the **Cleanup** option).

You can perform ongoing maintenance tasks on the data collectors installed with your platform to suit the changing requirements of your organization.

About Data Collector Maintenance

The Mercury Business Availability Center platform includes installable components that provide data collection capabilities. The Data Collector Maintenance page enables you to manage and maintain the data collectors in your platform.

Note: Data collectors can be installed from the Downloads page in Platform Administration. For details on downloading, see "Downloads" on page 3.

The Data Collector Maintenance page is available in the Data Collection tab of Platform Administration and displays the current data collector instances registered in the management database for each data collector type. The page is divided into 4 tabs representing the following types of data collectors:

- SiteScope
- Business Process Monitor
- Client Monitor
- Real User Monitor

You use the Data Collector Maintenance page to:

- view a detailed list of all data collectors in your platform
- upgrade Business Process Monitor instances
- remove a Business Process Monitor instance
- manage Client Monitor hosts
- track the status of upgrade, remove, and uninstall processes
- view a data collector's current properties

You can also view the status of a maintenance action that is still in progress, such as the removal or upgrade of a data collector, and link to the administration site of the data collector (except for Client Monitors).

Understanding the Data Collector Maintenance Page

The Data Collector Maintenance page includes the following information, depending on which data collector tab is selected:

- a location filter at the top of the page, which enables you to filter the list of data collectors by host location
- a check box beside each data collector (or containers and groups for Client Monitor), which must be checked to select the data collector, container, or group for various host management options.
- a list, by host name, of all data collectors registered in the management database for the type selected.

Note: A Business Process Monitor instance is identified by the combination of the **Host Name** and **Location Name**. Both the host name and location name are defined by the user when setting up a Business Process Monitor instance. For details, see “Business Process Monitor Host Page” in *Business Process Monitor Administration*.

- IP address of the data collector
- the location defined for the SiteScopes and Business Process Monitor instances
- the version, including build number for SiteScope, of the data collector software installed
- the last time the data collector pinged the management database
- a column indicating whether the data collector is removable (for details, see “Removing a Business Process Monitor” on page 108)
- a details button which opens the data collector’s information page
- a link to the data collector’s administration site (except for Client Monitors), enabling you to perform administrative tasks on the data collector directly from this page

- for Client Monitor, buttons for creating and editing containers and groups for Client Monitor hosts
- clear all, select all, and invert selection buttons to clear all selections, select all data collectors, and to invert selection (clear data collectors that were selected and select data collectors that were not selected)
- a **Refresh** button

Upgrading a Business Process Monitor

Mercury Business Availability Center enables you to upgrade the version of your data collector software remotely from the Administration Console. The upgrade is performed silently, directly on the selected data collector. You do not have to be on the machine on which the data collector is installed.

When an updated version of the data collector software becomes available or when a patch is released, you can upgrade all the data collectors at one time.

The upgrade is done by supplying a URL address for the setup file. You obtain the setup file from your Mercury Customer Support representative.

Note: If the Mercury Business Availability Center server is using a server-side certificate, there are additional steps for performing the remote upgrade. For details, see “Auto Upgrading Data Collectors Remotely when Using Basic Authentication” in *Hardening the Platform*.

Note: When you are running the Business Process Monitor and/or Mercury Business Availability Center from behind a proxy server, you can access the Business Process Monitor installation file from a remote location only when the installation file is stored on the Mercury Business Availability Center server machine. The remote installation uses the Business Process Monitor connection to Mercury Business Availability Center and passes the proxy. You cannot access the installation file behind any other proxy.

To upgrade your data collector software:

1 Select **Admin** > **Platform** > **Data Collection**. Choose **Data Collector Maintenance**. The Data Collector Maintenance page opens.

2 Select the check box for the data collector instance you want to upgrade.

To make your selections, you can also use the buttons at the bottom of the page for, **Select All**, **Clear All**, and **Invert Selection .**

3 Click **Upgrade** at the bottom of the page. The Upgrade dialog box opens listing those data collectors that were selected in step 2.

These data collectors are listed according to those that are available for the upgrade action and those that cannot be upgraded, along with a reason why the upgrade cannot be performed on each.

4 In the Upgrade dialog box, enter the **Setup file URL** address. You obtain the setup file from your Mercury Customer Support representative. Enter either an HTTP/HTTPS URL or the path to the upgrade file, including the file name, that was copied onto the local machine.

5 If accessing the location of the setup file requires authentication, select **Use Basic Authentication**.

6 If you selected **Use Basic Authentication**, enter the appropriate **User Name**, **Password**, and **Domain**.

7 Click **Start Upgrade**. The Actions Status window opens, and the upgrade process continues there. For details of the rest of the procedure, see “Tracking Actions Status” on page 116.

Removing a Business Process Monitor

Using the Data Collector Maintenance page to remove a data collector removes it from the management database. This may be required if a specific data collector instance becomes obsolete.

Removing a data collector deletes it only from the management database, not from the profile database. For example, a removed Business Process Monitor instance that was added to a profile at least once, no longer appears in the list of available hosts that is displayed when creating profiles. However, the location of the removed host still appears in different areas of Mercury Business Availability Center (for example, in reports and filters). If you do not want a removed Business Process Monitor instance to appear in reports, use report filters to remove the location associated with the data collector. For details on configuring report filters, see "Report Filters" in *Application Configuration and Administration*, and "Configuring Report Filters Globally" on page 127.

Mercury Business Availability Center enables you to remove only those data collectors that are no longer in use according to the following criteria:

- **Business Process Monitor –** The Business Process Monitor is not associated with any profiles or the Business Process Monitor has not pinged the database server hosting the management database for at least 24 hours. To stop the Business Process Monitor from pinging the database server, you must shut down the Business Process Monitor.

To remove a Business Process Monitor instance:

1. Select **Admin** > **Platform** > **Data Collection**. Choose **Data Collector Maintenance**. The Data Collector Maintenance page opens.
2. If required, filter the list using the **Location** filters to view specific locations from which you want to remove data collector instances.
3. Select the check box for the data collector instance you want to remove, checking the removable column to see if it is removable.

   If the Removable column has **No** listed for this instance, you can click the information button to see why the data collector is not removable. A dialog box displaying information on the data collector opens. For details, see "Viewing Data Collector Information" on page 117.

4 Click **Remove**, and confirm that you want to remove the instance(s).

To refresh the list of services:

Click the **Refresh** button at the bottom of the page.

Managing Client Monitor Hosts

Client Monitor transaction monitors and traceroutes are assigned to run on containers or groups of Client Monitor hosts. For details on assigning transaction monitors and traceroutes, see “Managing Business Process Profiles and Creating Client Monitor Profiles” in *End User Management Data Collector Configuration*.

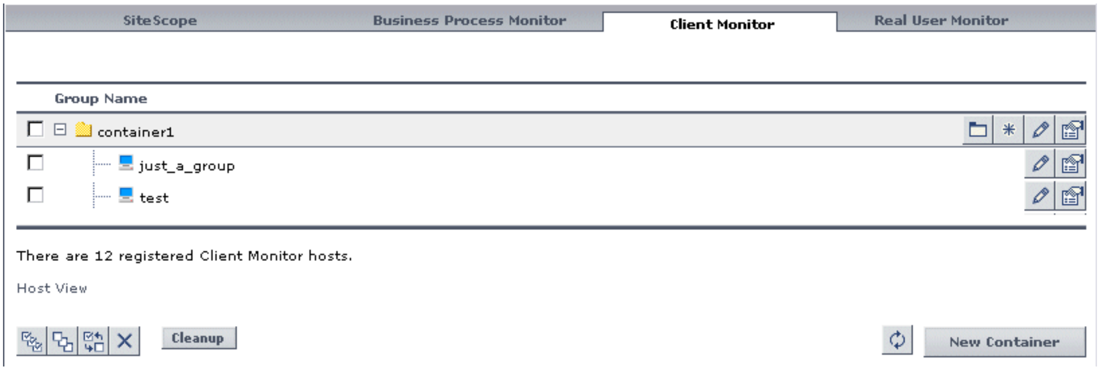
You use the Client Monitor tab in the main Data Collector Maintenance page to create, maintain, and view the containers and groups of Client Monitor hosts. The Client Monitor tab contains the following views:

- Group View. Used to create, maintain and view the containers and groups of Client Monitor hosts.
- Host View. Used to view details of individual Client Monitor hosts.

Group View

New Container

The top part of the Group view displays a tree showing all the containers and groups of Client Monitor hosts. Containers can include both sub containers and groups. To create a new container, click the **New Container** button at the bottom of the screen. The New Container dialog box opens. Enter the name of the container and click **OK** to save it. The new container appears in the tree.



There are 12 registered Client Monitor hosts.

Next to each container or group is a check box that can be checked to select the container or group for being cleaned up or deleted. You can also make your selections by using the buttons at the bottom of the page for **Select All**, **Clear All**, and **Invert Selection** . When a container is selected, all sub containers and groups within the selected container are automatically selected as well and cannot be deselected individually, although they can be selected individually.

For each container, there are buttons to create a new sub container, create a new group, edit the container, and view the container details. For each group, there are buttons to edit the group and view the group details.

The bottom part of the Group view includes buttons for deleting containers and groups, cleaning up containers and groups, and refreshing the Client Monitor tree displayed, as well as a link to the Host view.

To create a new sub container:

1 Click the **New Container** button for the container in which you want to create the sub container. The New Container dialog box opens.

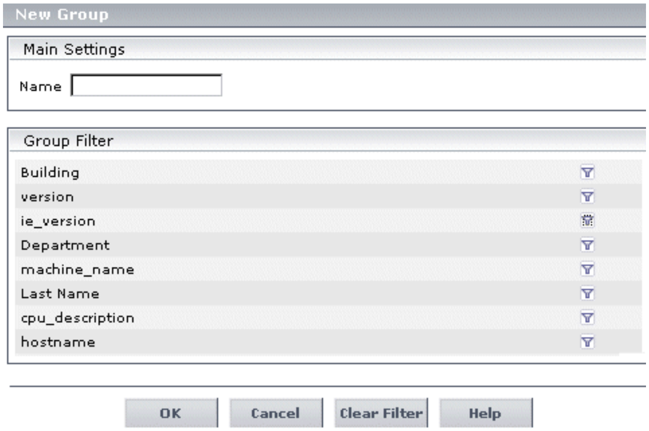
2 In the New Container dialog box, enter the name of the new sub container and click OK to save the new container.

3 The new sub container appears in the Client Monitor tree under the container in which it was created.

To create a new group:

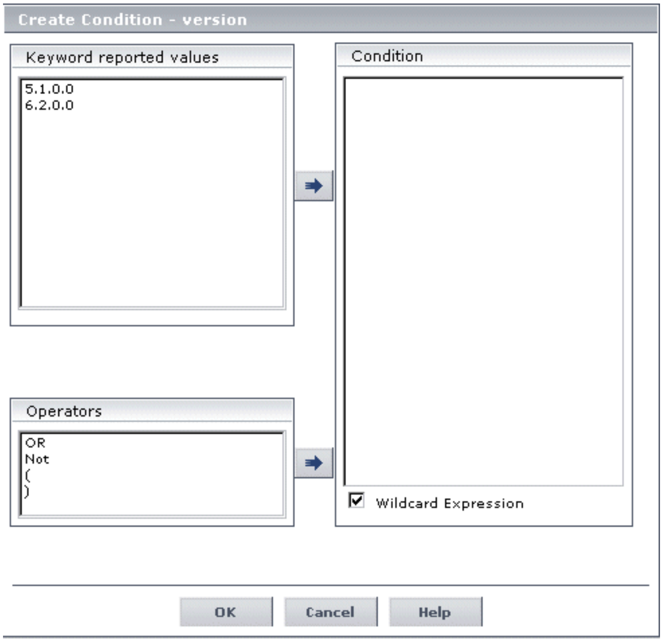
To be able to create a Client Monitor group, at least one Client Monitor host must be registered to Mercury Business Availability Center.

1 Click the **New Group** button for the container in which you want to create the group. The New Group dialog box opens.



2 Enter the name of the group.

3 In the **Group Filter** column, all the keywords from all of the registered Client Monitor hosts are listed. For details on setting keywords on Client Monitor hosts, see “Modifying Client Monitor Settings” in *Client Monitor Administration*. Click the **Edit Keyword Condition** button for the keyword on which you want to filter the Client Monitor hosts. The Create Condition dialog box opens.



Keyword reported values:
5.1.0.0
6.2.0.0

Operators:
OR
Not
(
)

☑ Wildcard Expression

4 Select the keyword values and operators to create the condition you want to use for filtering the Client Monitor hosts. Use the arrows to move the values and operators to the Condition pane on the right.

If the asterisk (*****) or question mark (**?**) characters are used in any of the conditions, you can instruct Mercury Business Availability Center to treat them either as a literals (that is, simply as the character itself), or as a wildcard. The asterisk wildcard represents any string, and the question mark wildcard represents any, single character. Check the **Wildcard Expression** check box to treat asterisks and question marks as wildcards, or clear the check box to treat them as literals.

Click **OK** to save the condition and return to the New Group dialog box.

5 In the New Group dialog box, click **OK** to create the new group. All the Client Monitor hosts that match the set condition are included as part of the new group.

Note: In the New Group dialog box, clicking the **Clear Filter** button removes any existing filter conditions.

To edit a container:

1 Click the **Edit** button for the container you want to edit. The Edit Container dialog box opens.

2 Change the container's name as required.

3 Click the **Show Profiles** link to display all the profiles assigned to the container. For each profile, the profile name, profile action, and assigned jobs are displayed.

4 Click the **Show Hosts** link to display all the Client Monitor hosts that are assigned to the container. For each Client Monitor host, the host name, IP address, Client Monitor version, and last ping time are displayed.

5 Click **OK** to save your changes and exit.

To view details of a container:

1 Click the **Details** button for the container for which you want to view details. The Container Properties dialog box opens displaying the container's name.

2 Click the **Show Profiles** link to display all the profiles assigned to the container. For each profile, the profile name, profile action, and assigned jobs are displayed.

3 Click the **Show Hosts** link to display all the Client Monitor hosts that are assigned to the container. For each Client Monitor host, the host name, IP address, Client Monitor version, and last ping time are displayed.

To edit a group:

1. Click the **Edit** button for the group want to edit. The Edit Group dialog box opens.
2. Change the group's name as required.
3. Change the group's filtering condition as required. For details on configuring a group's filtering condition, refer to the procedure for creating a new group on page 111.
4. Click the **Show Profiles** link to display all the profiles assigned to the group. For each profile, the profile name, profile action, and assigned jobs are displayed.
5. Click the **Show Hosts** link to display all the Client Monitor hosts that are assigned to the group. For each Client Monitor host, the host name, IP address, Client Monitor version, and last ping time are displayed.
6. Click **OK** to save your changes and exit.

To view details of a group:

1. Click the **Details** button for the group for which you want to view details. The Group Properties dialog box opens displaying the group's name and the configured filtering conditions.
2. Click the **Show Profiles** link to display all the profiles assigned to the group. For each profile, the profile name, profile action, and assigned jobs are displayed.
3. Click the **Show Hosts** link to display all the Client Monitor hosts that are assigned to the group. For each Client Monitor host, the host name, IP address, Client Monitor version, and last ping time are displayed.

To delete containers and groups:

1. Select the containers and groups to be deleted by checking the check boxes to the left of the container and group names. Selecting a container automatically selects all the sub containers and groups included in the container.
2. Click the **Delete** button. The selected containers and groups are deleted.

To clean up containers and groups:

Cleaning up a container or group checks all the Client Monitor hosts that are part of that container or group to see if they are removable, and removes those that are. A Client Monitor host is removable if it has not communicated with Mercury Business Availability Center for the past 24 hours.

1. Select the containers and groups for cleaning by checking the check boxes to the left of the container and group names. Selecting a container automatically selects all the sub containers and groups included in the container.

Cleanup

2. Click the **Cleanup** button. The **CM Group Cleanup** dialog box opens.
3. Click **Show Hosts** to view the Client Monitor hosts that are removable, or click **OK** to remove the Client Monitor hosts.

To refresh the Client Monitor tree display:

1. Click the **Refresh** button at the bottom of the page.

Host View

The Host view displays a table of all the Client Monitor hosts that have been registered to Mercury Business Availability Center. The table includes the following columns:

- **Host Name.** The name of the Client Monitor host machine.
- **Applies to Groups.** The Client Monitor groups to which the host belongs.
- **Last Ping Time.** The last time that the Client Monitor host machine was pinged my Mercury Business Availability Center.

For each Client Monitor host listed in the table, click the **Details** button to display the host's details. The Host Detail dialog box opens. In the top half of the Host Detail dialog box, a list of all the keywords and values configured for the Client Monitor host is displayed. For details on setting keywords on Client Monitor hosts, see "Modifying Client Monitor Settings" in *Client Monitor Administration*.

In the bottom half of the Host Detail dialog box, a list of all the groups to which the Client Monitor host belongs is displayed. To view details of a group, click the **Details** button. The Group Properties dialog box opens displaying the group's name and the configured filtering conditions. You can also click the **Show Profiles** link to display all the profiles assigned to the group, and the **Show Hosts** link to display all the Client Monitor hosts that are assigned to the group.

At the bottom of the Host view is a link to the Group view, and a **Refresh** button which you click to refresh the list of registered Client Monitor hosts.

Tracking Actions Status

You use the Actions Status window to track the status of upgrade, update, remove and uninstall processes for Business Process Monitors. The final stage of each of these processes occurs in this window. In the Actions Status window, you can sort the list of actions, you can view a log file for each action, and you can delete an action.

Note that the Actions Status window is refreshed every 30 seconds with the latest statuses.

To sort the list of actions:

You can sort by Action, IP Address, or Current Version: An arrow next to a title shows by which column the actions are sorted, and also the direction in which the column has been sorted (that is, from highest to lowest, or vice versa).

To access an action's log file:

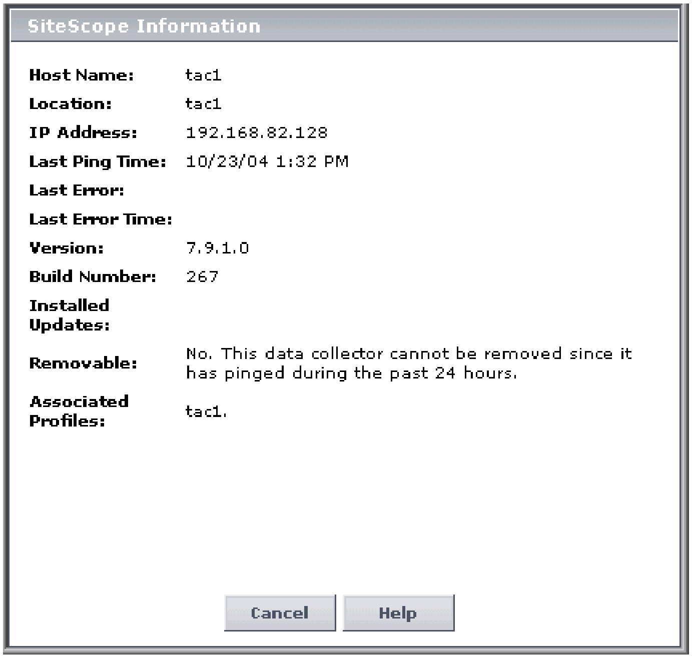
To view a log message, click the **Action Log** button.

To delete an action:

To remove an action from the window, click the **Delete** button. Note that deleting an action's status from the Action Status window does not stop the action.

Viewing Data Collector Information

To view more information on a data collector, including an explanation of why the instance is or is not removable, click the **Information** button to open the data collector's Information dialog box.



SiteScope Information

Host Name: tac1

Location: tac1

IP Address: 192.168.82.128

Last Ping Time: 10/23/04 1:32 PM

Last Error:

Last Error Time:

Version: 7.9.1.0

Build Number: 267

Installed Updates:

Removable: No. This data collector cannot be removed since it has pinged during the past 24 hours.

Associated Profiles: tac1.

On the data collector's Information page, the following is displayed:

- the type of data collector
- the name of the host machine on which the selected data collector is installed
- the location of the host machine on which the data collector is installed
- the IP address of the host machine on which the data collector is installed
- the last time the service pinged the management database
- the last reported error message, if one exists
- the time of the last reported error message, if one exists

- the version number, including build number, of the data collector software
- a list of the updates that have been installed on the data collector software
- an indication of whether or not the data collector instance is removable, and if not, why
- the profiles currently associated with the data collector

Note: For details on the Client Monitor Host Details dialog box, see “Host View” on page 115. For details on the Client Monitor Container Properties dialog box, see “Group View” on page 110.

10

Downtime/Event Scheduling

Downtime or other scheduled events can sometimes skew the results of system availability and performance reports. You may want to exclude these periods of time from reports and alerts.

Defining Downtime and Other Influencing Events

You define downtime or a scheduled event that will occur in the future, and Mercury Business Availability Center excludes data collected during this time interval from its reports. For example, you might want to exclude a recurring maintenance event or a holiday.

Using the Downtime/Event Scheduling page, you can apply a downtime event to multiple profiles. For the defined time interval, you select whether Mercury Business Availability Center stops sending alerts, stops running the associated profiles, or both.

Note for users who have upgraded downtime/event scheduling data from Topaz (versions x - 4.5 Feature Pack 2) to Mercury Business Availability Center 6.x: For details on how to manage the upgraded events, see “Managing Upgraded Downtime/Event Schedule Data from Previous Versions” on page 124.

To define downtime or a scheduled event:

1. Select **Admin** > **Platform** > **Data Collection** > **Downtime/Event Scheduling**. The Downtime/Event Scheduling page opens.

Click **New Event**. The Downtime/Event Scheduling dialog box opens and is divided into three sections:

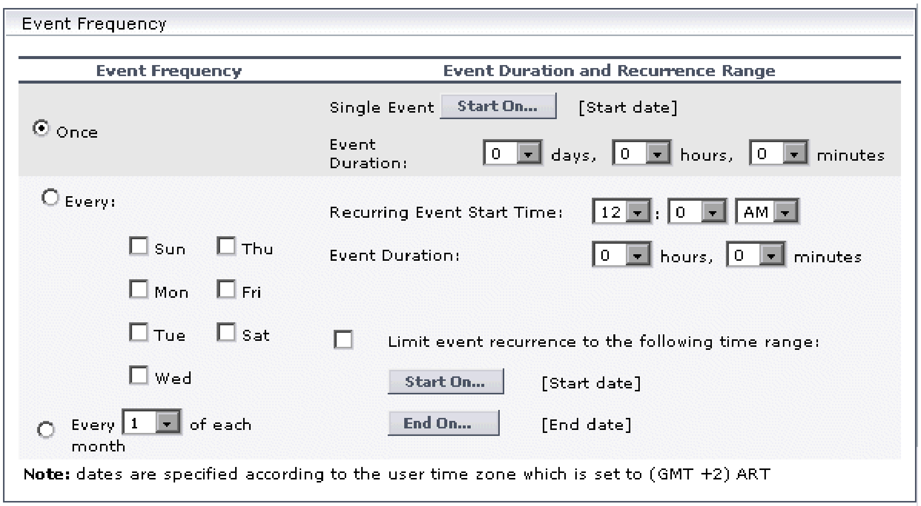
➤ Event Schedule General Properties

➤ Event Frequency

➤ Event Schedule Action

2. In the Event Schedule General Properties area, enter a name and a description of the downtime or scheduled event in the appropriate boxes.

3 In the Event Frequency area, define the time period for the event. You can define a one-time event or a recurring event.



Event Frequency

Event Frequency	Event Duration and Recurrence Range
● Once	Single Event [Start On...] [Start date] Event Duration: 0 days, 0 hours, 0 minutes
○ Every: □ Sun □ Thu □ Mon □ Fri □ Tue □ Sat □ Wed	Recurring Event Start Time: 12 : 0 AM Event Duration: 0 hours, 0 minutes □ Limit event recurrence to the following time range: [Start On...] [Start date]
○ Every 1 of each month	[End On...] [End date]

Note: dates are specified according to the user time zone which is set to (GMT +2) ART

Important: The time period that you define here should be according to the time at the Mercury Business Availability Center server, and not according to the time on the client on which you are working (if the server and client are in different time zones).

Choose from the following alternatives:

➤ **Once:** To define a one-time event, select **Once** in the Event Frequency column. Click **Start On** to choose the start date and time of the event. Choose the duration of the event in days, hours, and minutes.

➤ **Every:** To define a recurring event that occurs on specific days of the week, select **Every** and select the days on which the event occurs. Enter the start time for the event, and its duration.

To limit the event's duration to a particular time range, select the **Limit event recurrence to the following time range** check box, click **Start On** and **End On**, and choose the dates from the calendar.

For example, you have defined an open-ended event frequency for every Sunday at 1 AM for 2 hours. You could limit the event so that it occurs every Sunday for a period of two hours.

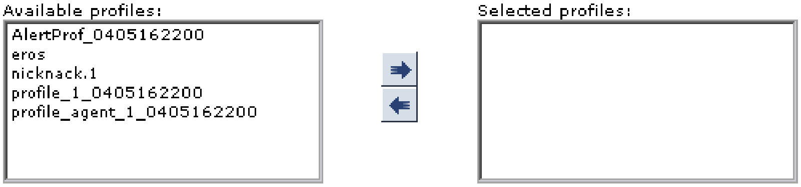
4 In the Event Schedule Action area, you can prevent alerts from being generated and profiles from being run during defined downtime or scheduled events.

- ➤ To prevent alerts from being generated during the time the event is scheduled to occur, select **Stop sending legacy alerts during the event occurrence**.
- ➤ To stop running the selected Business Process profile and collecting data during the time the event is scheduled to occur, select **Stop running the profile during the event occurrence**.

Note: These settings do not affect the generation of alerts defined in SiteScope and cannot stop SiteScope from running during downtime or scheduled events.

---

5 In the Event Schedule Action area, select which profiles to associate with this event.



Available profiles:

AlertProf_0405162200
eros
nicknack.1
profile_1_0405162200
profile_agent_1_0405162200

Selected profiles:

Highlight a profile in the **Available profiles** list and click the right arrow to move it to the **Selected profiles** list. If you do not want a profile that is listed under **Selected profiles** to be associated with this event, highlight the profile and click the left arrow to move it to the **Available profiles** list.

Note: Only those profiles for which the user has full permissions appear in the **Available** or **Selected profiles** list. Additional profiles for which the user does not have permissions may be defined in the platform, but they will not appear for this user.

---

6 Click **OK**. The event you defined is now listed in the Downtime/Event Scheduling page.

To edit an existing downtime or scheduled event:

1 In the Downtime/Event Scheduling page, select the check box next to the event you want to edit. The Downtime/Event Scheduling dialog box opens.

2 Make any changes to the event parameters.

3 Click **OK** to save your changes.

Note: You can edit only those events for which you have full permissions on all the profiles associated with the event. For details on permissions, see “Configuring User Permissions” on page 329.

To delete an existing downtime or scheduled event:

1 In the Downtime/Event Scheduling page, select the event you want to delete. To make selections, use the buttons at the bottom for **Select All**, **Clear All**, and **Invert Selection**.

2 Click the delete button. The event is removed from the Downtime / Event Schedule page.

Note: You can delete only those events for which you have full permissions on all the profiles associated with the event. For details on permissions, see "Configuring User Permissions" on page 329.

Managing Upgraded Downtime/Event Schedule Data from Previous Versions

Mercury Business Availability Center enables you to define a schedule for an event and associate that event schedule with multiple profiles. In previous versions of Mercury Business Availability Center, this was not possible because schedules were defined per profile.

When downtime/event schedule data is upgraded from a previous version, Mercury Business Availability Center converts each profile schedule into a separate event schedule, with the relevant profile associated to the newly created event schedule. After upgrading all the downtime/event schedule data, each schedule that was defined for a profile in the database is listed in the Downtime/Event Schedule page.

Note: For information on performing the data upgrade from previous versions for downtime/schedule event data, see "Upgrading Mercury Business Availability Center" on page 11.

During the upgrade, Mercury Business Availability Center may have created several event schedules that actually all refer to the same event in your system. This means that each of these event schedules has exactly the same configuration, and each has one associated profile. In this case to maintain your events, you should attach all the relevant profiles to one of the event schedules, and delete all the duplicate schedules.

To consolidate upgraded downtime/event schedule data:

1. In the Downtime/Event Scheduling page, select an event that has both configurations that you know are duplicated in other events, and settings that are applicable to several profiles.
2. Edit the settings for the event as required. For example, you can edit the name or description to indicate that the event is associated with multiple profiles. For details, see the procedures for editing an existing event above.
3. While editing the event, associate all relevant profiles to this event. For details, see step 5 in the procedures for defining a new event above.
4. Delete those events that you know are duplicates of the events you want to keep. For details, see the procedures for deleting an existing event above.

11

Profile Entity Maintenance

Platform Administration includes a tool for filtering transactions, locations, and groups from reports. It can also delete obsolete transactions, locations, and groups from the database.

Configuring Report Filters Globally

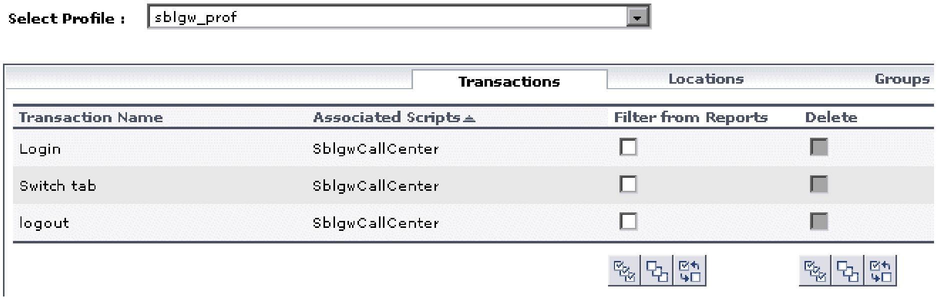
Global report filters enable administrators to exclude—per profile—specific transactions, locations, and/or groups from all Mercury Business Availability Center reports for the current and future profile sessions.

Global report filters affect all users. Any transaction, location, or group that is filtered out using global report filters is unavailable in the user-level report filters. For details on specifying report filters per user, see “Report Filters” in *Application Configuration and Administration*.

You configure report filters globally in the Profile Entity Maintenance page, accessed in the Data Collection tab of Platform Administration.

To configure global report filters:

1. Select **Admin** > **Platform** > **Data Collection** > **Profile Entity Maintenance**. The Profile Entity Maintenance page opens.



Select Profile : sblgw_prof

Transaction Name	Associated Scripts ▲	Filter from Reports	Delete
Login	SblgwCallCenter	□	■
Switch tab	SblgwCallCenter	□	■
logout	SblgwCallCenter	□	■

2. From the **Select profile** list, select the profile from which you want to select transactions, locations, or groups to exclude from reports.

3. Select the tab for the type of entity you want to filter from all reports: **Transactions**, **Locations**, or **Groups**.

4. Select the check box under the **Filter from Reports** column beside the transaction(s), location(s), or group(s) you want to exclude from reports for all users in the system.

   To make your selections, use the buttons at the bottom of the page for **Select All**, **Clear All**, and **Invert Selection**.

5. Click **Apply** to save your settings.

Note:

To activate global filter settings for the current user, log out of Mercury Business Availability Center and log in again.

Filtered values still appear in user-defined (custom and Trend) reports that were created before configuring the filter. To remove newly filtered values from existing user-defined reports, you must remove and re-add the components containing the elements for which filters have been set, and save the report.

Deleting Entities from the Database

Mercury Business Availability Center enables you to delete obsolete entities that are no longer associated with Business Process profiles. These entity types include transactions, locations, and groups.

When you add a transaction monitor to a Business Process profile, the transaction and the transaction's location and group are added to the profile database. Even when a transaction monitor is deleted from the Business Process profile, the transaction and its location and group are still listed in the profile database. Until they are deleted in the Profile Entity Maintenance page, they appear in reports and filter lists for the profile.

Note: You use the Monitor Administration page to create Business Process profiles and add transaction monitors to those profiles. You also delete transaction monitors from profiles in Monitor Administration. For details, see "Managing Business Process Profiles and Creating Client Monitor Profiles" in *End User Management Data Collector Configuration*.

Deleting transactions, locations, and groups affects all users. You delete only those transactions, locations, and groups that are no longer associated with the selected profile. You do this in the Profile Entity Maintenance page, accessed in the Data Collection tab of Platform Administration.

To delete transactions, locations, and groups that are not associated with selected profiles:

1. In Platform Administration, select **Data Collection** > **Profile Entity Maintenance**. The Profile Entity Maintenance page opens.
2. From the **Select profile** list, select the profile from which you want to delete transactions, locations, or groups.
3. Select the tab for the type of entity you want to delete: **Transactions**, **Locations**, or **Groups**.
4. Select the check box under the **Delete** column beside the transaction(s), location(s), or group(s) you want to delete for the selected profile.

You can delete only those transactions, locations, or groups which are no longer associated with the selected profile, meaning not in use. Only the check boxes for those entities are enabled for deletion. If an entity is still associated with the selected profile, the deletion check box is disabled for that entity.

To make your selections, you can also use the buttons at the bottom of the page for **Select All**, **Clear All**, and **Invert Selection**.

5 Click **Apply** to save your settings.

12

Working with Measurement Filters

Note to Mercury Managed Services customers: Mercury Operations administers this page and the interface is hidden from your view.

This chapter explains how to define measurement filters that enable you to filter data being sent to Mercury Business Availability Center from its data collectors, or from external systems or data sources.

Measurement Filters Overview

Measurement filters enable you to harvest significant data from the quantities of data sent to the Mercury Business Availability Center database from various data sources (including Mercury data collectors and third-party data sources) by creating filters that only display the most relevant data required.

You can create measurement filters for all data samples for which Mercury Business Availability Center uses the Universal Data Exchange (UDX) framework. These include Real User Monitor data samples, SiteScope Integration Monitor data samples, and Business Logic Engine data samples. For details on the samples used in Mercury Business Availability Center, see “Samples” in *Reference Information*.

Once you set up measurement filters, you can use them in various contexts in Mercury Business Availability Center, including:

- when defining trend reports using the Custom monitor type
- when creating views in CMDB Administration (all defined measurement filters are automatically added as CIs to the UDX Measurement Filters view)
- when creating service level agreements (by adding measurement filter CIs to the SLA)

Note: In certain contexts in the Mercury Business Availability Center Web interface, the term “custom” data is used to categorize the data samples for which Mercury Business Availability Center uses the Universal Data Exchange (UDX) framework.

Defining Measurement Filters

You define measurement filters from the Measurement Filters page, which you access from the **Admin** > **Platform** > **Data Collection** tab.

For details on the data types listed on the Measurement Filters page, see "Samples" in *Reference Information*.

When creating a measurement filter keep the following guidelines in mind:

- You build an expression by working in the following order: Field, Operator, Value.
- The values you enter in the Value box are case sensitive and you must enter them precisely as they are used in the samples.

To define a measurement filter:

1. Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter** to open the Measurement Filters page.
2. From the Data Type list, select the data type for which you want to define a filter. For details on the data types listed on the Measurement Filters page, see "Samples" in *Reference Information*.

   Filters previously defined for the data type are displayed by name. If no filters exist for the data type, Mercury Business Availability Center displays a message.

   To display existing filters by category, select **Category**. (You create categories to organize your filters. For details on creating a category, see "Creating a Category" on page 135.)
3. Click **New Filter** to open the Filter dialog box.
4. Enter a name for the filter. This is the name that you will see when building reports or in the UDX Measurement Filters view.
5. Build a Boolean expression, using the **And** and **Add 'OR' Expression** buttons.

   For each statement, define the following:

   - **Field.** Choose fields by which to filter the sample. For a list of fields associated with each sample, see "Samples" in *Reference Information*.
   - **Operator.** The list of operators displayed depends on the selected field.

- **Value.** Enter a value that the expression compares with the value in the data sample.

Note that:

- During the process of building the expression, you can view the results so far in the Boolean Expression box.
- If you select a numeric operator, the value must be in the same numeric format as appears in the database.
- If you select a text operator, you can enter a single value without quotation marks as they are added automatically when Mercury Business Availability Center builds the expression. To add two values, add quotation marks around each value, and separate them by a comma. For example, to define a filter that searches for a transaction name that is either **HP** or **OVO**, enter **"HP","OVO"**.
- You should not use a field and operator combination twice in the same **And** phrase.
- If you are building a measurement filter for certain Real User Monitor data types, you can choose the value from a list (instead of typing it in the field). This is true for the following data types:

Data Type	**Field**	**Operator**
RUM Pages	Page Name End User Name	in/not in
RUM End Users	End User Name	in/not in
RUM Transactions	Transaction Name End User Name	in/not in

6 Click **OK**. The filter appears in the list of filters.

You can assign one or more categories to a filter to help you organize the filters. For details, see "Assigning a Category to a Measurement Filter" on page 135.

Creating a Category

You define categories that help to organize your filters in a meaningful manner.

To create a category:

1. Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter** to open the Measurement Filters page.
2. Select the **View By Category** option to display the filters by category.
3. Click the **Category Manager** button to open the Category Manager dialog box.
4. Click **New Category** to open the New Category dialog box.
5. Enter a name for the category, and click **OK**. You are returned to the Category Manager dialog box. The new category appears in the list of categories.
6. Click **OK** to return to the Measurement Filters page.

Assigning a Category to a Measurement Filter

You can assign one or more categories to a filter.

To assign a category to a filter:

1. Select **Admin** > **Platform** > **Data Collection** > **Measurement Filters** to open the Measurement Filters page. Select **View By Name**.
2. Locate the measurement filter in the list, or enter the complete or partial filter name in the Search box, and click **Go**.

   When searching, you can type an asterisk to replace characters. For example, to search for the filter **probe on cats machine**, enter ***cat***.
3. Click the **Category** button to open the Filter Categories dialog box.
4. Select or clear categories to include or exclude them in the filter. Click **All** to select all choices. Click **None** to clear all selections. To invert your selection (clear filters that were selected and select filters that were not selected), click **Invert**.

5 Click **OK**.

Editing a Measurement Filter

You can edit a measurement filter only if it is not being used by any Mercury Business Availability Center entity. If the filter is being used, you can view its properties but you cannot edit it.

To edit a measurement filter:

1 Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter** to open the Measurement Filters page. Select **View By Name**.

2 Locate the measurement filter in the list, or enter the complete or partial filter name in the Search box, and click **Go**.

When searching, you can type an asterisk to replace characters. For example, to search for the filter **probe on cats machine**, enter ***cat***.

3 Click the filter name to open the Filter dialog box.

4 Make any necessary changes. For details, see step 4 in “Defining Measurement Filters” on page 133.

5 Click **OK**.

To edit a measurement filter being used by a Mercury Business Availability Center entity:

1 Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter** to open the Measurement Filters page. Select **View By Name**.

2 Locate the measurement filter in the list, or enter the complete or partial filter name in the Search box, and click **Go**.

When searching, you can type an asterisk to replace characters. For example, to search for the filter **probe on cats machine**, enter ***cat***.

3 Hold the cursor over **See Details** to view a list of entities that are using the filter.

Click **See Details** to display the Filter dialog box in read-only mode.

4 Access each entity and remove the filter.

5 Return to the Measurement Filters page and edit the filter.

Duplicating a Measurement Filter

You can create a measurement filter by duplicating an existing filter, and making any necessary changes.

Note: If categories were assigned to the duplicated filter, they are also assigned to the new filter. If necessary, you can change these assignments. For details, see “Assigning a Category to a Measurement Filter” on page 135.

To duplicate an existing filter:

1 Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter** to open the Measurement Filters page. Select **View By Name**.

2 Locate the measurement filter in the list, or enter the complete or partial filter name in the Search box, and click **Go**.

When searching, you can type an asterisk to replace characters. For example, to search for the filter **probe on cats machine**, enter ***cat***.

3 Click the **Duplicate** button to open the Filter dialog box.

4 Change the name of the filter, and make any other changes as necessary.

5 Click **OK**. The new filter is listed with **(Duplicated)** next to its name.

Deleting a Measurement Filter

You can delete measurement filters, as long as they are not being used by any Mercury Business Availability Center entity. If the filter is being used, the Delete button is disabled.

To delete a filter:

1. Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter** to open the Measurement Filters page. Select **View By Name**.
2. Locate the measurement filter in the list, or enter the complete or partial filter name in the Search box, and click **Go**.

   When searching, you can type an asterisk to replace characters. For example, to search for the filter **probe on cats machine**, enter ***cat***.
3. Click the **Delete** button. Note that no warning message is displayed before Mercury Business Availability Center deletes the filter.

13

Script Repository

Note to Mercury Managed Services customers: The repository for Mercury Managed Services scripts functions differently from the repository described here. For details on working with scripts, see "Mercury Managed Services Script Repository" on page 162.

The Script Repository allows you to manage and maintain your scripts in one central location and enables version control of those scripts.

About the Script Repository

The Script Repository is the central storage in which all your organization's Business Process Monitor scripts and Client Monitor scripts are stored. The repository enables you to organize your scripts into logical groups and to view and manage the properties of those scripts. The repository also enables version control and version updates.

The Script Repository enables you to:

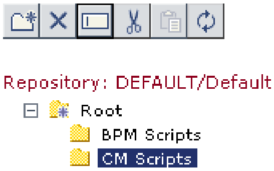
- create and manage user-defined folders for organizing your scripts (for details, see "Working with Script Repository Folders" on page 141)
- upload scripts to a repository folder for use when creating monitors
- manage the scripts that have been uploaded to the repository
- control the versions of the file sets with check in and check out functionality, including downloading script content onto your local system for editing

The Script Repository is installed during Mercury Business Availability Center deployment and resides along with the management database configured for your Mercury Business Availability Center installation.

To generate business process data, you must create profiles and transaction monitors to run scripts that include those processes you want monitored. When you add a transaction monitor to a profile in Monitor Administration, you can add only those scripts that have been stored in the Script Repository. For details on adding profiles and transaction monitors, see "Managing Business Process Profiles and Creating Client Monitor Profiles" in *End User Management Data Collector Configuration*.

Working with Script Repository Folders

Scripts are organized into folders that you create and maintain in the Script Repository. Scripts can be added to the repository only within a user-defined folder. The folders are organized in a tree hierarchy that appears in the left pane of the Script Repository page.



The top level folder is the **Root** level. You create folders below the **Root** level folder. You manage the folders using the buttons that appear above the folder tree.

The Folder Content area in the right pane of the page lists all the scripts that have been uploaded to the folder that is highlighted in the folder tree hierarchy.

You can:

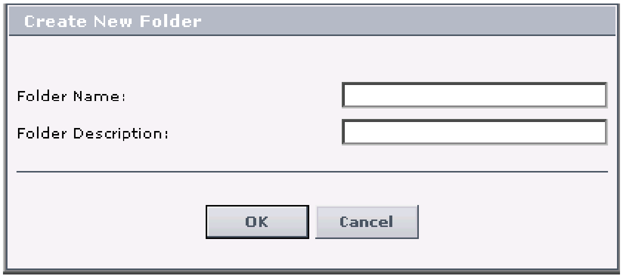
- create new folders (for details, see below)
- delete existing folders (for details, see page 142)
- rename folders (for details, see page 143)
- move folders into other folders (for details, see page 143)
- refresh the folder tree (for details, see page 144)

Creating New Folders

You can create a new folder under the **Root** folder or any other folder in the folder tree hierarchy. A folder can contain both Business Process Monitor and Client Monitor scripts but it is recommended that you create separate folders for each type of script.

To create a new folder:

1. Access the Script Repository page from Platform Administration by selecting **Admin** > **Platform** > **Data Collection** > **Script Repository**.
2. Click to highlight the **Root** or other parent folder under which you want to create the new folder.
3. Click the **New Folder** button. The Create New Folder dialog box opens.



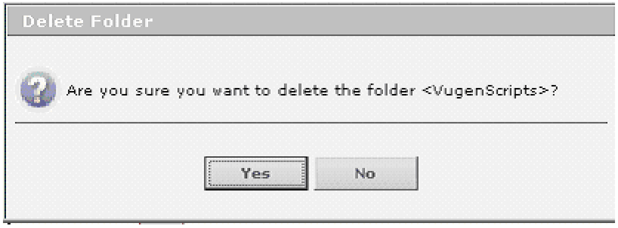
4. Enter a folder name and description. The description is optional.
5. Click **OK** to create the new folder.

Deleting Folders

When you delete a folder, all sub folders and scripts under that folder are permanently erased from the repository. The only exception is if a script is checked out at the time that the folder containing it is deleted. In this case, the repository deletes all folders and scripts until it reaches the checked out file set and its folder, which cannot be deleted, and ceases the delete process.

To delete a folder:

1. Select the folder that you want to delete.
2. Click the **Delete Folder** button. The Delete Folder dialog box opens.


Are you sure you want to delete the folder <VugenScripts>?

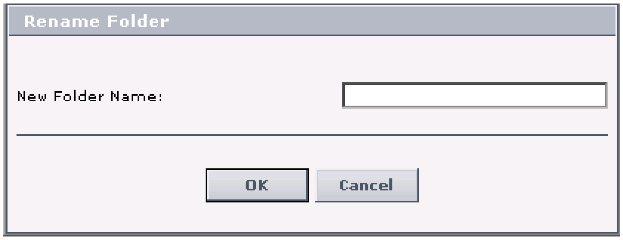
3. Click **Yes** to delete the folder.

Renaming Folders

You can rename a folder in the tree hierarchy. This will not change any of the contents of the folder.

To rename a folder:

1. In the tree hierarchy, select the folder that you want to rename. It can be a parent folder or a sub folder.
2. Click the **Rename Folder** button. The Rename Folder dialog box opens.



3. Enter a new folder name.
4. Click **OK** to change the folder name.

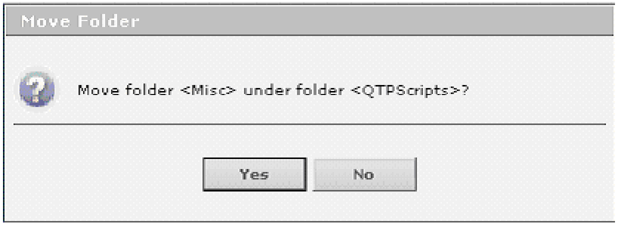
Moving a Folder

You can move a folder from one location to another location within the tree hierarchy using cut and paste functions. You cannot paste a folder into the same folder from which it was cut.

To move a folder:

1. In the tree hierarchy, select the folder that you want to move. It can be a parent folder or a sub folder.
2. Click the **Cut** button.
3. Select the target folder which will be the new location for your folder.

4 Click the **Paste** button. The Move Folder dialog box opens.



Move Folder

Move folder <Misc> under folder <QTPScripts>?

5 Click **Yes** to move the folder.

Refreshing the Folder Tree

The **Refresh Tree** button enables you manually refresh the navigation tree in the Script Repository. You refresh the tree to load the folder data that may have been modified by other users using the Script Repository.

When you perform any of the folder operations, the tree refreshes automatically, so it is not necessary to refresh it manually.

Uploading Scripts and Creating File Sets

You create file sets that contain the scripts you upload to the Script Repository. File sets are the collection of files that make up the script and enable the transactions to be run by the Business Process Monitor or Client Monitor. These file sets must be created within an existing folder in the Script Repository. For details on creating folders, see “Working with Script Repository Folders” on page 141.

To create scripts for use in Mercury Business Availability Center:

- Record Business Process Monitor scripts using the Mercury Virtual User Generator recording tool. For details, see “VuGen Recording Tips” in *Introduction to Creating Scripts*.
- Create scripts in the Client Monitor Recorder page. For details, see *Using Client Monitor Recorder*.

Once these scripts are recorded and saved as zip files, you upload them to the Script Repository.

Note: When zipping a script in Virtual User Generator for upload to the Script Repository, it is recommended that you zip only the script's run-time files.

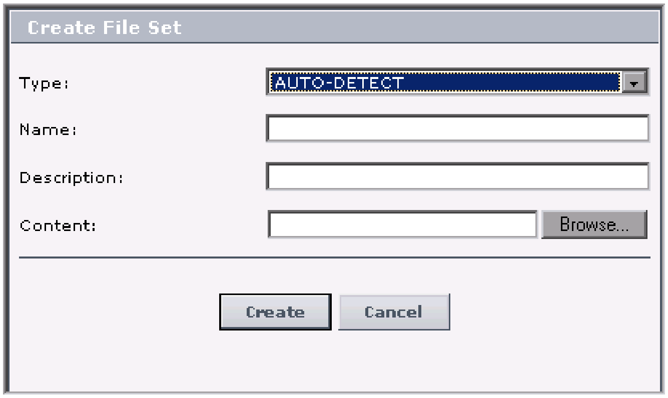
You must upload scripts to the repository to access them when creating profiles in Monitor Administration. You create profiles and transaction monitors to collect performance data on the transactions within the scripts. For details on creating profiles, see "Managing Business Process Profiles and Creating Client Monitor Profiles" in *End User Management Data Collector Configuration*.

To create file sets and upload scripts to the Script Repository:

1 Access the Script Repository page by selecting **Admin** > **Platform** > **Data Collection** > **Script Repository**.

2 In the folder tree in the left pane, highlight the folder into which to add the script.

3 In the right pane, click the **New** button on the bottom right of the Folder Content area. The Create File Set dialog box opens.



Create File Set

Type: AUTO-DETECT

Name:

Description:

Content:

4 Choose the type of file set you want to add to the Script Repository from the **Type** list. If you select **AUTO-DETECT**, the script type is determined during the upload.

Note: Currently the following types are supported in Mercury Business Availability Center: **AUTO-DETECT**, **VUGEN SCRIPT**, **QTP SCRIPT**, and **CLIENT MONITOR**.

5 The name of the content or zip file you specify in step 7 becomes the name of the file set. The name appears in the file set table in the right pane and when viewing the file set properties.

This is also the name that appears in the list of available scripts when creating transaction monitors in Monitor Administration. For details, see "Adding and Editing Transaction Monitors" in *End User Management Data Collector Configuration*.

6 Optionally, add a description for the new file set. This description appears in the file set properties.

7 In the **Contents** box, enter the path of the zip file containing the script. You can also click **Browse** to locate the zip file in your file system.

8 Click **Create** to add the new file set.

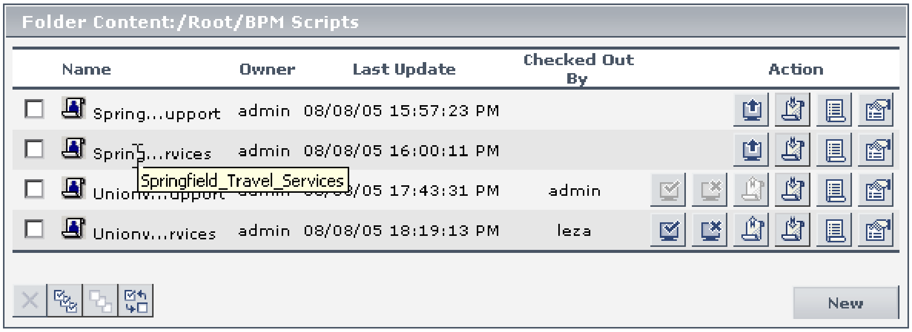
The file set is added to the table in the right pane. This may take a few moments depending on the size of the content of the file.

Managing File Sets

Mercury Business Availability Center enables you to manage the file sets that are stored within the Script Repository folders. The right pane of the Script Repository page lists in table format all the file sets that have been created within the folder that is highlighted in the folder tree.

Understanding the File Set Table

When you select a folder in the tree view, the Script Repository displays a list of the available file sets for that folder.



Folder Content:/Root/BPM Scripts

	Name	Owner	Last Update	Checked Out By	Action
□	Spring...upport	admin	08/08/05 15:57:23 PM		
□	Sprin...rvices	admin	08/08/05 16:00:11 PM		
□	Unionv...upport	admin	08/08/05 17:43:31 PM	admin	
□	Unionv...rvices	admin	08/08/05 18:19:13 PM	leza	

Springfield_Travel_Services

Each line represents a file set for the selected folder and the actions that can be performed on the file set.

You can view the following:

- Type of script – Script type is indicated by these icons that appears next to the file set name:
  - Virtual User Generator (VUGen) script
  - Client Monitor script
  - QuickTest Professional script
- **Name.** The name given to the file set when it was created and the script was uploaded. In the case of a long name, the name is truncated in the table. To view the entire name, click the name as it appears and a tooltip opens displaying the full name of the file set as in the above diagram.
- **Owner.** The user who created the file set by uploading the script.

- **Last Update.** The date when the file set was last checked into the repository. This could be the date it was first created.
- **Checked Out By.** The user who has the file set currently checked out. If the file set is not checked out, this column is blank.
- **Action.** You can perform the following actions on each file set:
  - Check out the file set to ensure version control. For details, see “Checking out a Version” on page 151.
  - Check in the file set, cancel the check out, or upload without checking in. These buttons are displayed only for those files sets that have been checked out and are enabled only for the user who performed the check out. For details, see “Working with File Set Versions” on page 151.
  - Download file set contents for editing. For details, see “Downloading File Set Content” on page 152.
  - Show versions. For details, see “Viewing File Set Versions” on page 157.
  - View file set properties. For details, see “Viewing File Set Properties” on page 150.

Deleting File Sets from a Script Repository Folder

When deleting file sets from a selected repository folder, keep in mind:

- All files within the deleted file set are permanently erased from the repository.
- If you delete a file set that is currently running in a transaction monitor, the transaction monitor continues running the file set’s script but the properties of the transaction monitor cannot be edited in Monitor Administration until the file set is added back to the script repository.
- A file set that is currently checked out cannot be deleted by another user and can be deleted only by the same user who checked it out.

To delete a file set:

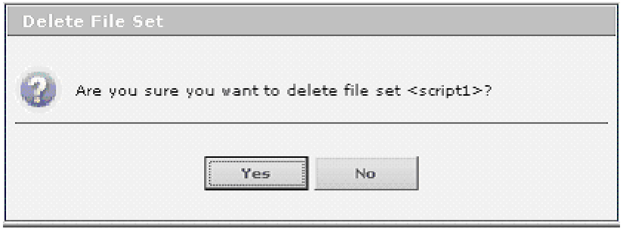
1. In the folder tree in the left pane of the Script Repository, highlight the folder that contains the file set that you want to delete.

2 Select the check box for the file set you want to delete.

To make your selections, use the buttons at the bottom of the page for **Select All**, **Clear All**, and **Invert Selection**.

3 Click the **Delete File Set** button at the bottom of the table. The delete button is enabled only if at least one file set is selected.

The Delete File Set dialog box opens.



Delete File Set

Are you sure you want to delete file set <script1>?

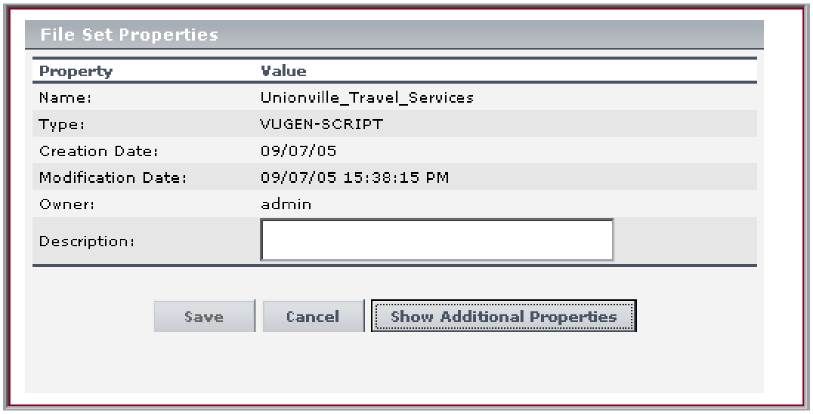
4 Click **Yes** to confirm that you want to delete the file set.

Viewing File Set Properties

You can view the properties of the current version of the file set. All the fields are view only and cannot be edited while viewing the properties.

To view file set properties:

1 Click the **File Set Properties** button on the line of the file set whose properties you want to view. The File Set Properties window of the working version of the file set opens.



File Set Properties

Property	Value
Name:	Unionville_Travel_Services
Type:	VUGEN-SCRIPT
Creation Date:	09/07/05
Modification Date:	09/07/05 15:38:15 PM
Owner:	admin
Description:	

2 Optionally, you can click **Show Additional Properties** to view the properties related to the script itself.

Note: When a file is checked in, none of the fields in the File Set Properties dialog box are editable. When a file set is checked out, the description property can be edited only by the user who checked out the file set.

Working with File Set Versions

The Script Repository enables you to control the versions of your file sets. The procedure when working within the Script Repository for editing a script is to check out the file set, download the script for editing, and then check in the file set. When the file set is checked in, the Script Repository automatically assigns the script a new version number.

You can also view version properties and restore previous versions of file sets. For details, see “Viewing File Set Versions” on page 157.

Checking out a Version

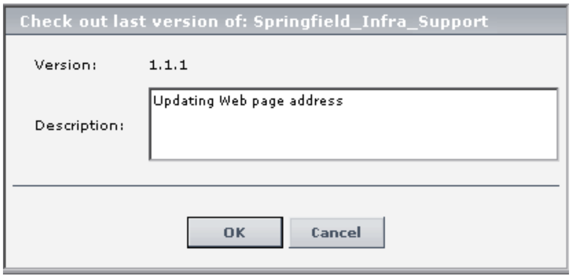
You can check out a file set to ensure that no other user makes changes to this version of the script while you are editing it. Only one user at a time can check out a file set. Once that file set is checked out, only that user can check it in, delete it, or create a new version.

Note: When a file set is checked out, the script can still be added as a transaction monitor while working in Monitor Administration. If the file set is checked in with a newer version, the transaction monitor includes a message to the user indicating that a newer version of the script is available in the repository.

To check out a file set:

1 Click the Check Out button on the line of the file set you want to check out.

The Check Out Last Version dialog box opens.



Check out last version of: Springfield_Infra_Support

Version: 1.1.1

Description: Updating Web page address

2 Optionally, enter a description for the version. This is recommended so that all users have access to the information regarding why different versions have been created in the repository.

3 Click **OK**. The file set is checked out.

You can now download the file set, knowing that the version cannot be edited by another user.

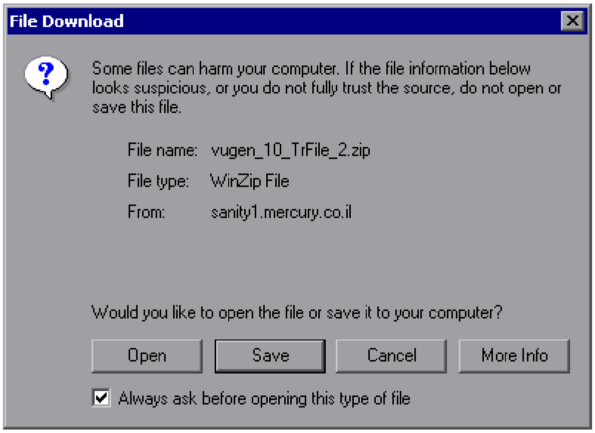
Downloading File Set Content

When you download a file set, the current working version of the file set is downloaded. It is good practice to check out the file set before downloading it to ensure that another user is not simultaneously editing the same file set's script.

To download the content of a file set's current working version:

1 Click the **Download File Set Content** button on the line of the file set that you want to download.

If the file set has content, the File Download dialog box opens.



File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: vugen_10_TrFile_2.zip

File type: WinZip File

From: sanity1.mercury.co.il

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

If the selected file set is empty, the Script Repository issues a warning indicating that the file set has no content.

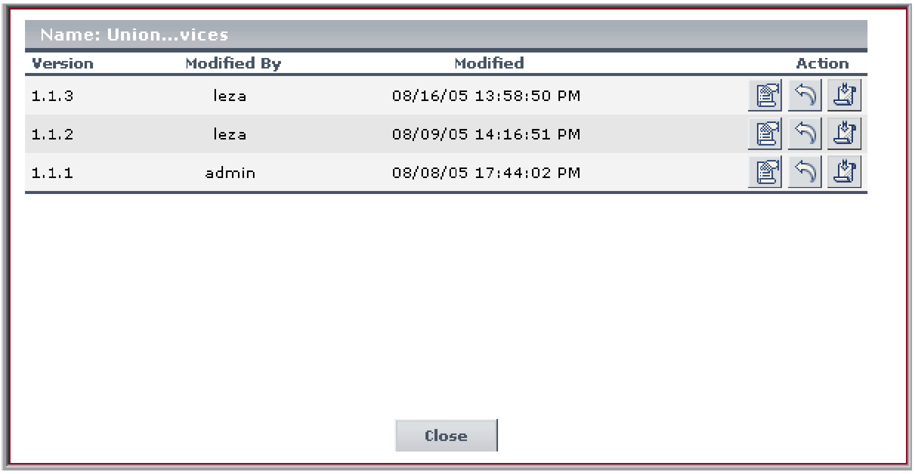
2 Click **Save** to save the zip file that contains the script to your local file system. The Save As dialog box opens.

3 Specify a location in your file system for saving the zipped file of the script and click **Save**.

You can now use your recording tool to open and edit the downloaded script.

To download the specified version of a file set:

1 Click the **Show Versions** button on the line of the file set whose content you want to download. The File Set Versions dialog box opens.



Name: Union...vices

Version	Modified By	Modified	Action
1.1.3	leza	08/16/05 13:58:50 PM	
1.1.2	leza	08/09/05 14:16:51 PM	
1.1.1	admin	08/08/05 17:44:02 PM	

2 Click the **Download File Set Content** button on the line of the file set version that you want to download. Select from the list of checked in file set versions.

You cannot download the version of a file set version that is checked out. For details, see “Viewing File Set Versions” on page 157.

3 Continue with steps 2 through 3 in the procedure for downloading the current working version of a file set, which appears on page 152.

Checking in a Version

You check the file set back into the Script Repository once you have finished editing the script and saving the zip file in your file system.

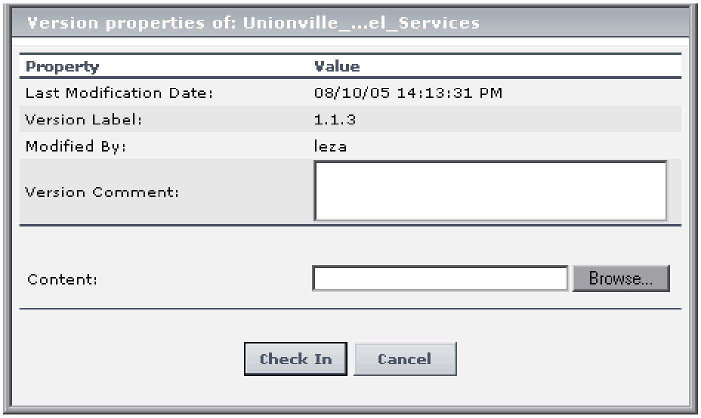
When you check in a file set, the Script Repository automatically creates a new version for the file set. For example, if you checked out version number 1.1.1 of a file set, the Script Repository creates version number 1.1.2 as a result of checking the file set back into the Script Repository. File set version 1.1.1 is still accessible and its script can be added to transaction monitors in Monitor Administration, but the latest version, file set version 1.1.2, becomes the default version.

To check in a version:

1 Click the **Check In** button on the line of the checked out version of the file set you want to check in.

Note: This button appears only for file sets that are checked out.

A check in version of the Version Properties dialog box opens.



Version properties of: Unionville_...el_Services

Property	Value
Last Modification Date:	08/10/05 14:13:31 PM
Version Label:	1.1.3
Modified By:	leza
Version Comment:	

Content:

2 Optionally, enter **Version comments** for this new version of the file set. This is recommended so that other users know what has been updated in the script.

3 Optionally, click **Browse** to locate and select the zip file of the latest version of the script.

➤ If you specify a location for the file set content, the name of the uploaded zip file must match identically to the name of the file set.

➤ If you do not specify a location for the file set content:

- And the file set content has been uploaded and not yet checked in, the most recently uploaded version of the content is checked in. No location has to be specified. For details, see "Uploading File Set Content" on page 156.
- And the file set content was not uploaded, the same content of the file set that was checked out is checked in again and given a new version number.

4 Click **Check In** to check in the version or **Cancel** to cancel the operation.

Cancelling Check Out

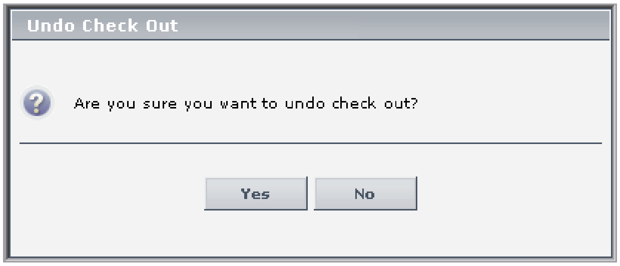
You can cancel a check out. Cancelling a check out prevents the Script Repository from creating a new version number and leaves the file checked in with its current version number. If you have made modifications to the script that you do not want saved in the Script Repository file set, cancelling the check out ensures that those changes are not brought into the Script Repository.

To cancel a check out:

1 Click the **Undo Check Out** button on the line of the checked out file set.

Note: This button appears only for file sets that are checked out.

The Undo Check Out dialog box opens.



Undo Check Out

Are you sure you want to undo check out?

2 Click **Yes** to undo the check out or **No** to keep the file set checked out.

Uploading File Set Content

When a file set is checked out, you can upload a script without creating a new file set version. You upload scripts to save to the Script Repository the recent modifications you have made to the script. This is only if you do not yet want to create a new version by checking in the file set. You may want to do this as an extra precaution when making many modifications to scripts so that the file set is saved to the repository. This is useful, for example, while you are testing the script in the recording tool.

When you upload a script without checking in the file set, the content of this version of the file set is not available to other users.

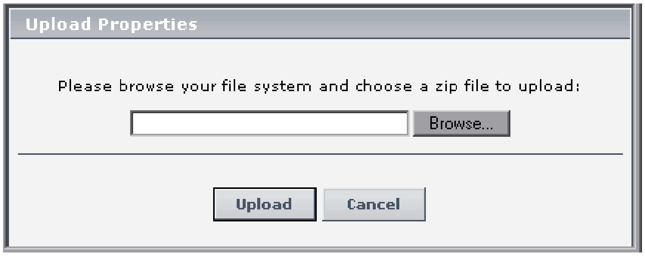
When you check in a file set that has been uploaded, you do not have to specify a location in your file system to locate the file set. The most recently uploaded file set is automatically checked in during the check in procedure.

To upload the content of a checked out file set:

1 Click the **Upload File Set Content** button on the line of the checked out file set.

Note: This button appears only for file sets that are checked out.

The Upload Properties dialog box opens.



Upload Properties

Please browse your file system and choose a zip file to upload:

2 Click **Browse** to locate and select the zip file of the latest version of the script.

3 Click **Upload** to save the script to the Script Repository.

This content is used when checking in the file set if during check in, you do not specify a location for the zip file.

Viewing File Set Versions

You can view the versions of a file set in the File Set Versions dialog box. It includes a listing of all the versions of a file set and the actions that can be performed on that file set version.

The versions list and available actions are different for a file set that is checked in from those for a file set that is checked out.

You can restore a previous version of a file set that is not checked out.

Viewing Checked in File Set Versions

When you view the file set versions of a file set that is not checked out, you see all the versions of the file set that have existed in the Script Repository. You can view the following:

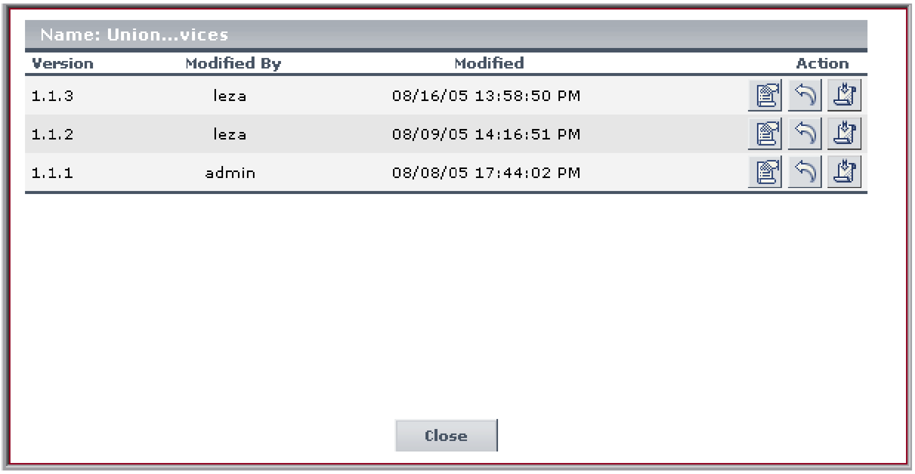
- **Version.** The number given to the file set when it was last checked into the Script Repository.
- **Modified by.** The user who last checked in the version of the file set.
- **Modified.** The date and time when the file set was last checked into the repository. If the file set has never been checked in, this is the date the script was first downloaded and the file set was first created.
- **Action.** You can perform the following actions on the version:
  - **View version properties.** While viewing version properties, you can modify only the **Version Comments** field. All other fields are uneditable.
  - **Restore version.** This enables you to restore a previous version of a file set and make it the current version. For details, see “Restoring Previous File Set Versions” on page 158.
  - **Download file set contents for editing.** For details, see “Downloading File Set Content” on page 152.

Restoring Previous File Set Versions

When you restore a file set version, the Script Repository automatically assigns that version the next available version number. For example, if you select version number 1.1.1 to restore, the Script Repository assigns that same file set content the next available version number which in the diagram below, would be version number 1.1.4. Thus version 1.1.1 and version 1.1.4 are identical.

To restore a previous version of a file set:

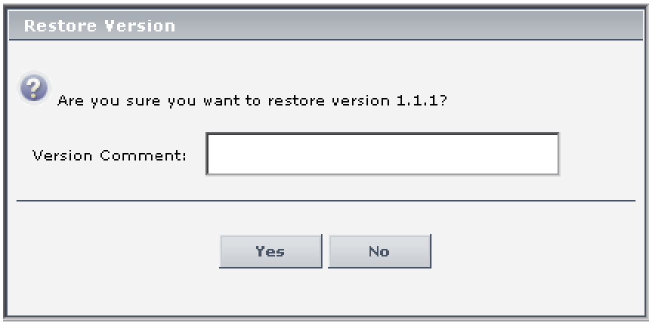
1 Click the **Show Versions** button on the line of the file set whose previous version you want to restore. The File Set Versions dialog box opens.



Name: Union...vices

Version	Modified By	Modified	Action
1.1.3	leza	08/16/05 13:58:50 PM	
1.1.2	leza	08/09/05 14:16:51 PM	
1.1.1	admin	08/08/05 17:44:02 PM	

2 Click the **Restore Version** button on the line of the version you want to restore. The Restore Version dialog box opens.



Restore Version

Are you sure you want to restore version 1.1.1?

Version Comment:

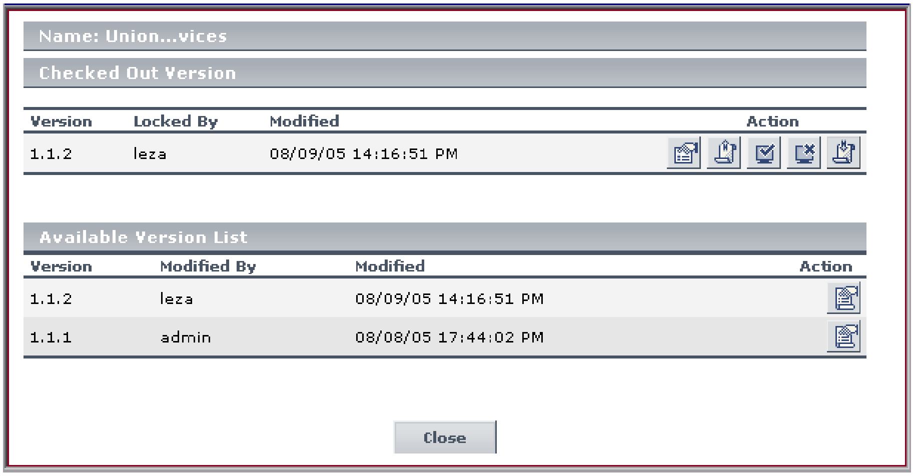
3 Optionally, enter the relevant information in the **Version Comments** field. Because the contents of the new version you are creating are identical to the old version, it is recommended that you include the version number that was restored in the comments.

4 Click **Yes** to confirm.

The new version now appears with its new version number in the File Set Versions dialog box.

Viewing Checked out File Set Versions

When you view the file set versions of a file set that has been checked out, you see the checked out version listed separately from the previous versions of the file set.



Name: Union...vices

Checked Out Version

Version	Locked By	Modified	Action
1.1.2	leza	08/09/05 14:16:51 PM	

Available Version List

Version	Modified By	Modified	Action
1.1.2	leza	08/09/05 14:16:51 PM	
1.1.1	admin	08/08/05 17:44:02 PM	

- In the Checked Out Version area, you can view the following for the checked out version:
  - **Version.** The version number of the file set that is checked out.
  - **Locked by.** The user who checked out the file set.
  - **Modified.** The date and time when the file set was last checked into the repository. If the file set has never been checked in, this is date it was first created.
  - **Action.** If you are the user who checked out the file set, you can perform the following actions on the version:

- **View file set properties.** For details, see "Viewing File Set Properties" on page 150.
- **Check in the file set, cancel the check out, or upload without checking in.** These buttons are enabled only for the user who performed the check out. For details, see "Working with File Set Versions" on page 151.
- **Download file set contents for editing.** For details, see "Downloading File Set Content" on page 152.

➤ In the Available Versions area, you can view the following for all the previous versions of the checked out file set:

  ➤ **Version.** The number given to the file set when it was last checked into the Script Repository.

  ➤ **Modified by.** The user who last checked in this version of the file set.

  ➤ **Modified.** The date and time when this version of the file set was last checked into the repository.

  ➤ **Action.** You can perform the following action on the version:

  - **View version properties.** While viewing version properties, you can modify only the **Version Comments** field. All other fields are uneditable.

14

Data Collection Administration for Mercury Managed Services

Note: The Location IP Ranges, Script Repository, and Package Information pages are available to Mercury Managed Services customers only.

Data Collection Administration for Mercury Managed Services allows you to view the customer's list of locations and related information, to maintain your scripts and view their verification information, as well as to view package location information.

Location IP Ranges

The Location IP Ranges page presents a list of locations defined in your package. This list includes the detailed IP address ranges.

In Platform Administration, click **Data Collection** > **Location IP Ranges** to open the **Location Info** area.

You can view the following information:

- **Location Name.** The physical location: city, county, state, or province, and the name of the location.
- **IP Address/Subnet Mask.** The range of IP addresses for the location. The first number is the IP Address (and the beginning of the range). The second number is the Subnet Mask. The Subnet Mask is used to calculate the number of addresses in the range by subtracting the last set of three numbers (in this example: 240) from the set of three numbers before last (in this example: 255). The result is: 255-240=15. This result is then added to the last set of three numbers in the IP Address (in this example 144+15=159) to provide the upper IP Address in the range: 195.193.104.159. The range of Amsterdam IP Addresses is then from the IP Address: 195.193.104.144 to the calculated upper IP address: 195.193.104.159.

Mercury Managed Services Script Repository

The script repository is a central database in which all your organization's Business Process Monitor scripts and Client Monitor scripts are stored.

When you add a monitor to a profile in Monitor Administration, you can add only those scripts that have been stored in the Script Repository ("Managing Business Process Profiles and Creating Client Monitor Profiles" in *End User Management Data Collector Configuration*).

Once you have created and recorded the scripts (for details, see "Recording Business Process Monitor and Client Monitor Scripts" on page 163), you upload them using the Script Repository page (for details, see "Uploading Scripts" on page 163). You can then view the scripts, edit them, and upload them again (for details, see "Understanding the Script Repository" on page 164). You can reload a previous version and make it the current version and you can view the results of the verification process performed by Mercury Business Availability Center (for details, see "Editing Scripts" on page 165). You can also specify the recipients to whom the results of the verification process should be sent (for details, see "Notifying Recipients of Script Verification" on page 171).

Recording Business Process Monitor and Client Monitor Scripts

You record Business Process Monitor scripts using the Mercury Virtual User Generator recording tool. Once they are recorded, you zip the related files and upload them to the script repository (for details, see "VuGen Recording Tips" in *Introduction to Creating Scripts*). Business Process Monitor scripts are listed in the Business Process Monitor tab in the Script Repository page.

You create Client Monitor scripts in the Client Monitor Recorder page (for details, see *Using Client Monitor Recorder*). Client Monitor scripts are listed in the Client Monitor tab in the Script Repository page.

Note: When zipping a script in Virtual User Generator for upload to the script repository, it is recommended that you zip only the script's run-time files. Zipping all files may cause script verification to fail due to a limit in the file size allowed by the repository.

Uploading Scripts

You upload scripts from the Script Repository page.

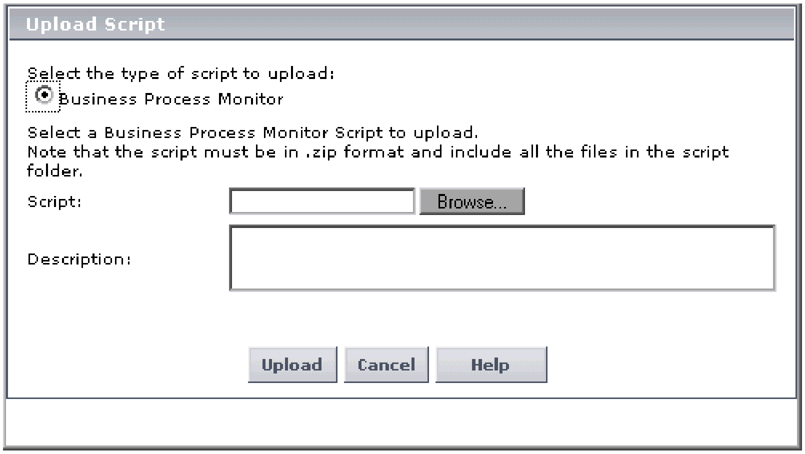
When the upload is finished, Mercury Business Availability Center displays the script in the appropriate list of uploaded scripts on the Script Repository page. For details, see "Understanding the Script Repository" on page 164. The version of the script that is stored is the active version. To use a newer version or to go back to an older version of the script you must upload the script corresponding to the version you want. That script will then become the active version of the script.

After you upload a script, Mercury Business Availability Center runs the verification process. For details, see "Understanding the Script Verification Results" on page 168.

You must upload scripts to the repository to access them when creating profiles. For details on creating profiles, see "Managing Business Process Profiles and Creating Client Monitor Profiles" in *End User Management Data Collector Configuration*.

To upload scripts from the Script Repository page:

1 In the Script Repository page, click **Upload** to open the Upload Script page.



Upload Script

Select the type of script to upload:

● Business Process Monitor

Select a Business Process Monitor Script to upload.
Note that the script must be in .zip format and include all the files in the script folder.

Script:

Description:

2 Select the type of script you want to upload (if not already selected).

3 Click **Browse** to open the Choose File dialog box.

4 Browse to the location on your computer or network where the recorded script is located, select the file, and click **Open**.

- Business Process Monitor scripts must be in **.zip** format.
- Client Monitor scripts must be in **.obs** format.

5 Click **Upload** to upload the script.

Understanding the Script Repository

The Script Repository page lists the scripts that have been uploaded in the repository.

In Platform Administration, click **Data Collection** > **Script Repository** to open the **Script Repository** area with the **Business Process Monitor** tab selected.

You can view the following information – the same information is displayed in the **Business Process Monitor** tab and in the **Client Monitor** tab:

- **Script Name.** The name of the script. Click the script name to open the **.zip** files or the **.obs** files that comprise the transaction. For details, see “Editing Scripts” on page 165.
- **Owner.** The name of the last user who updated the script.
- **Version.** The current version of the script. Double-click the version to modify it. For details, see “Displaying Script Versions” on page 166.
- **Status.** The status of the verification process for the script. Double-click the status to modify it. For details, see “Understanding the Script Verification Results” on page 168.
- **Last Update**. The date when the script was last updated.

You can:

- Download a special Virtual User Generator by clicking **Click to download Mercury Virtual User Generator** to. For details, see “Recording Business Process Monitor and Client Monitor Scripts” on page 163.
- Open the **.usz** file directly in the Virtual User Generator (if you have installed it) by clicking **Edit**. For details, see below.
- Manually verify the script by clicking **Manually Verify**. For details, see “Manually Verifying the Script” on page 168.
- Upload the script from the Script Repository page by clicking **Upload**. For details, see “Uploading Scripts” on page 163.
- Refresh the displayed information by clicking **Refresh**. The data is refreshed from the server (from the database that stores the list of scripts).

Editing Scripts

You can access Business Process Monitor scripts stored in the repository by clicking the script name link and saving the script to a local or network drive. You can then edit the file at a later time using the Virtual User Generator or you can open the file using any program that supports the **.zip** format.

You can access Client Monitor scripts stored in the repository by clicking the script name link and saving the script to a local or network drive. You can then edit the file using the Client Monitor Recorder (for details, see “Client Monitor Recorder Introduction” in *Using Client Monitor Recorder*). Client Monitor scripts are stored using the **.obs** format.

You can view information about the script version (for details, see “Displaying Script Versions” on page 166).

You can view the conditions under which the script verification ran, and the actual result of each condition (for details, see “Manually Verifying the Script” on page 168 and “Understanding the Script Verification Results” on page 168).

After editing a script, you must upload it again to the repository. Business Process Monitor scripts must be zipped before being uploaded. After you upload the edited script, Mercury Business Availability Center reruns the verification process on the script.

Mercury Business Availability Center indicates the update date and time of editing in the Last Update column.

Displaying Script Versions

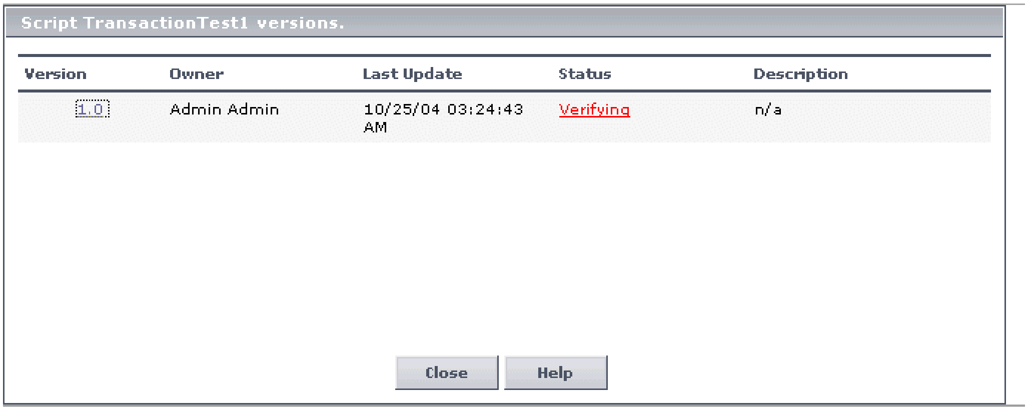
You can use the Script <script-name> versions page to track changes made to scripts and to access them to perform changes.

The Script <script-name> versions page displays the history of the script. Each time you upload the script, a new line is added to this list and the version is incremented.

To select a previous version of the script you must download it and upload it again; it then becomes the current version.

To display the list of versions of a script

1 In the **Script Repository** area, click the script version to open the Script <script-name> versions page.



Script TransactionTest1 versions.

Version	Owner	Last Update	Status	Description
1.0	Admin Admin	10/25/04 03:24:43 AM	Verifying	n/a

2 View the following information:

Version – The version of the script. Click the version to open the scripts, which are stored in **.zip** format if they are Business Process Monitor scripts or in **.obs** format if they are Client Monitor scripts. The current version is underscored.

- **Owner.** The name of the last user who updated the script.
- **Last update.** The date when the script was last updated.
- **Status.** The status of the script. Click the status to open the Script Verification Results page. For details, see “Manually Verifying the Script” on page 168.
- **Description.** The description of the script. The description is useful for version control: you can describe why changes were made to this version of the script.

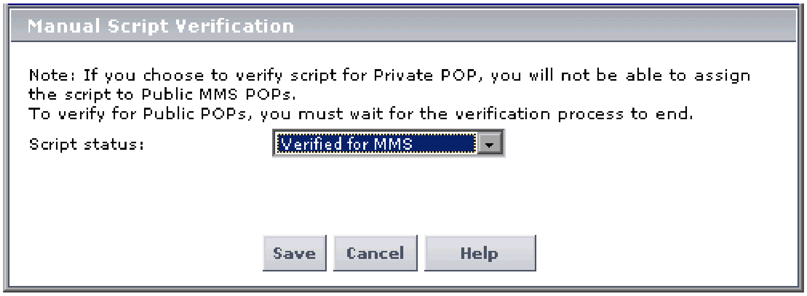
3 Click **Close** to close the page.

Manually Verifying the Script

You can use this page to change the verification status of a script and to remove a script from use.

To manually verify the script:

1 In the **Script Repository** area, click **Manually Verify** to open the Manual Script Verification page



Manual Script Verification

Note: If you choose to verify script for Private POP, you will not be able to assign the script to Public MMS POPs.
To verify for Public POPs, you must wait for the verification process to end.

Script status: Verified for MMS

2 Select the appropriate **Script status**:

- **Verified for private POP.** Select this status for scripts that you want to verify for using on your private Business Process Monitor.
- **Verification failed.** You can use this status to disable a transaction before running your profile.

3 Click **Save** to save the changes.

Understanding the Script Verification Results

After you upload a script to the script repository, Mercury Business Availability Center runs a verification process to verify that the script will execute properly when it is run in a profile. Once the script passes verification, Mercury Business Availability Center displays the **Passed** status in the Status column. You can add a script to a profile only after it passes verification.

You can check the verifications for which your transaction failed in the script <script-name> versions page.

The complete list of conditions is as follows:

Running Verifications	Rule	Actual Result
Disallowed function calls: system;lr_load_dll	Do not use the function calls that are listed.	Lists the actual function calls used in the script.
Download size must be less than 3000000 bytes	The maximum size of the download.	Indicates the actual download size
Execution must be less than 300 seconds	The maximum execution time of the script.	Indicates the actual execution time of the script.
Expected protocol: qtWb;NCA;WinSock;Sap_web; SaPgui	Only use the listed protocol types.	Indicates the actual protocol type used in the script.
Extra files with the following extensions are allowed: ini;h;tst	Only use extra files with the listed extensions.	Lists the actual extensions used in the script.
Failed transactions are disallowed	Do not use failed transactions.	Indicates whether there were failed transactions in the script.
Maximum number of dynamic transactions allowed:0	Do not use more dynamic transactions than the allowed maximum number.	Indicates the number of dynamic transactions in the script. Dynamic transactions are the transactions that are not defined in the USR file; meaning their name has been generated dynamically (for example: Transaction + i == Transaction 1,Transaction 2, and so forth).

Running Verifications	Rule	Actual Result
Maximum number of iterations allowed:1	Do not use more iterations than the allowed maximum number.	Indicates the number of time each action in a script is run. Every script is composed of actions (.c code files) which can be run more than once during one running of the script (a feature used mainly in LoadRunner and not in Mercury Business Availability Center). This iteration number must be limited so that duplicate transactions are not reported.
Maximum number of transaction instances allowed:1	Do not use more transaction instances than the allowed maximum number.	Indicates the number of transaction instances in the script.
Maximum number of transactions allowed:100	Do not use more transaction than the allowed maximum number.	Indicates the number of transactions in the script.
Total size must be less than 600000 bytes	The maximum total size of the script.	Indicates the actual total size of the script.

Note: The verification process differs depending on the contents of the script. Some scripts may go through a subset of the verifications listed above.

If any of these verification checks are not applicable to your organization, contact Mercury Managed Services Support.

To view the script verification results

1 In the Script <transaction-name> versions page, click the value in the **Status** column to open the Script Verification Results page.

2 You can view the following information:

- **Expected/Allowed Value Verifications.** Lists the conditions for the script verification.
- **Actual results.** The current results of the verification.
- **Description.** The description of the verification.
- **Status.** The status of the verification. It can be: Passed, Warning, or Failed.

3 Click **Close** to close the page.

Notifying Recipients of Script Verification

Note: This section applies only to Business Process Monitor scripts.

You can instruct Mercury Business Availability Center to send e-mail notification to specified recipients when Business Process Monitor script verification is complete.

To send e-mail notification when verification is complete:

1 In the **Verification Subscription** area, check the **Notify the following recipients when script verification is complete** check box.

2 Specify one or more e-mail addresses of the recipients in the **E-mail address(es)** box, separated by semi-colons.

3 Click **Apply**.

Package Information

Package information includes information about the customer package. This information is entered in the Mercury Business Availability Center application when the Mercury Managed Services contract is signed.

You can use the Package Information page for:

- Viewing Package Information (for details, see page 172)
- Selecting Locations for Business Process Monitors and Hosts for Client Monitors (for details, see page 173)
- Viewing and Modifying Package Properties Information (for details, see page 174)

Viewing Package Information

You can view information about the package name, expiration date, Business Process Monitor transactions, URLs, POPs, and Client Monitor transactions and hosts.

To view package information:

1. Select **Admin** > **Platform** > **Data Collection** > **Package Information** to open the **Package Information** area.
2. View the following information:
   - **Name.** The name of the package.
   - **Expiration.** The expiration date. The expiration date becomes red 14 days before the expiration date of a paying customer package, and 7 days before the expiration date of an evaluation customer package. For more details, see “Viewing and Modifying Package Properties Information” on page 174.
   - **Business Process Monitor Transactions.** The total number of Business Process Monitor transactions that can be run as part of the package.
   - **URLs.** The total number of single URLs monitors that can be accessed as part of the package.
   - **Global POPs.** The total number of global POPs that can be run as part of the package.

- **Private POPs.** The total number of private POPs that can be run as part of the package.
- **Client Monitor Hosts.** The total number of Client Monitor hosts that can be used as part of the package.
- **Client Monitor Transactions.** The total number of Client Monitor transactions that can be run as part of the package.

3 You can:

- Click **Package Location** to open the Package Locations page. For details, see "Selecting Locations for Business Process Monitors and Hosts for Client Monitors" on page 173.
- Click **Package Host** to open the Package Hosts for Client Monitor page. For details, see "Selecting Locations for Business Process Monitors and Hosts for Client Monitors" on page 173.
- Click **Edit** to open the Package Properties page. For details, see "Viewing and Modifying Package Properties Information" on page 174.

Selecting Locations for Business Process Monitors and Hosts for Client Monitors

You can view the available Business Process Monitor locations or Client Monitor hosts on which to run the packages. You can also select, among all the possible locations, the appropriate Business Process Monitor locations or Client Monitor hosts up to the number specified by the customer package.

To view package location information or select locations for Business Process Monitors:

1. Select **Admin** > **Platform** > **Data Collection** > **Package Information** to open the **Package Information** area.
2. In the Package Information page, click **Package Location** to display the Package Locations page.
3. Select the appropriate locations, up to the number of locations allowed for your package.
4. Click **Save** to save the changes.

To view package host information or select hosts for Client Monitor:

1. Select **Admin** > **Platform** > **Data Collection** > **Package Information** to open the **Package Information** area.
2. In the Package Information page, click **Package Host** to display the Package Hosts for Client Monitor page.
3. Select the appropriate hosts, up to the number of hosts allowed for your package.
4. Click **Save** to save the changes.

Viewing and Modifying Package Properties Information

The Package Properties page displays information about the customer package for specific applications (Business Process Monitor, Client Monitor, and SiteScope). This information is entered in Mercury Business Availability Center when the contract is signed with Mercury. You can modify only the subscribed recipients.

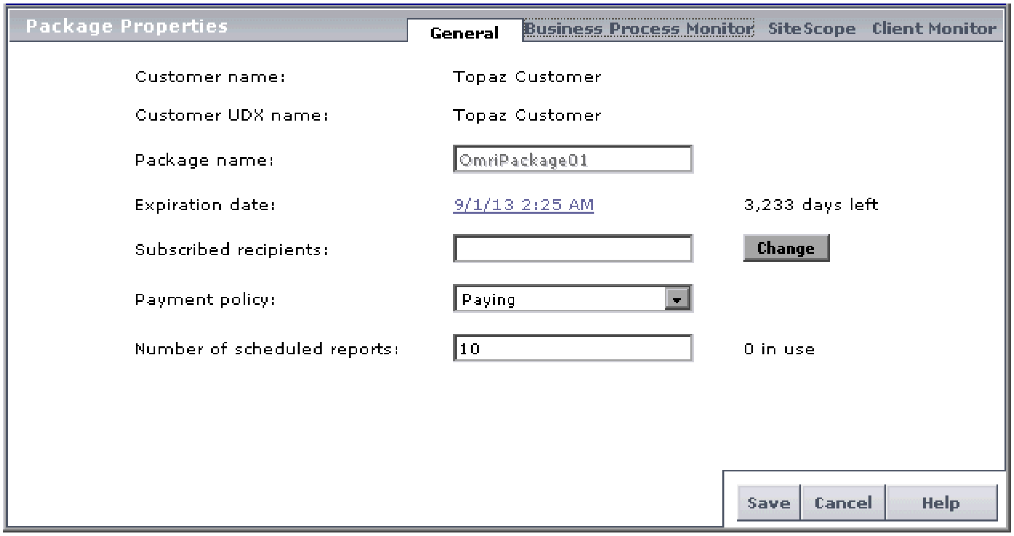
Modifying the Subscribed Recipients and Viewing the General Package Properties Information

The Package Properties area > **General** tab displays general information about the package.

To modify the subscribed recipients and view the general package properties information:

1. Select **Admin** > **Platform** > **Data Collection** > **Package Information** to open the **Package Information** area.

2 In the Package Information page, click **Edit** to display the Package Properties page. Click the **General** tab:



Package Properties

Customer name:	Topaz Customer	
Customer UDX name:	Topaz Customer	
Package name:	OmriPackage01	
Expiration date:	9/1/13 2:25 AM	3,233 days left
Subscribed recipients:		Change
Payment policy:	Paying	
Number of scheduled reports:	10	0 in use

3 You can view the names of the recipients who will receive package expiration notices via e-mail in the **Subscribed recipients** field. Click **Change** to open the Select Recipients page. For details, see “Assigning Recipients” on page 99.

- If you are a paying customer, the appropriate recipient will receive a package expiration notice via e-mail 14 days before the due date.
- If you are an evaluation customer, the appropriate recipient will receive a package expiration notice via e-mail 7 days before the due date.

4 You can also view the following information:

- **Customer name.** The name of the customer.
- **Package name.** The name of the package.
- **Expiration date.** The expiration date of the package. The number to the right of the box indicates the number of days left before the package expiration date.
- **Number of scheduled reports.** Number of scheduled reports included in the package. The number to the right of the box indicates the number of scheduled reports that have already been configured.

5 Click **Save** to save your changes.

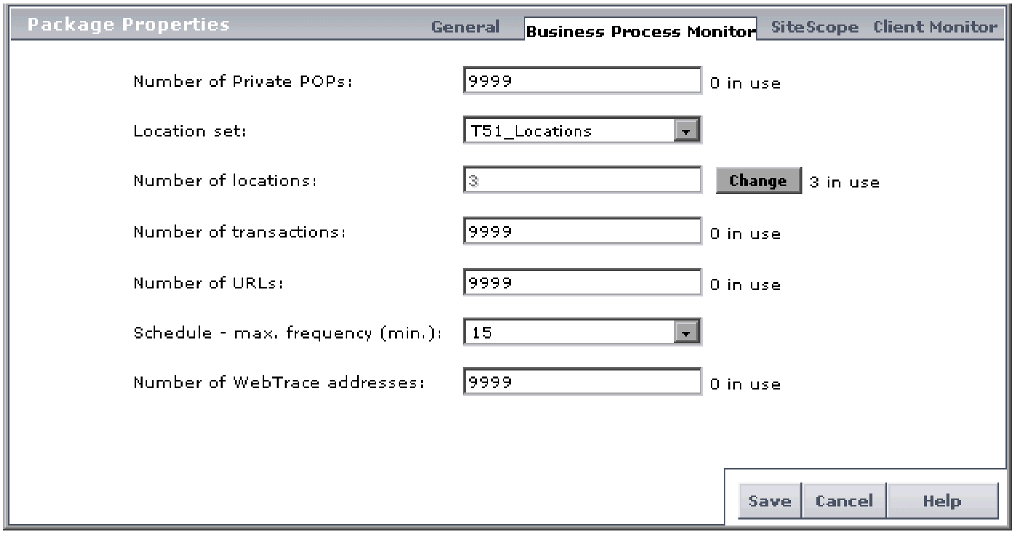
Viewing Business Process Monitor Package Properties Information

The Package Properties area > **Business Process Monitor** tab displays package information related to Business Process Monitors.

To view Business Process Monitor package properties information:

1 Select **Admin** > **Platform** > **Data Collection** > **Package Information** to open the **Package Information** area.

2 In the Package Information page, click **Edit** to display the Package Properties page. Click the **Business Process Monitor** tab:



Number of Private POPs: 9999 0 in use

Location set: T51_Locations

Number of locations: 3 3 in use

Number of transactions: 9999 0 in use

Number of URLs: 9999 0 in use

Schedule - max. frequency (min.): 15

Number of WebTrace addresses: 9999 0 in use

3 View the following information:

- **Number of private POPs.** The number of private POPs allowed for this package. The number to the right of the box indicates the number of private POPs already in use.
- **Number of locations.** The number of locations allowed by the package. The number to the right of the box indicates the number of locations already in use.

- **Number of transactions.** The number of transactions allowed by the package. The number to the right of the box indicates the number of transactions already in use.
- **Number of URLs.** The number of single URLs monitors allowed by the package. The number to the right of the box indicates the number of URLs already in use.
- **Schedule - max. frequency (min.).** The maximum frequency in minutes that your profiles can be scheduled to run.
- **Number of WebTrace addresses.** The number of WebTrace addresses allowed for this package. The number to the right of the box indicates the number of WebTrace addresses already being monitored.

4. Click **Save** to save your changes.

Viewing SiteScope Package Properties Information

The Package Properties area **- SiteScope** tab displays package information related to SiteScopes.

To view SiteScope package properties information:

1. Select **Admin** > **Platform** > **Data Collection** > **Package Information** to open the **Package Information** area.
2. In the Package Information page, click **Edit** to display the Package Properties page. Click the **SiteScope** tab.
3. You can view the following information:
   - **Number of SiteScope profiles.** The number of SiteScope profiles allowed for this package. The number to the right of the box indicates the number of SiteScope profiles already in use.
4. Click **Save** to save your changes.

Viewing Client Monitor Package Properties Information

The Package Properties area > **Client Monitor** tab displays package information related to Client Monitor Agents.

To view Client Monitor package properties information:

1. Select **Admin** > **Platform** > **Data Collection** > **Package Information** to open the **Package Information** area.

2 In the Package Information page, click **Edit** to display the Package Properties page. Click the **Client Monitor** tab.

3 You can view the following information:

- ➤ **Number of private POPs.** The number of private POPs allowed for this package. The number to the right of the box indicates the number of private POPs already in use.
- ➤ **Number of transactions.** The number of transactions allowed for this package. The number to the right of the box indicates the number of transactions already in use.
- ➤ **Number of traceroute addresses.** The number of traceroute addresses allowed for this package. The number to the right of the box indicates the number of traceroute addresses already in use.

4 Click **Save** to save your changes.

Part III

Alerts Management

15

Configuring and Selecting Recipients

Mercury Business Availability Center enables you to define and configure recipients for alerts, scheduled reports, and subscription and package notifications (Mercury Managed Services customers only).

About Defining Recipients

You define recipients in the Recipients page of Platform Administration. For each recipient, you define one or more notification method, the template to use for alert notices, and a notification schedule.

You can:

- define new recipients – for details, see page 182
- select recipients for receiving alerts, notifications, and scheduled reports – for details, see page 190
- edit or delete existing recipient properties – for details, see page 192

You can define the following types of notification methods:

- e-mail – for details, see page 185
- pager – for details, see page 188
- SMS – for details, see page 189

Note: Only those recipients who have been configured to receive e-mail can be selected to receive scheduled reports and are listed in Available Recipients when configuring scheduled reports.

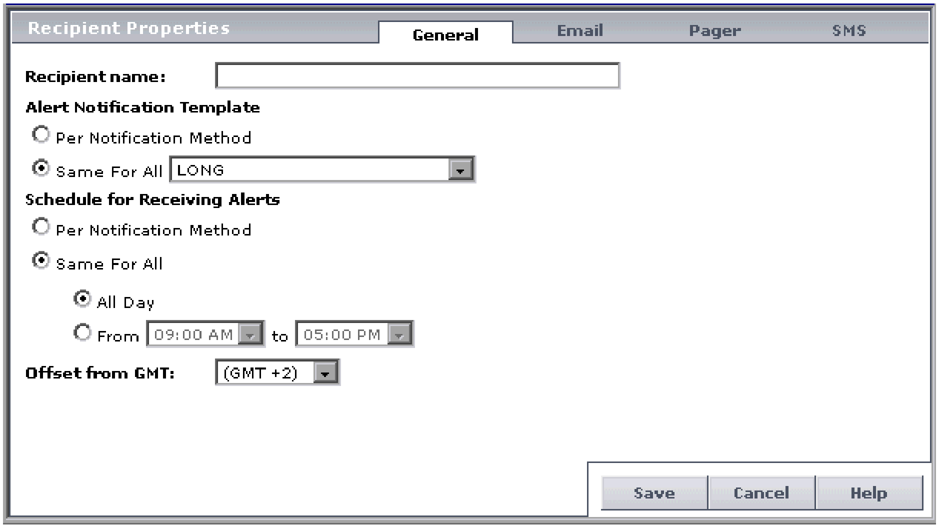
Defining a Recipient

You define recipients and how notices are sent to those recipients in the Recipients page of Platform Administration.

To define recipients:

1. Select **Admin** > **Platform** > **Alerts and Recipients** > **Recipients** to open the Recipients page.

2 Click the **New Recipient** button to define a new recipient. The Recipient Properties dialog box opens.



Recipient name:

Alert Notification Template

○ Per Notification Method

● Same For All LONG

Schedule for Receiving Alerts

○ Per Notification Method

● Same For All

● All Day

○ From 09:00 AM to 05:00 PM

Offset from GMT: (GMT +2)

3 Type the recipient's name in the **Recipient name** box.

4 Specify an alert notification template:

- ➤ Select **Per notification method** if you want the recipient's alert notification template to differ for each notification method, for example, if you want to use the LONG template for e-mail alerts and the SHORT template for pager alerts.
- ➤ Select **Same for all** if you want the recipient's alert notification template to be identical for all notification methods. Choose **LONG**, **SHORT**, or any custom template already created.

For details on alert notification templates and creating custom templates, see "About Alert Notification Templates" on page 265.

Note: You must select the alert notification template and specify an alert notices schedule for recipients who are to receive alerts and you do not have to for recipients who are to receive only scheduled reports.

---

5 Specify a schedule for receiving notifications. The schedule enables you to control exactly at what hours of the day a recipient receives notices.

➤ Select **Per notification method** if you want the recipient's schedule to differ for each notification method, for example, if you want a recipient to receive notices via e-mail from 9:00 AM to 5:00 PM, and via pager from 5:00 PM to 7:00 PM.

➤ Select **Same for all** if you want the recipient's schedule to be identical for all notification methods.

- To instruct Mercury Business Availability Center to send messages any time of the day, select **All Day**.
- To limit the time of day that Mercury Business Availability Center sends messages, select the time range option, and specify a time range.

6 In the **Offset from GMT** box, specify the time zone according to which Mercury Business Availability Center sends alert notices and Mercury Managed Services notifications to the selected recipient.

➤ The GMT offset selected for the recipient is the time zone specified in the alert notifications that the recipient receives. For example, if an alert is triggered anywhere in the world and a notification is sent, the date and time of the alert is converted to the time zone in the GMT offset selected for the recipient.

➤ If you defined a schedule for the recipient to receive notifications, the GMT offset selected for the recipient is also the time zone that Mercury Business Availability Center uses for calculating when to send the recipient notifications. For example, if you configure a recipient to receive pager alerts from 9:00 AM - 9:00 PM, and choose a GMT offset of -5 hours, the recipient will receive alerts via pager only from 9:00 AM - 9:00 PM Eastern Time.

Note: Scheduled reports are sent based on the schedule configured in the Scheduled Reports page and not on the schedule configured for the recipient. For details, see Chapter 19, "Scheduled Reports."

For a reference list of GMT time zones for locations throughout the world, see “GMT Time Zones” in *Reference Information*.

7 Specify how you want the recipient to receive notices: e-mail, pager, or short message service (SMS). You can select more than one method for a recipient receiving alerts or Mercury Managed Services notifications. Recipients receiving scheduled reports must be configured to receive e-mail.

For details on configuring notification methods, see “Specifying Notification Methods” on page 185.

8 Click **Save** to save the recipient settings and close the Recipient Properties dialog box. The recipient’s name appears in the Recipients list.

Specifying Notification Methods

You specify one or more notification methods for each recipient you define.

If you selected the **Per notification method** alert notification template option for the recipient, you also set template information for each notification method.

If you selected the **Per notification method** scheduling option for the recipient, you also set schedule information for each notification method.

You can specify any of the following notification methods:

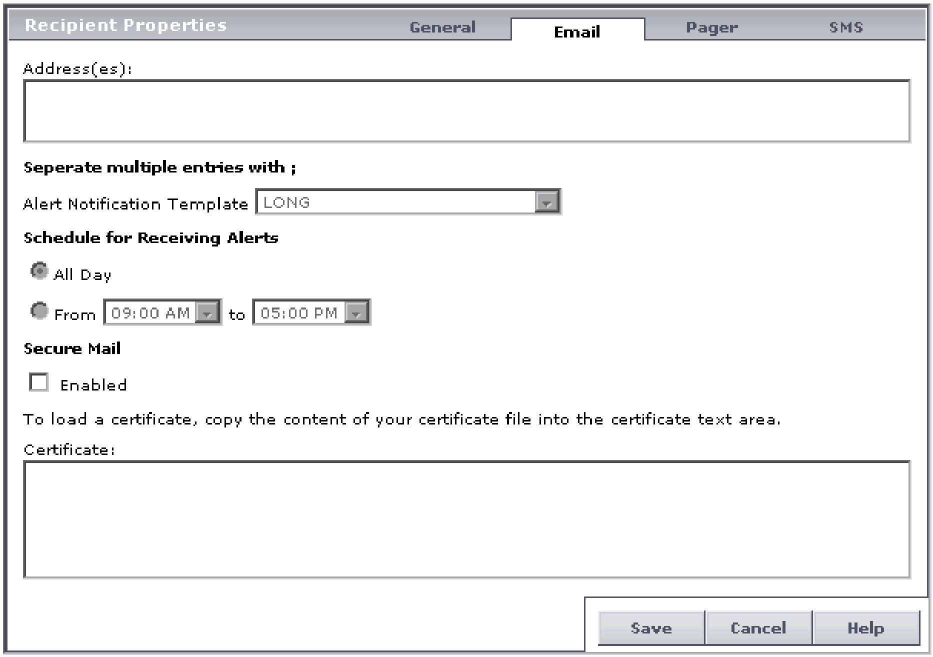
- e-mail
- pager
- SMS

E-mail Messages

You configure Mercury Business Availability Center to send e-mail notifications to one or more e-mail address.

To configure e-mail notification method:

1 In Platform Administration, select **Alerts and Recipients** > **Recipients**. Access the Recipient Properties dialog box by clicking the **New Recipient** button or the edit button next to an existing recipient. Select the **E-mail** tab.



Recipient Properties

Address(es):

Seperate multiple entries with ;

Alert Notification Template: LONG

Schedule for Receiving Alerts

● All Day

○ From 09:00 AM to 05:00 PM

Secure Mail

□ Enabled

To load a certificate, copy the content of your certificate file into the certificate text area.

Certificate:

2 Type one or more e-mail addresses in the **Address(es)** box. Separate multiple entries with a semi-colon (;).

3 If you selected the **Per notification method** alert notification template option for the recipient, choose the template you want to use. Choose **LONG**, **SHORT**, or any custom template already created.

For details on alert notification templates and creating custom templates, see "About Alert Notification Templates" on page 265.

4 If you selected the **Per notification method** scheduling option for the recipient, choose whether you want the recipient to receive e-mail messages all day, or only between the specified time range.

The time range will be calculated based on the GMT offset selected for the recipient.

Note: Scheduled reports are sent based on the schedule configured in the Scheduled Reports page and not on the schedule configured for the recipient. For details, see Chapter 19, "Scheduled Reports."

5 Optionally, you can specify that you want the recipient to receive encrypted mail by checking the **Enabled** option under **Secure Mail** and copying into the text box the contents of the certificate that the recipient used to secure incoming e-mail messages.

Note:

- The encrypted mail option is supported only for alerts. Encrypted mail is not supported for scheduled reports or subscription and package notifications (Mercury Managed Services customers only).
- The encrypted mail option is supported only when the Mercury Business Availability Center Core Server is installed on a Windows machine.

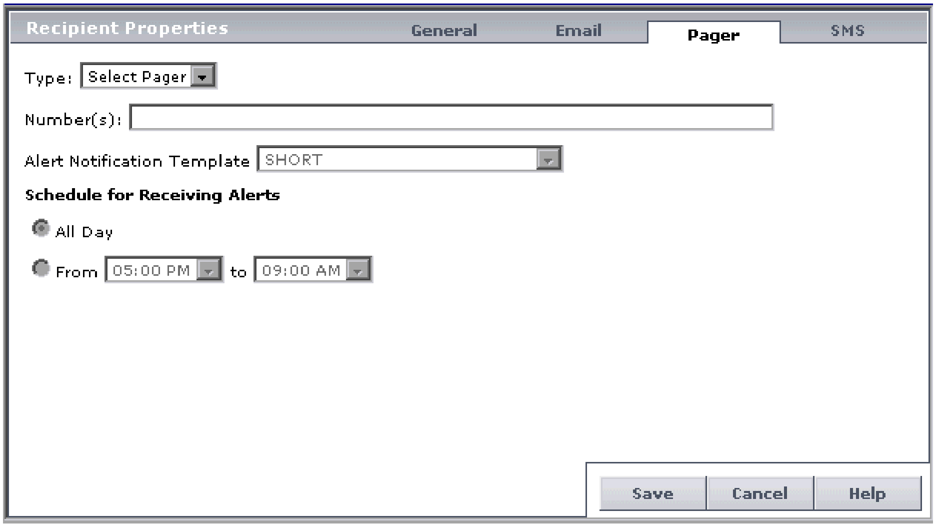
6 Click **Save** to save the settings, or to specify an additional notification method, select its tab.

Pager Messages

You configure Mercury Business Availability Center to send pager messages, via the specified pager service provider, to one or more pager access numbers.

To configure pager messages:

1 In the Recipient Properties dialog box, select the **Pager** tab.



Type: Select Pager

Number(s):

Alert Notification Template SHORT

Schedule for Receiving Alerts

● All Day

○ From 05:00 PM to 09:00 AM

2 Select a pager service provider from the Provider list.

3 Type one or more pager access numbers in the Numbers box. Separate multiple entries with a semi-colon (;).

4 If you selected the **Per notification method** alert notification template option for the recipient, choose the template you want to use. Choose **LONG**, **SHORT**, or any custom template already created.

For details on alert notification templates and creating custom templates, see “About Alert Notification Templates” on page 265.

5 If you selected the **Per notification method** scheduling option for the recipient, choose whether you want the recipient to receive pager messages all day, or only between the specified time range.

6 Click **Save** to save the settings, or to specify an additional notification method, select its tab.

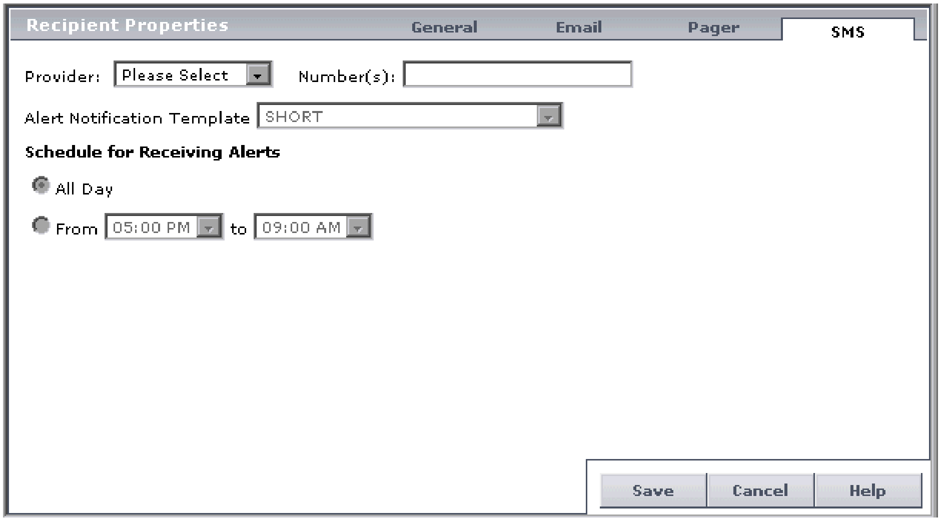
SMS Messages

You configure Mercury Business Availability Center to send SMS (short message service) messages, via the specified SMS service provider, to one or more SMS access numbers.

SMS is a text messaging service provided by most GSM-based cellular phone providers. SMS messages are useful to notify staff who are mobile, or who do not have e-mail or pager access. Note that the maximum message length of SMS text messages is generally 160 characters.

To configure SMS messages:

1 In the Recipient Properties dialog box, select the **SMS** tab.



Provider: Please Select Number(s):

Alert Notification Template SHORT

Schedule for Receiving Alerts

● All Day

○ From 05:00 PM to 09:00 AM

2 Select an SMS service provider from the **Provider** list.

3 Type one or more SMS access numbers in the **Numbers** box. Separate multiple entries with a semi-colon (;).

4 If you selected the **Per notification method** alert notification template option for the recipient, choose the template you want to use. Choose **LONG**, **SHORT**, or any custom template already created.

For details on alert notification templates and creating custom templates, see “About Alert Notification Templates” on page 265.

5 If you selected the **Per notification method** scheduling option for the recipient, choose whether you want the recipient to receive SMS messages all day, or only between the specified time range.

6 Click **Save** to save the settings, or to specify an additional notification method, select its tab.

Selecting Recipients

Once you define a recipient, the recipient is added to the list of available recipients in the Select Recipients dialog box. The Select Recipients dialog box opens when selecting recipients for:

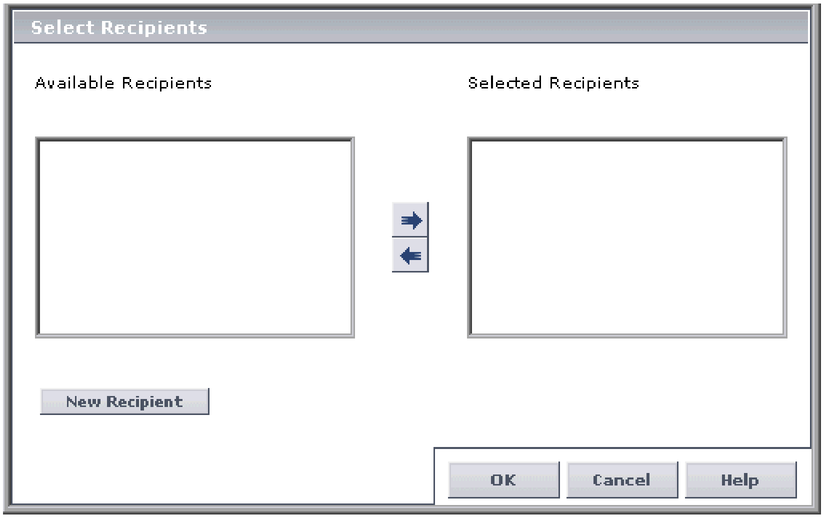
- **Alerts.**
  - **Profile alerts.** For details, see “Creating Alert Schemes” on page 193.
  - **SLA status alerts.** For details, see “SLA Status Alerts” in *Application Administration*.
  - **CI status alerts.** For details, see “Configuring CI Status Alerts” in *Application Administration*.
- **Scheduled reports.** For details on defining scheduled reports, see “Scheduled Reports” on page 299.
- **System notifications** (Mercury Managed Services only). For details on viewing current and archive system notifications, see “System Tickets for Mercury Managed Services” on page 95.
- **Package information** (Mercury Managed Services only). For details on viewing package information, see “Package Information” on page 172.

To select recipients:

1 When performing the following, the Select Recipients dialog box opens.

- configuring alerts
- defining scheduled reports

- selecting recipients for system and package information notifications (Mercury Managed Services only)



2 Select the recipient(s) to whom you want notifications sent from the **Available Recipients** list, and use the upper arrow to move your selection(s) to the **Selected Recipients** list. You can select multiple recipients using the CTRL key.

To define a new recipient, click **New Recipient**. For details on defining recipients, see "Configuring and Selecting Recipients" on page 181.

3 Click **OK** to close the Select Recipients dialog box.

To remove a specified recipient from the selection:

1 In the Select Recipients dialog box, select the recipient you want to remove from the **Selected Recipients** list, and use the lower arrow to remove the recipient. After removing, the recipient appears in the **Available Recipients** list. You can select multiple recipients using the CTRL key.

2 Click **OK** to close the Select Recipients dialog box.

Editing and Deleting Recipients

You can edit the properties of recipients or delete existing recipients.

To edit recipient properties:

1. Select **Admin** > **Platform** > **Alerts and Recipients** > **Recipients** to open the Recipients page.
2. Click the **Modify Recipient Properties** button beside the recipient whose properties you want to modify. The Recipient Properties window opens.
3. Modify settings as required, and click **Save**.

To delete an existing recipient:

1. Select **Admin** > **Platform** > **Alerts and Recipients** > **Recipients** to open the Recipients page.
2. In the Recipients table, click the **Delete Recipient** button beside the recipient's name, or select one or more recipients and click the **Delete Selected** button at the bottom of the table. Confirm that you want to delete the recipient.

16

Creating Alert Schemes

Mercury Business Availability Center alerts proactively inform you when predefined performance limits are breached. To instruct Mercury Business Availability Center under what conditions to send alerts, you create alert schemes using the Alert Wizard. You can specify alert filters, trigger criteria, actions, and settings.

About Creating Alert Schemes

Once you create a Business Process or Client Monitor profile, you create one or more alert schemes for the profile, using the Alert Wizard. In each alert scheme, you define a unique set of alert properties. You can add as many alert schemes to your Business Process or Client Monitor profile as required.

You use the Alert Wizard to:

- define alert trigger criteria
- define alert trigger criteria for the Real User Monitor
- specify alert filters
- configure alert actions
- configure additional alert settings

After you create an alert scheme, you view and edit it in the Alerts table. For details, see “Viewing an Alert Scheme” on page 259 and “Managing Alert Schemes” on page 260.

You can also create alert schemes for:

- SiteScope monitors using Monitor Administration. For details, see “Welcome to Configuring SiteScope Alerts” in *Configuring SiteScope Alerts*.
- configuration items in the CI Status Alerts tab in Dashboard Administration. You create these alert schemes to notify users of changes in a CI’s KPI. For details, see “Configuring CI Status Alerts” in *Application Administration*.

Tips for Creating Effective Alert Schemes

Before creating alert schemes, you should consider how to most effectively alert personnel to performance issues. The information described below can assist you with effective alert planning.

Note: Mercury Services offers best practice consulting on this subject. For information on how to obtain this service, contact your Mercury representative.

- When creating alert schemes, categorize alerts by severity. Create critical alerts for events that require immediate corrective action, for example, transaction failure, or excessive response times for critical transactions. Create non-critical alerts for events that require early notification, for example, slow response times.
- Determine the personnel that will receive the different types of alerts, and consider the alert delivery method that best suits the alert type. For example, pager, as opposed to e-mail, delivery might be more effective for critical alerts. When determining delivery method, take the time of day into account as well. For example, e-mail alerts might not be effective during non-business hours.
- Set Mercury Business Availability Center to alert you to a recurring problem, not one-time events. Alerts that are recurring are the most accurate indicator of problems with your application. The rule of thumb is that you should set the number of events in a row to the number of Business Process Monitor locations from which you are monitoring. For example, if you had three failures, but you were monitoring from 100 locations, it would not be as critical as if you had five failures in all five locations.
- Consider the following guidelines when specifying alert trigger criteria:
    - Set your alerts to about 10-20% over your average times.
    - Use the following values for transaction response time alert triggers: 4 seconds for general transactions, like loading a home page; 10 seconds for more complex transactions, like searching; 12 seconds for the most complex activities, like logging to the database.

- ➤ If you configure transaction thresholds in profiles to be similar to thresholds established in your organization's service level agreements, you can use threshold-based alerts to alert you to performance issues related to deviation from SLA criteria.

Creating an Alert Scheme

To create an alert scheme using the Alert Wizard, you perform the following steps:

1 **Select a profile.**

In **Admin** > **Platform** > **Alerts and Recipients** > **Alerts**, select the profile for which you want to create the alert from the list of profiles at the top of the page.

If you are creating an alert for a Real User Monitor, select the **[RUM Engines]** item from the profile list.

Note: If you are a licensed Mercury Diagnostics user, you can create alerts for Diagnostics by selecting the **[Diagnostics Alerts]** item from the profile list. For details on creating Diagnostics alerts, refer to the Mercury Diagnostics documentation.

---

2 **Open the Alert Wizard.**

Access the Alert Wizard by clicking **New Alert**.

If **[All Profiles]** was selected in the profile list when you clicked **New Alert**, the New Alert dialog box for selecting a profile opens and you must select a profile before continuing.

If **[RUM Engines]** was selected in the profile list when you clicked **New Alert**, the New Alert dialog box opens and you must select a Real User Monitor engine as well as the type of alert (page, transaction, server, or end-user) before continuing.

3 **Define the alert trigger criteria.**

You define the transaction response time and availability criteria that trigger the alert. For details, see "Defining Alert Trigger Criteria" on page 197.

4 **Set the alert filters.**

You set alert filters that enable you to customize the alert scheme for more accurate alerting. For details, see "Setting Alert Filters" on page 232.

5 **Configure the alert action settings.**

You specify what actions you want Mercury Business Availability Center to take when alert trigger criteria are met. For details, see "Configuring Alert Actions" on page 238.

6 **Configure additional alert settings.**

You specify various settings, including alert name, label, and status. For details, see "Configuring Additional Alert Settings" on page 254.

When creating an alert scheme in the Alert Wizard, click **Finish** to save your settings and close the Alert Wizard. Mercury Business Availability Center adds the alert scheme to the Alerts table.

Click **Cancel** to close the Alert Wizard without saving the settings.

Defining Alert Trigger Criteria

Alert trigger criteria enable you to specify the transaction response time and availability conditions that trigger an alert. You can choose to trigger the alert based on either an event related to the transaction's success or failure, or based on the time it takes for the transaction to be completed.

You define the alert trigger criteria from the Trigger Criteria tab of the Alert Wizard.

If you are defining alert criteria for a Real User Monitor alert, see "Configuring Alert Triggers for the Real User Monitor" on page 212.

If you are defining alert criteria for a Business Process Monitor or Client Monitor profile, you can choose from the following two types of alert trigger criteria:

- **event-based triggers**

  Event-based triggers enable Mercury Business Availability Center to send alerts when a specific event occurs, for example, when a transaction fails or exceeds a specified amount of time.

  For details on configuring event-based triggers, see page 198.

- **time-based triggers**

  Time-based triggers enable Mercury Business Availability Center to send alerts when specific conditions exist over a specified period of time, for example, when average transaction response time is greater than 10 seconds for a period of 1 hour.

  If you select multiple, time-based alert trigger criteria, you also specify multiple trigger condition properties.

  If you set alert filters, Mercury Business Availability Center considers trigger criteria within the context of the selected items only.

  For details on configuring time-based triggers, see page 203.

Note: An alert scheme can contain either event-based trigger criteria exclusively or time-based trigger criteria exclusively.

Configuring Event-Based Triggers

When configuring event-based trigger criteria, you also specify alert frequency criteria for each trigger selected. For example, you can specify that the alert must be sent if the trigger conditions occur 3 times out of 5. For details, see “Defining Alert Frequency Criteria” on page 202.

The following event-based triggers are available:

- Transaction failure – for details, see page 199
- Transaction response time – for details, see page 199
- Transaction response time relative to threshold – for details, see page 200

Transaction Failure

If you select this trigger, Mercury Business Availability Center sends an alert if transactions fail.

To send an alert if transactions fail:

1 In the upper box, select **Transactions fail**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Send alert if trigger conditions occur** to set the alert frequency criteria.

For details on setting alert frequency criteria, see "Defining Alert Frequency Criteria" on page 202.

3 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

If you select multiple alert triggers, see "Selecting Multiple Triggers" on page 211.

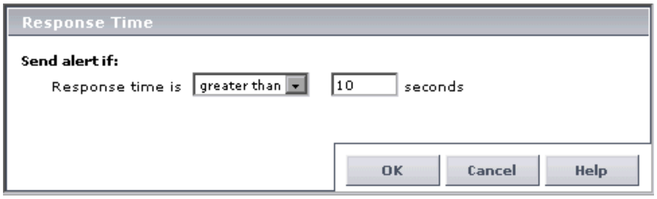
Transaction Response Time

If you select this trigger, Mercury Business Availability Center sends an alert if transaction response time is greater than or less than the selected number of seconds. Note that only completed transactions are considered. If a transaction fails—that is, is not completed successfully—no alert will be sent.

To send an alert based on response time:

1 In the upper box, select **Transaction response time**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Transaction response time** to configure the trigger. The Response Time dialog box opens.



Response Time

Send alert if:

Response time is greater than 10 seconds

3 Specify the required criteria. For example, specify **greater than** and **10** to instruct Mercury Business Availability Center to send the alert if response time is greater than 10 seconds.

4 Click **OK** to close the Transaction Response Time dialog box.

5 In the lower box, click the linked value in the sentence that begins **Send alert if trigger conditions occur** to set the alert frequency criteria.

For details on setting alert frequency criteria, see “Defining Alert Frequency Criteria” on page 202.

6 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

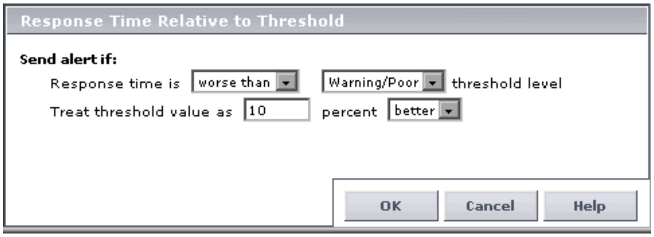
If you select multiple alert triggers, see “Selecting Multiple Triggers” on page 211.

Transaction Response Time Relative to Threshold

If you select this trigger, Mercury Business Availability Center sends an alert if transaction response time is better or worse than the selected transaction threshold. Note that only completed transactions are considered.

In addition, you can instruct Mercury Business Availability Center to treat the threshold value as better or worse than the set threshold, by a specified percentage.

In the example below, Mercury Business Availability Center sends the alert if response time for a given transaction is worse than the set Warning/Poor level threshold, but treats the threshold value as 10 percent better. Thus, if the Warning/Poor level threshold for the transaction is, for example, 10 seconds, Mercury Business Availability Center sends an alert if transaction response time is worse than 9 seconds (since 9 seconds is 10 percent better than 10 seconds).



Response Time Relative to Threshold

Send alert if:

Response time is worse than Warning/Poor threshold level

Treat threshold value as 10 percent better

You configure transaction thresholds in Monitor Administration. For details, see “Transaction Threshold Settings” in *End User Management Data Collector Configuration*.

To send an alert based on response time relative to threshold:

1 In the upper box, select **Transaction response time relative to threshold**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Transaction response time relative to threshold is** to configure the trigger. The Response Time Relative to Threshold dialog box opens.

3 Select the required threshold criteria. For example, select **worse than** and **Warning/Poor** to instruct Mercury Business Availability Center to send the alert if response time is worse than the set Warning/Poor threshold.

   Further, specify whether Mercury Business Availability Center should treat the set threshold value as better or worse, and by what percentage. For example, select **10** percent and **better** to instruct Mercury Business Availability Center to treat the threshold value as 10 percent better than the value set in the Business Process profile.

Note: Transaction thresholds for Business Process profiles are set in Monitor Administration. For details see "Configuring Profile, Host, and Monitor Settings" in *End User Management Data Collector Configuration*.

4 Click **OK** to close the Response Time Relative to Threshold dialog box.

5 In the lower box, click the linked value in the sentence that begins **Send alert if trigger conditions occur** to set the alert frequency criteria.

For details on setting alert frequency criteria, see "Defining Alert Frequency Criteria" on page 202.

6 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

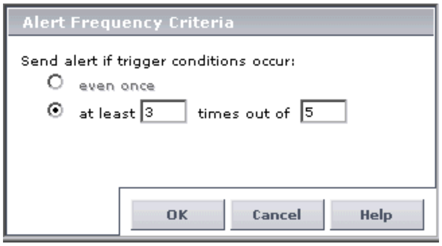
If you select multiple alert triggers, see "Selecting Multiple Triggers" on page 211.

Defining Alert Frequency Criteria

You define how often Mercury Business Availability Center sends an alert notice when the event-based alert trigger conditions defined above occur. If you selected any of the event-based alert triggers, you can define the alert frequency criteria.

To define alert frequency criteria:

1 In the lower box, click the linked value in the sentence that begins **Send alert if trigger conditions occur**. The Alert Frequency Criteria dialog box opens.



Alert Frequency Criteria

Send alert if trigger conditions occur:

○ even once

● at least 3 times out of 5

2 Select the required frequency criteria:

- Select **Even once** to have Mercury Business Availability Center send an alert every time the defined alert trigger conditions occur.
- Select **At least X times out of Y** to have Mercury Business Availability Center send an alert only when the defined alert trigger conditions occur X times out of Y, where X represents the number of times the alert conditions occur, and Y represents the total number of transaction instances Mercury Business Availability Center considers.

  For example: for the alert trigger **Transactions fail**, if you specify **at least 3 times out of 5**, Mercury Business Availability Center sends an alert only if 3 out of every 5 transactions fail; for the alert trigger **Transaction response time is greater than 10 seconds**, if you specify **At least 2 times out of 4**, Mercury Business Availability Center sends an alert only if transaction response time is greater than 10 seconds in at least 2 out of 4 transaction instances.

3 Click **OK** to save the settings and close the Alert Frequency Criteria dialog box.

Configuring Time-Based Triggers

When configuring time-based trigger criteria, you also specify the time period over which to calculate the trigger. For example, you can specify that the alert must be sent if the trigger conditions exist for a period of 15 minutes.

The following time-based triggers are available:

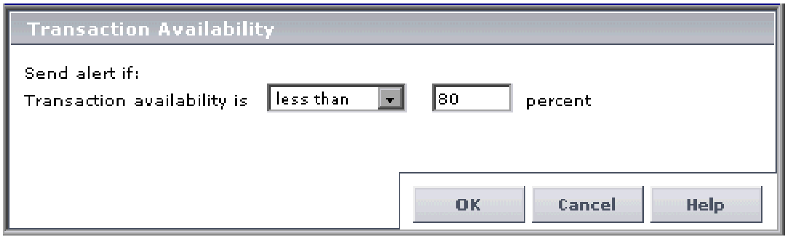
- Availability – for details, see page 204
- Transaction response time for specified percentage of transactions – for details, see page 205
- Transaction response time relative to threshold for specified percentage of transactions – for details, see page 207
- Average transaction response time – for details, see page 210

Availability

If you select this trigger, Mercury Business Availability Center sends an alert if transaction availability is greater than or less than the selected percentage, calculated over the selected time period. Transaction availability is defined as the number of times that transactions succeed as a percentage of the total number of transaction instances.

To send an alert based on availability:

1. In the upper box, select **Availability**. The trigger appears in the lower box.
2. In the lower box, click the linked value next to **Availability is** to configure the trigger. The Transaction Availability dialog box opens.

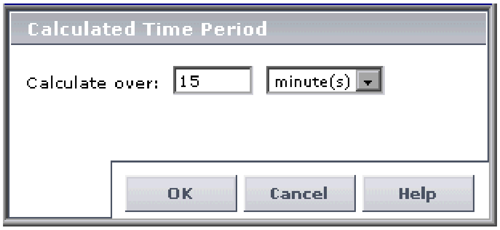


Transaction Availability

Send alert if:

Transaction availability is less than 80 percent

3. Select the required criteria. For example, select **less than** and **80** to instruct Mercury Business Availability Center to send the alert if transaction availability is less than 80 percent, over the calculated time period (which you configure in step 6).
4. Click **OK** to close the Transaction Availability dialog box.
5. In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates availability. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 15 minute(s)

6 Specify the required time period. Continuing the example from step 3, select **15** and **minute(s)** to instruct Mercury Business Availability CenterMercury Business Availability Center to send the alert if transaction availability is less than 95 percent, over a 15 minute-period.

7 Click **OK** to close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

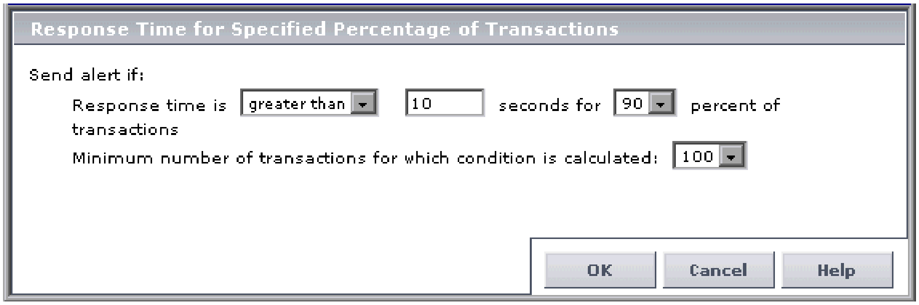
If you select multiple alert triggers, see "Selecting Multiple Triggers" on page 211.

Transaction Response Time for Specified Percentage of Transactions

If you select this trigger, an alert is sent if response time is greater or less than the selected number of seconds, for the specified percentage of transactions, calculated over the selected time period. Only completed transactions are considered for this alert trigger.

In addition, you can instruct Mercury Business Availability Center to count a minimum number of transactions over the calculated time period.

In the example below, Mercury Business Availability Center sends the alert if transaction response time is greater than 10 seconds for 90 percent of all transaction instances that occur over the calculated time period (which you set in a separate dialog box). Further, the alert is only sent if at least 100 transactions occur during the calculated time period.



Response Time for Specified Percentage of Transactions

Send alert if:

Response time is greater than 10 seconds for 90 percent of transactions

Minimum number of transactions for which condition is calculated: 100

To send an alert based on response time for a specified percentage of transactions:

1 In the upper box, select **Transaction response time for specified percentage of transactions**. The trigger appears in the lower box.

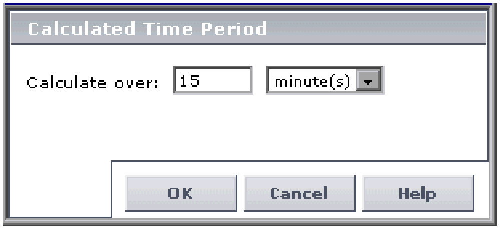
2 In the lower box, click the linked value in the sentence that begins **Transaction response time for specified percentage of transactions is** to configure the trigger. The Response Time for Specified Percentage of Transactions dialog box opens.

3 Select the required response time and percentage criteria. For example, select **greater than**, **7 seconds**, and **50 percent** to instruct Mercury Business Availability Center to send the alert if response time is greater than 7 seconds for 50 percent of transaction instances, over the calculated time period (which you configure in step 6).

Further, select the minimum number of transactions to count. For example, select **50** to instruct Mercury Business Availability Center to send the alert only if there are at least 50 transaction instances over the calculated time period.

4 Click **OK** to close the Response Time for Specified Percentage of Transactions dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center considers transactions. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 15 minute(s)

6 Specify the required time period. Continuing the example from step 3, select **2** and **hour(s)** to instruct Mercury Business Availability Center to send the alert if response time is greater than 7 seconds for 50 percent of all transaction instances that occur over a 2-hour period, but only if there were at least 50 transaction instances during the 2 hours.

7. Click **OK** to close the Calculated Time Period dialog box.
8. Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

   If you select multiple alert triggers, see “Selecting Multiple Triggers” on page 211.

Transaction Response Time Relative to Threshold for Specified Percentage of Transactions

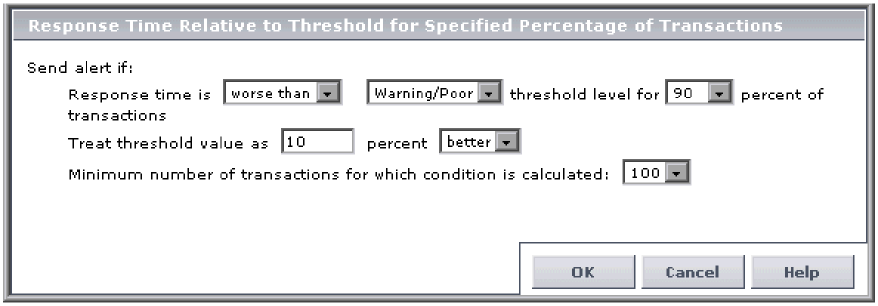
If you select this trigger, Mercury Business Availability Center sends an alert if response time is better or worse than the selected transaction threshold, for the specified percentage of transactions, calculated over the selected time period. Only completed transactions are considered for triggering this alert.

In addition, you can instruct Mercury Business Availability Center to:

- treat the threshold value as better or worse than the set threshold, by a specified percentage
- count a minimum number of transactions over the calculated time period

In the following example, Mercury Business Availability Center sends the alert if response time is worse than the set Warning/Poor level threshold for 90 percent of all transaction instances that occur over the calculated time period (which you set in a separate dialog box). In addition, Mercury Business Availability Center treats the threshold value as 10 percent better, and the alert is only sent if at least 100 transactions occur during the calculated time period.

Thus, if the Warning/Poor level threshold for the transaction is, for example, 10 seconds, and there are, for example, 120 transactions during the calculated time period, Mercury Business Availability Center sends an alert if transaction response time for at least 108 transactions (120 x 90%) is worse than 9 seconds (since 9 seconds is 10 percent better than 10 seconds).



Response Time Relative to Threshold for Specified Percentage of Transactions

Send alert if:

Response time is worse than Warning/Poor threshold level for 90 percent of transactions

Treat threshold value as 10 percent better

Minimum number of transactions for which condition is calculated: 100

You configure transaction thresholds in Monitor Administration. For details, see “Transaction Threshold Settings” in *End User Management Data Collector Configuration*.

To send an alert based on response time relative to threshold for a specified percentage of transactions:

1 In the upper box, select **Transaction response time relative to threshold for specified percentage of transactions**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Transaction response time relative to threshold for specified percentage of transactions is** to configure the trigger. The Response Time Relative to Threshold for Specified Percentage of Transactions dialog box opens.

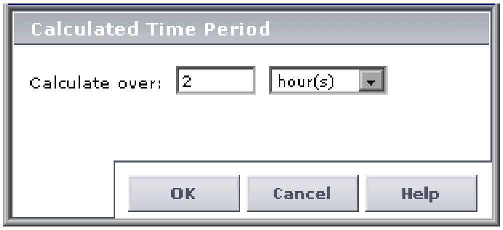
3 Select the required threshold and percentage criteria. For example, select **worse than**, **Warning/Poor**, and **90 percent** to instruct Mercury Business Availability Center to send the alert if response time is worse than the set Warning/Poor threshold for 90 percent of transaction instances, over the calculated time period (which you configure in step 6).

Further, specify the following criteria:

- whether Mercury Business Availability Center should treat the set threshold value as better or worse, and by what percentage. For example, select **10 percent** and **better** to instruct Mercury Business Availability Center to treat the threshold value as 10 percent better than the value set in the Business Process profile.
- the minimum number of transactions to count. For example, select **100** to instruct Mercury Business Availability Center to send the alert only if there are at least 100 transaction instances over the calculated time period.

4 Click **OK** to close the Response Time Relative to Threshold for Specified Percentage of Transactions dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center considers transactions. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 2 hour(s)

6 Specify the required time period. Continuing the examples from step 3, select **2** and **hour(s)** to instruct Mercury Business Availability Center to send the alert if response time is worse than the set Warning/Poor threshold (treated as 10 percent better than the set value) for 90 percent of transaction instances that occur over a 2-hour period, but only if there were at least 100 transaction instances during the 2 hours.

7 Click **OK** to close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

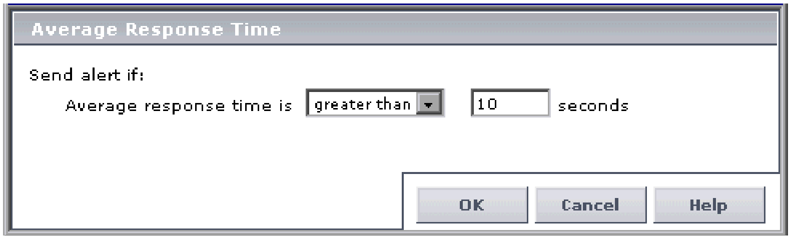
If you select multiple alert triggers, see "Selecting Multiple Triggers" on page 211.

Average Transaction Response Time

If you select this trigger, Mercury Business Availability Center sends an alert if average transaction response time is greater than or less than the selected number of seconds, calculated over the selected time period. Only completed transactions are considered when triggering this alert.

To send an alert based on average response time:

1. In the upper box, select **Average transaction response time**. The trigger appears in the lower box.
2. In the lower box, click the linked value in the sentence that begins **Average transaction response time is** to configure the trigger. The Average Response Time dialog box opens.

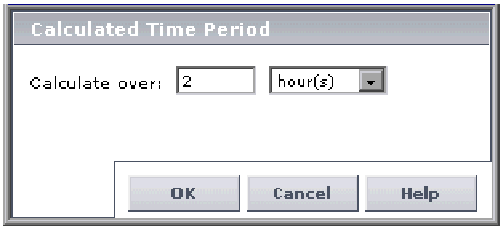


Average Response Time

Send alert if:

Average response time is greater than 10 seconds

3. Select the required criteria. For example, select **greater than** and **10** to instruct Mercury Business Availability Center to send the alert if average response time is greater than 10 seconds, over the calculated time period (which you configure in step 6).
4. Click **OK** to close the Average Response Time dialog box.
5. In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates average response time. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 2 hour(s)

6 Specify the required time period. Continuing the example from step 3, select **2** and **hour(s)** to instruct Mercury Business Availability Center to send the alert if average response time is greater than 10 seconds, over a 2-hour period.

7 Click **OK** to close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

If you select multiple alert triggers, see "Selecting Multiple Triggers" on page 211.

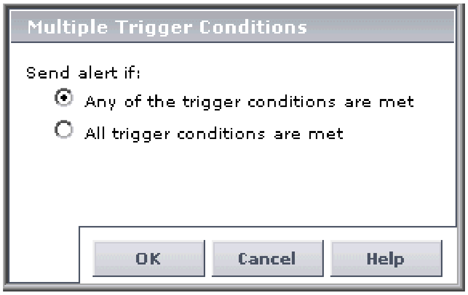
Selecting Multiple Triggers

If you select multiple time-based alert trigger criteria, you specify whether you want Mercury Business Availability Center to send the alert:

- if any of the trigger conditions are met
- only if all the time-based trigger conditions are met

To specify multiple trigger condition properties:

1 In the lower box, click the linked value in the sentence **Send alert if <specified> trigger conditions are met**. The Multiple Trigger Conditions dialog box opens.



Multiple Trigger Conditions

Send alert if:

● Any of the trigger conditions are met

○ All trigger conditions are met

2 Select the required setting.

3 Click **OK** to close the Multiple Trigger Conditions dialog box.

Calculating Alert Trigger Time Periods

By default, the Calculated Time Period dialog box displays a time period of either 2 hours or 15 minutes, depending on the trigger you are configuring. If you want to specify a different time period for your alert trigger, you can change the number and time unit accordingly.

For example, if you set an alert trigger for an average response time that is greater than 10 seconds, and you set the time period in the Calculated Time Period dialog box to 45 minutes, Mercury Business Availability Center sends an alert if the average response time exceeds 10 seconds at any time over a 45-minute period.

For details on defining alert criteria for a Business Process Monitor or Client Monitor profile, see “Defining Alert Trigger Criteria” on page 197.

For details on defining alert criteria for the Real User Monitor, see “Configuring Alert Triggers for the Real User Monitor” on page 212.

Configuring Alert Triggers for the Real User Monitor

The alert trigger criteria that you can configure for the Real User Monitor depend on the alert type you selected in the New Alert dialog box.

The following alert types are available:

- Page Alerts – for details, see below
- Transaction Alerts – for details, see page 219
- Server Alerts – for details, see page 228
- End-User Alerts – for details, see page 230

Page Alerts

If you selected to define criteria for a page alert, you can select one or more of the following triggers in the Alert Wizard’s Trigger Criteria tab:

- Page Availability – for details, see below
- Page Performance - Page Response Time for Specified Percentage of Pages – for details, see page 214

- Page Performance - Server Response Time for Specified Percentage of Pages – for details, see page 216
- Page Volume – for details, see page 217

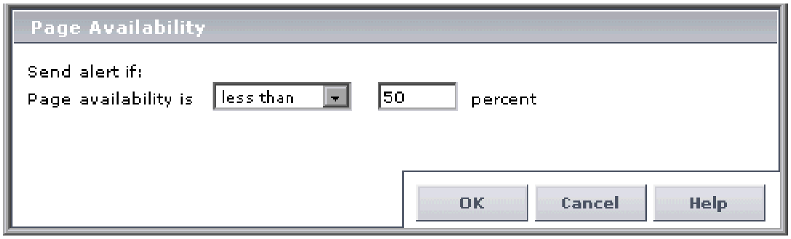
Note: Page alerts will only be sent for pages that you configure in Monitor Administration.

Page Availability

If you select this trigger, Mercury Business Availability Center sends an alert if page availability is less than or greater than the specified percentage, calculated over the selected time period.

To send an alert based on page availability:

1. In the upper box, select **Page availability**. The trigger appears in the lower box.
2. In the lower box, click the linked value in the sentence that begins **Page availability is** to configure the trigger. The Page Availability dialog box opens.



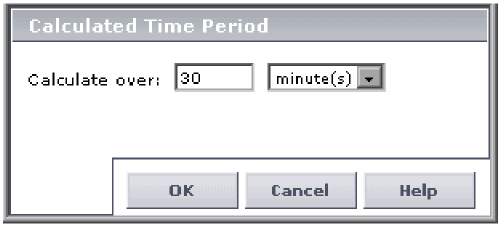
Page Availability

Send alert if:

Page availability is less than 50 percent

3. Select the required criteria. For example, select **less than** and **50** to instruct Mercury Business Availability Center to send the alert if page availability is less than 50 percent, over the calculated time period (which you configure in step 6).
4. Click **OK** to save your settings and close the Page Availability dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates page availability. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 30 minute(s)

6 Specify the required time period. Continuing the example from step 3, select **30** and **minute(s)** to instruct Mercury Business Availability Center to send the alert if page availability is less than 50 percent, over a 30-minute period.

7 Click **OK** to save your settings and close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

If you select multiple alert triggers, see “Selecting Multiple Triggers” on page 211.

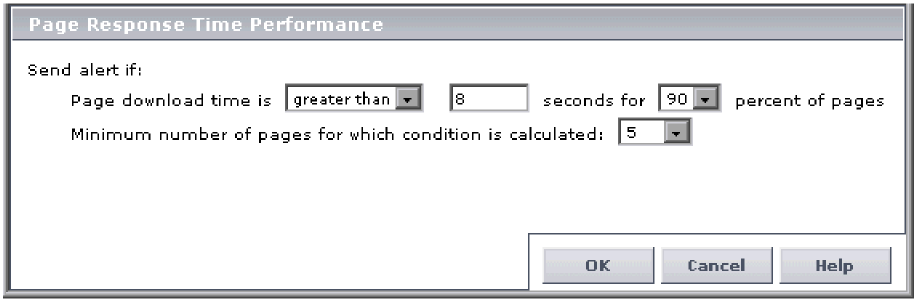
Page Performance - Page Response Time for Specified Percentage of Pages

If you select this trigger, Mercury Business Availability Center sends an alert if page download time is greater than or less than the selected number of seconds for no less than the specified percentage of pages, calculated over the selected time period. You can also set a minimum number of pages that must be downloaded in order for the alert conditions to be calculated.

To send an alert based on page response time performance:

1 In the upper box, select **Page performance - page response time for specified percentage of pages**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Page response time for** to configure the trigger. The Page Response Time Performance dialog box opens.



Page Response Time Performance

Send alert if:

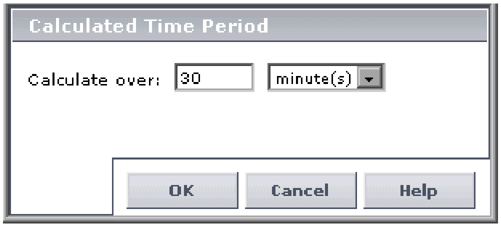
Page download time is greater than 8 seconds for 90 percent of pages

Minimum number of pages for which condition is calculated: 5

3 Select the required criteria. For example, select **greater than**, enter a value of **8** seconds, and select **90** percent to instruct Mercury Business Availability Center to send the alert if page response time exceeds 8 seconds for at least 90 percent of the downloaded pages, over the calculated time period (which you configure in step 6). Select a minimum number of pages that must be downloaded in order for the above conditions to be calculated.

4 Click **OK** to save your settings and close the Page Response Time Performance dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates page response time performance. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 30 minute(s)

6 Specify the required time period. Continuing the example from step 3, select **30** and **minute(s)** to instruct Mercury Business Availability Center to send the alert if page response time is greater than 8 seconds for 90 percent of the downloaded pages, over a 30-minute period.

7 Click **OK** to save your settings and close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

If you select multiple alert triggers, see “Selecting Multiple Triggers” on page 211.

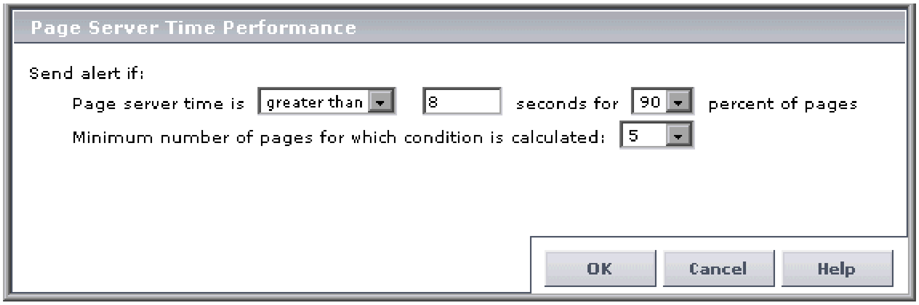
Page Performance - Server Response Time for Specified Percentage of Pages

If you select this trigger, an alert is sent if the page server time is greater than or less than the selected number of seconds for no less than the selected percentage of pages, calculated over the selected time period. You can also set a minimum number of pages that must be downloaded in order for the alert conditions to be calculated.

To send an alert based on page server time performance:

1 In the upper box, select **Page performance - server response time for specified percentage of pages**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Server response time for** to configure the trigger. The Page Server Time Performance dialog box opens.



Page Server Time Performance

Send alert if:

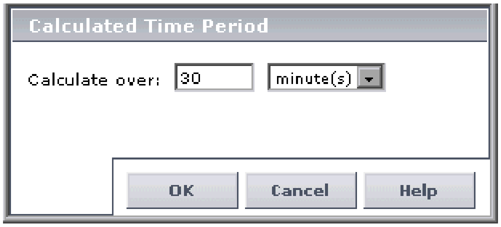
Page server time is greater than 8 seconds for 90 percent of pages

Minimum number of pages for which condition is calculated: 5

3 Select the required criteria. For example, select **greater than**, enter a value of **8** seconds, and select **90** percent to instruct Mercury Business Availability Center to send the alert if server response time exceeds 8 seconds for at least 90 percent of the downloaded pages, over the calculated time period (which you configure in step 6). Select a minimum number of pages that must be downloaded in order for the above conditions to be calculated.

4 Click **OK** to save your settings and close the Page Server Time Performance dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates page server time performance. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 30 minute(s)

6 Specify the required time period. Continuing the example from step 3, select **30** and **minute(s)** to instruct Mercury Business Availability Center to send the alert if server response time is greater than 8 seconds for 90 percent of the downloaded pages, over a 30-minute period.

7 Click **OK** to save your settings and close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

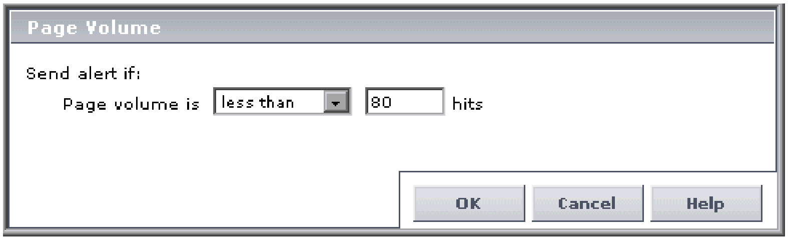
If you select multiple alert triggers, see “Selecting Multiple Triggers” on page 211.

Page Volume

If you select this trigger, Mercury Business Availability Center sends an alert if the number of page hits is less than or greater than the specified number, calculated over the selected time period.

To send an alert based on page volume:

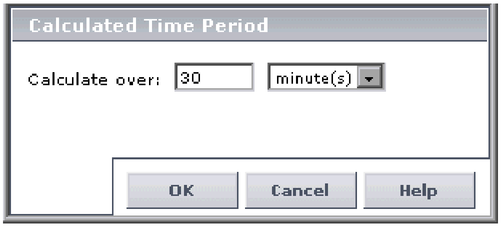
1. In the upper box, select **Page volume**. The trigger appears in the lower box.
2. In the lower box, click the linked value in the sentence that begins **Page volume is** to configure the trigger. The Page Volume dialog box opens.


Page Volume

Send alert if:

Page volume is less than 80 hits

3. Select the required criteria. For example, select **less than** and **80** to instruct Mercury Business Availability Center to send the alert if there were fewer than 80 page hits, over the calculated time period (which you configure in step 6).
4. Click **OK** to save your settings and close the Page Volume dialog box.
5. In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates page volume. The Calculated Time Period dialog box opens.


Calculated Time Period

Calculate over: 30 minute(s)

6. Specify the required time period. Continuing the example from step 3, select **30** and **minute(s)** to instruct Mercury Business Availability Center to send the alert if there were fewer than 80 hits to the page, over a 30-minute period.
7. Click **OK** to save your settings and close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

If you select multiple alert triggers, see "Selecting Multiple Triggers" on page 211.

Transaction Alerts

If you selected to define criteria for a transaction alert, you can select one or more of the following triggers in the Alert Wizard's Trigger Criteria tab:

- Transaction Availability – for details, see below
- Transaction Performance - Total Response Time for Specified Percentage of Transactions – for details, see page 221
- Transaction Performance - Net Response Time for Specified Percentage of Transactions – for details, see page 222
- Transaction Performance - Server Response Time for Specified Percentage of Transactions – for details, see page 224
- Total Transaction Volume – for details, see page 225
- Completed Transaction Volume – for details, see page 227

Note: Transaction alerts will only be sent for transactions that you configure in Monitor Administration.

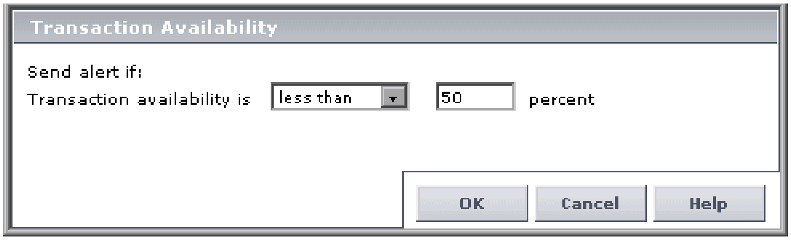
Transaction Availability

If you select this trigger, Mercury Business Availability Center sends an alert if transaction availability is less than or greater than the specified percentage, calculated over the selected time period.

To send an alert based on transaction availability:

1 In the upper box, select **Transaction availability**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Transaction availability is** to configure the trigger. The Transaction Availability dialog box opens.



Transaction Availability

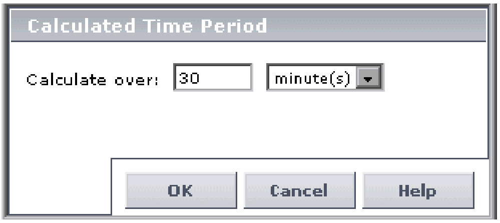
Send alert if:

Transaction availability is less than 50 percent

3 Select the required criteria. For example, select **less than** and **50** to instruct Mercury Business Availability Center to send the alert if transaction availability is less than 50 percent, over the calculated time period (which you configure in step 6).

4 Click **OK** to save your settings and close the Transaction Availability dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates transaction availability. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 30 minute(s)

6 Specify the required time period. Continuing the example from step 3, select **30** and **minute(s)** to instruct Mercury Business Availability Center to send the alert if transaction availability is less than 50 percent, over a 30-minute period.

7 Click **OK** to save your settings and close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

If you select multiple alert triggers, see "Selecting Multiple Triggers" on page 211.

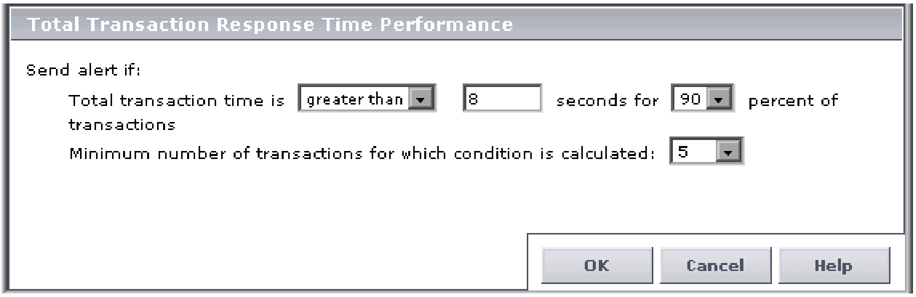
Transaction Performance - Total Response Time for Specified Percentage of Transactions

If you select this trigger, Mercury Business Availability Center sends an alert if total transaction time is greater than or less than the selected number of seconds for no less than the selected percentage of transactions, calculated over the selected time period. You can also set a minimum number of transactions that must run in order for the alert conditions to be calculated.

To send an alert based on total transaction response time performance:

1 In the upper box, select **Transaction performance - total transaction response time for specified percentage of transactions**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Total transaction response time for** to configure the trigger. The Total Transaction Response Time Performance dialog box opens.



Total Transaction Response Time Performance

Send alert if:

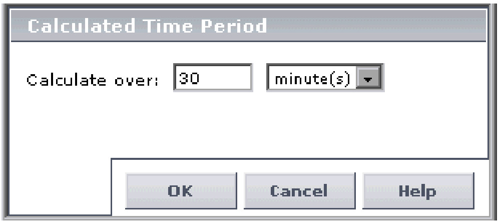
Total transaction time is greater than 8 seconds for 90 percent of transactions

Minimum number of transactions for which condition is calculated: 5

3 Select the required criteria. For example, select **greater than**, enter a value of **8** seconds, and select **90** percent to instruct Mercury Business Availability Center to send the alert if total transaction response time exceeds 8 seconds for at least 90 percent of the transactions that were run, over the calculated time period (which you configure in step 6). Select a minimum number of transactions that must run in order for the alert conditions to be calculated.

4 Click **OK** to save your settings and close the Total Transaction Response Time Performance dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates total transaction response time performance. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 30 minute(s)

6 Specify the required time period. Continuing the example from step 3, select **30** and **minute(s)** to instruct Mercury Business Availability Center to send the alert if total transaction response time is greater than 8 seconds for 90 percent of the transactions run, over a 30-minute period.

7 Click **OK** to save your settings and close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

If you select multiple alert triggers, see "Selecting Multiple Triggers" on page 211.

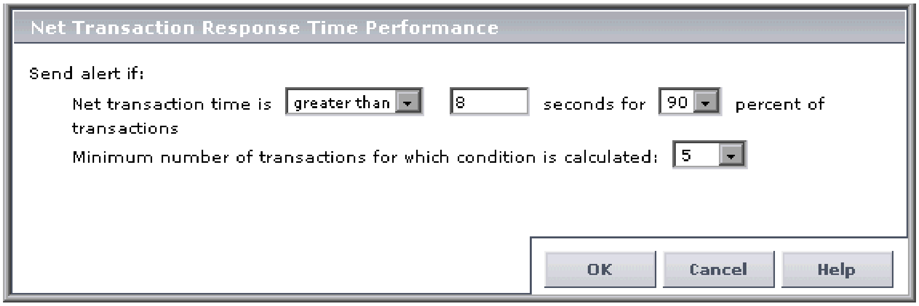
Transaction Performance - Net Response Time for Specified Percentage of Transactions

If you select this trigger, Mercury Business Availability Center sends an alert if net transaction time is greater than or less than the selected number of seconds for no less than the selected percentage of transactions, calculated over the selected time period. You can also set a minimum number of transactions that must run in order for the alert conditions to be calculated.

To send an alert based on net transaction response time performance:

1 In the upper box, select **Transaction performance - net transaction response time for specified percentage of transactions**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Net transaction response time for** to configure the trigger. The Net Transaction Response Time Performance dialog box opens.



Net Transaction Response Time Performance

Send alert if:

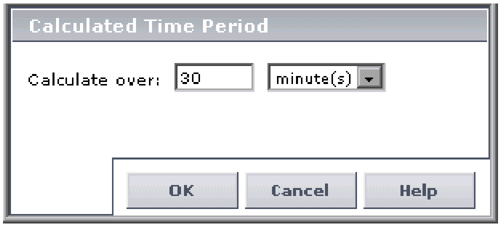
Net transaction time is greater than 8 seconds for 90 percent of transactions

Minimum number of transactions for which condition is calculated: 5

3 Select the required criteria. For example, select **greater than**, enter a value of **8** seconds, and select **90** percent to instruct Mercury Business Availability Center to send the alert if net transaction response time exceeds 8 seconds for at least 90 percent of the transactions that were run, over the calculated time period (which you configure in step 6). Select a minimum number of transactions that must run in order for the alert conditions to be calculated.

4 Click **OK** to save your settings and close the Net Transaction Response Time Performance dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates net transaction response time performance. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 30 minute(s)

6 Specify the required time period. Continuing the example from step 3, select **30** and **minute(s)** to instruct Mercury Business Availability Center to send the alert if net transaction response time is greater than 8 seconds for 90 percent of the transactions run, over a 30-minute period.

7 Click **OK** to save your settings and close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

If you select multiple alert triggers, see "Selecting Multiple Triggers" on page 211.

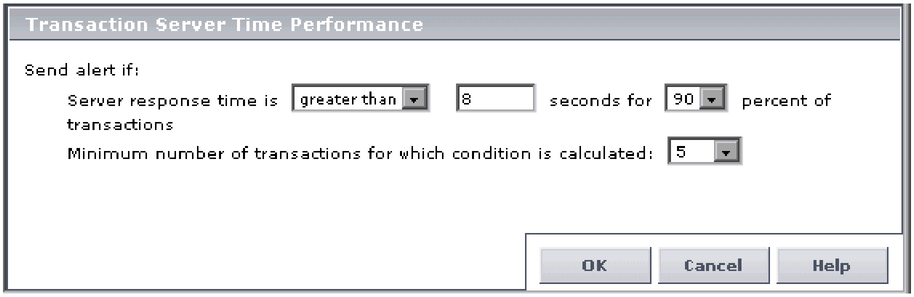
Transaction Performance - Server Response Time for Specified Percentage of Transactions

If you select this trigger, an alert is sent if transaction server time is greater than or less than the selected number of seconds for no less than the selected percentage of transactions, calculated over the selected time period. You can also set a minimum number of transactions that must run in order for the alert conditions to be calculated.

To send an alert based on transaction server time performance:

1 In the upper box, select **Transaction performance - server response time for specified percentage of transactions**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Server response time for** to configure the trigger. The Transaction Server Time Performance dialog box opens.



Transaction Server Time Performance

Send alert if:

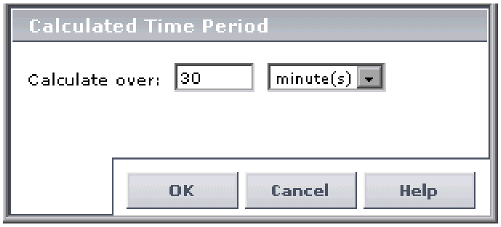
Server response time is greater than 8 seconds for 90 percent of transactions

Minimum number of transactions for which condition is calculated: 5

3 Select the required criteria. For example, select **greater than**, enter a value of **8** seconds, and select **90** percent to instruct Mercury Business Availability Center to send the alert if server response time exceeds 8 seconds for at least 90 percent of the transactions that were run, over the calculated time period (which you configure in step 6). Select a minimum number of transactions that must run in order for the alert conditions to be calculated.

4 Click **OK** to save your settings and close the Transaction Server Time Performance dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates transaction server time performance. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 30 minute(s)

6 Specify the required time period. Continuing the example from step 3, select **30** and **minute(s)** to instruct Mercury Business Availability Center to send the alert if server response time is greater than 8 seconds for 90 percent of the transactions that were run, over a 30-minute period.

7 Click **OK** to save your settings and close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

If you select multiple alert triggers, see “Selecting Multiple Triggers” on page 211.

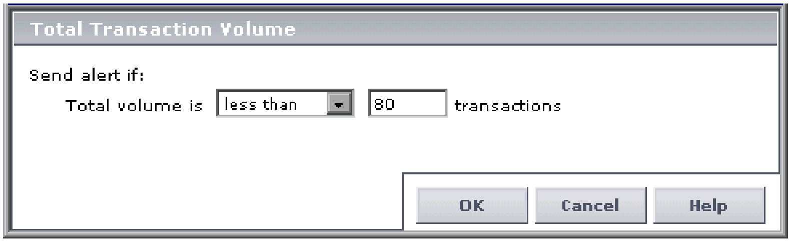
Total Transaction Volume

If you select this trigger, an alert is sent if the number of transaction runs is less than or greater than the specified number, calculated over the selected time period.

To send an alert based on total transaction volume:

1 In the upper box, select **Total transaction volume**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Total volume is** to configure the trigger. The Total Transaction Volume dialog box opens.


Total Transaction Volume

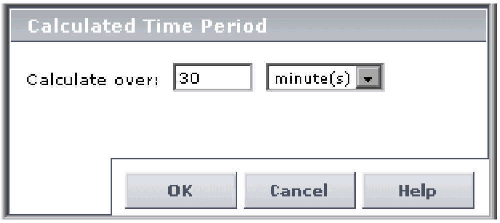
Send alert if:

Total volume is less than 80 transactions

3 Select the required criteria. For example, select **less than** and **80** to instruct Mercury Business Availability Center to send the alert if there were fewer than 80 transactions run, over the calculated time period (which you configure in step 6).

4 Click **OK** to save your settings and close the Total Transaction Volume dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates total transaction volume. The Calculated Time Period dialog box opens.


Calculated Time Period

Calculate over: 30 minute(s)

6 Specify the required time period. Continuing the example from step 3, select **30** and **minute(s)** to instruct Mercury Business Availability Center to send the alert if there were fewer than 80 transactions run, over a 30-minute period.

7 Click **OK** to save your settings and close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

If you select multiple alert triggers, see "Selecting Multiple Triggers" on page 211.

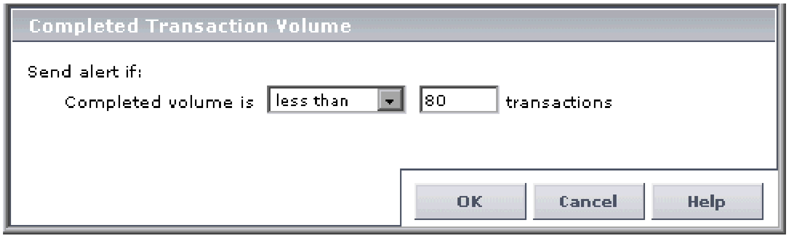
Completed Transaction Volume

If you select this trigger, Mercury Business Availability Center sends an alert if the number of completed transaction runs is less than or greater than the specified number, calculated over the selected time period.

To send an alert based on completed transaction volume:

1 In the upper box, select **Completed transaction volume**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Completed volume is** to configure the trigger. The Completed Transaction Volume dialog box opens.



Completed Transaction Volume

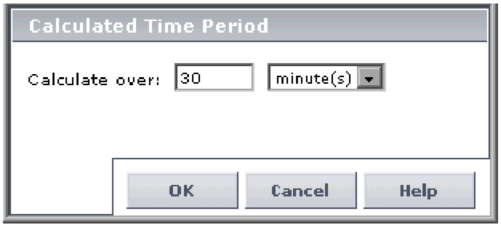
Send alert if:

Completed volume is less than 80 transactions

3 Select the required criteria. For example, select **less than** and **80** to instruct Mercury Business Availability Center to send the alert if there were fewer than 80 completed transaction runs, over the calculated time period (which you configure in step 6).

4 Click **OK** to save your settings and close the Completed Transaction Volume dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates completed transaction volume. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 30 minute(s)

6 Specify the required time period. Continuing the example from step 3, select **30** and **minute(s)** to instruct Mercury Business Availability Center to send the alert if there were fewer than 80 completed transaction runs, over a 30-minute period.

7 Click **OK** to save your settings and close the Calculated Time Period dialog box.

8 Select additional triggers, or click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

If you select multiple alert triggers, see “Selecting Multiple Triggers” on page 211.

Server Alerts

If you selected to define criteria for a server alert, you can select the following trigger in the Alert Wizard’s Trigger Criteria tab:

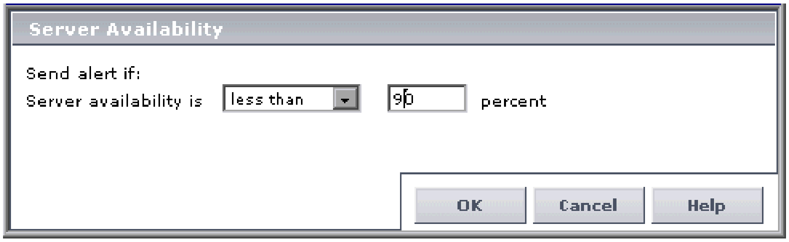
Server Availability

This trigger instructs Mercury Business Availability Center to send an alert if server availability is less than or greater than the specified percentage, calculated over the selected time period.

To send an alert based on server availability:

1 In the upper box, select **Server availability**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Server availability is** to configure the trigger. The Server Availability dialog box opens.



Server Availability

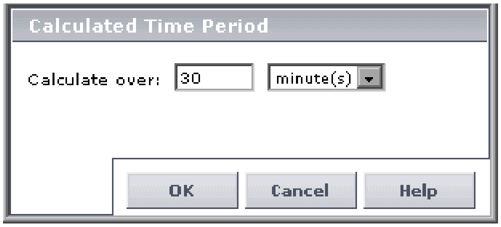
Send alert if:

Server availability is less than 90 percent

3 Select the required criteria. For example, select **less than** and **90** to instruct Mercury Business Availability Center to send the alert if server availability is less than 90 percent, over the calculated time period (which you configure in step 6).

4 Click **OK** to save your settings and close the Server Availability dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates server availability. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 30 minute(s)

6. Specify the required time period. Continuing the example from step 3, select **30** and **minute(s)** to instruct Mercury Business Availability Center to send the alert if server availability is less than 90 percent, over a 30-minute period.
7. Click **OK** to save your settings and close the Calculated Time Period dialog box.
8. Click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

End-User Alerts

If you selected to define criteria for an end-user alert, you can select the end-user performance trigger in the Alert Wizard's Trigger Criteria tab.

Note: End-user alerts will only be sent for end users that you configure in Monitor Administration.

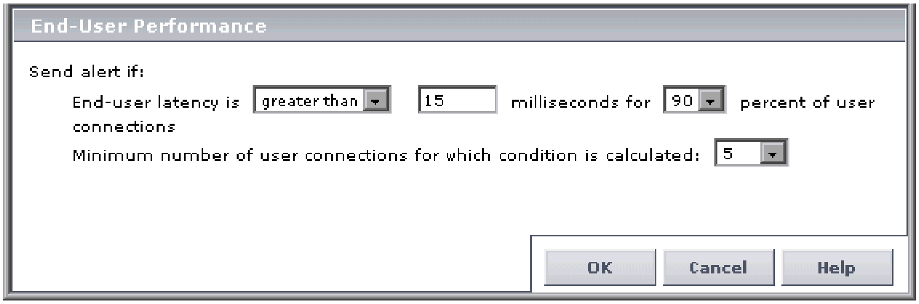
End-User Performance

This trigger instructs Mercury Business Availability Center to send an alert if end-user latency is greater than or less than the selected number of milliseconds for no less than the selected percentage of user connections, calculated over the selected time period. You can also set a minimum number of connections that must be made by end users in order for the alert conditions to be calculated.

To send an alert based on end-user performance:

1. In the upper box, select **End-user performance**. The trigger appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **End-user performance is** to configure the trigger. The End-User Performance dialog box opens.



End-User Performance

Send alert if:

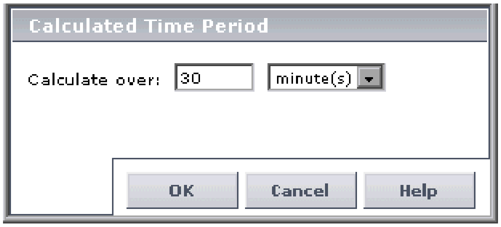
End-user latency is greater than 15 milliseconds for 90 percent of user connections

Minimum number of user connections for which condition is calculated: 5

3 Select the required criteria. For example, select **greater than**, enter a value of **15** milliseconds, and select **90** percent to instruct Mercury Business Availability Center to send the alert if end-user latency exceeds 15 milliseconds for at least 90 percent of end-user connections, over the calculated time period (which you configure in step 6). Select a minimum number of end-user connections that must be made in order for the alert conditions to be calculated.

4 Click **OK** to save your settings and close the End-User Performance dialog box.

5 In the lower box, click the linked value in the sentence that begins **Calculate over** to set the time period over which Mercury Business Availability Center calculates end-user performance. The Calculated Time Period dialog box opens.



Calculated Time Period

Calculate over: 30 minute(s)

6. Specify the required time period. Continuing the example from step 3, select **30** and **minute(s)** to instruct Mercury Business Availability Center to send the alert if end-user latency is greater than 15 milliseconds for 90 percent of end-user connections, over a 30-minute period.
7. Click **OK** to save your settings and close the Calculated Time Period dialog box.
8. Click the **Filters**, **Actions**, or **Settings** tab to continue creating an alert scheme.

Setting Alert Filters

Alert filters enable you to track performance issues related to specific monitored servers, monitors, or measurements.

You set the alert filters from the Alert Filters tab of the Alert Wizard.

You can filter the alerts that Mercury Business Availability Center sends based on the triggers you configured by:

- Grouping Performance Data – for details, see page 232
- Limiting Alerts to Specific Pages, Transactions, End Users, Servers, Locations and/or Groups – for details, see page 235

Mercury Business Availability Center determines which alerts are sent by how the alert triggers and alert filters are configured.

Grouping Performance Data

Mercury Business Availability Center sends an alert when a specific set of alert trigger criteria are met. By default, when assessing whether alert trigger criteria have been met, all the relevant performance data in the profile database (for example, when assessing whether a transaction has failed, all the transaction instances are checked) is considered.

You can instruct Mercury Business Availability Center to consider the performance data per transaction, per script (file containing transactions), per group, per location, or per any combination of the four.

If you are setting Real User Monitor alert filters, you can instruct Mercury Business Availability Center to consider the performance data per page name, per end-user name, per transaction name, and/or per server name, depending on the type of alert you are configuring. For more information on Real User Monitor alert filters, see "Setting Real User Monitor Alert Filters" on page 237.

Understanding How to Group Performance Data for Alert Filters

For example, let's say a profile contains two transactions, T1 and T2, both running from two locations, L1 and L2. Further, you want an alert to be triggered if average transaction response time is greater than 10 seconds. When assessing whether to send the alert, Mercury Business Availability Center has to consider the following data from the running profile:

Location	Transaction	Response Time (sec.)
L1	T1	12
L1	T2	11
L2	T1	12
L2	T2	1

Without the filter, Mercury Business Availability Center would calculate average response time as 9 seconds ((12+11+12+1)/4), and would thus not send an alert.

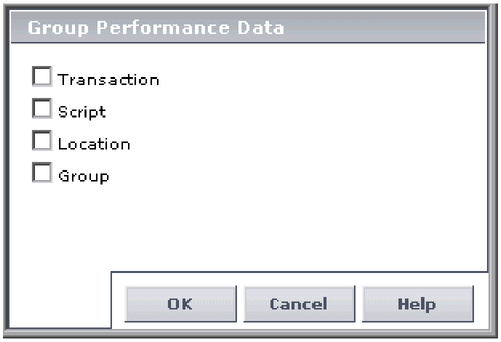
With the filter set to **Group performance data by transaction**, Mercury Business Availability Center would consider all instances of transaction T1 separately and all instances of transaction T2 separately. Since average response time for T1 is greater than 10 seconds ((12+12)/2), Mercury Business Availability Center would send an alert for T1. Since average response time for T2 is under 10 seconds ((11+1)/2), Mercury Business Availability Center would not send an alert for T2.

With the filter set to **Group performance data by location**, Mercury Business Availability Center would send an alert for location L1 but not for location L2.

With the filter set to **Group performance data by transaction and location**, Mercury Business Availability Center would consider all instances of transaction T1 from location L1 separately, all instances of T1 from L2 separately, all instances of T2 from L1 separately, and all instances of T2 from L2 separately. Mercury Business Availability Center would send an alert for T1 from L1 and T1 from L2, but not for T2 from L2.

To set the alert filters to group the performance data:

1. In the upper box of the **Filters** tab of the Alert Wizard, select the **Group performance data** check box. The selected filters appear in the lower box.
2. In the lower box, click the linked value in the sentence **Group performance data by <specified criteria>**. The Group Performance Data dialog box opens.



Group Performance Data

□ Transaction
□ Script
□ Location
□ Group

3. Select whether you want performance data grouped by:
   - **Transaction**
   - **Script**
   - **Location**
   - **Group**
   - any combination of the four

Note: For details on the options available when setting Real User Monitor alert filters, see “Setting Real User Monitor Alert Filters” on page 237.

---

4 Click **OK** to return to the Alert Wizard and the Filters tab.

Limiting Alerts to Specific Pages, Transactions, End Users, Servers, Locations and/or Groups

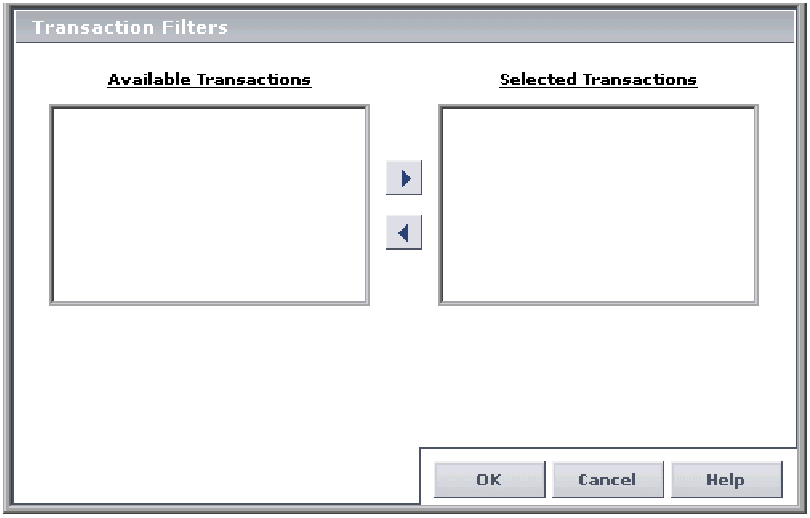
By default, Mercury Business Availability Center sends an alert when alert trigger criteria are met for any transaction, from any location or group, in the profile. By using any of these filters, you instruct Mercury Business Availability Center to limit the alert scheme to one or more specific transactions, locations, and/or groups.

Note: For the Real User Monitor, you can instruct Mercury Business Availability Center to limit the alert scheme to one or more specific pages, transactions, servers, end-user names, and/or end-user locations, depending on the type of alert you are configuring. For more information on Real User Monitor alert filters, see "Setting Real User Monitor Alert Filters" on page 237.

To set the alert filters:

1 In the upper box, select the check box beside the alert filter(s) you want to enable. The selected filter(s) appear in the lower box.

2 In the lower box, for each selected filter, click the <**as specified**> link to edit it. A Filters dialog box opens that is specific to the entity selected (transaction, location, or group—in this example, Transaction Filters).



3 Select the transaction(s), location(s), or group(s) for which you want alert notifications sent. Select from the **Available** list, and use the upper, right arrow to move your selection(s) to the **Selected** list. Use the lower, left arrow to remove an entity from the filter.

You can select multiple filters using the **CTRL** key.

4 Click **OK** to return to the Alert Wizard and the Filters tab.

Setting Real User Monitor Alert Filters

As with Business Process and Client Monitor profiles, you can filter the Real User Monitor alerts by:

- grouping performance data
- limiting alerts to specific data

The performance data by which you can group, and the data by which you can limit, a Real User Monitor alert scheme differ from other alert schemes. The grouping and limitation options also differ, depending on the type of Real User Monitor alert you are configuring.

The following table describes the grouping and limitation options available for each type of Real User Monitor alert:

Alert Type	Group Performance Data Options	Limitation Options
Page	Page name End-user name	Pages End-user names End-user locations
Transaction	Transaction name End-user name	Transactions End-user names End-user locations
Server	Server name	Servers
End-User	End-user name	End-user names End-user locations

Configuring Alert Actions

Alert actions enable you to specify the actions that Mercury Business Availability Center takes when alert trigger criteria are met.

You define the alert actions from the Alert Actions tab of the Alert Wizard.

You can choose from the following alert actions:

- send the alert to specified recipients – for details, see page 239
- include a specified user message in the alert – for details, see page 240
- access a URL when the alert is triggered – for details, see page 240
- send an SNMP trap when the alert is triggered – for details, see page 242
- run an executable file when the alert is triggered – for details, see page 243
- log an event to the Windows Event Viewer application log when the alert is triggered – for details, see page 245
- define alert dependency – for details, see page 247

Note: Regardless of the actions you select, each time alert trigger criteria are met, Mercury Business Availability Center logs an alert in the Alert Log, which you view on the Web site. For details on viewing the alert log, see "Alert Log" in *Using End User Management*.

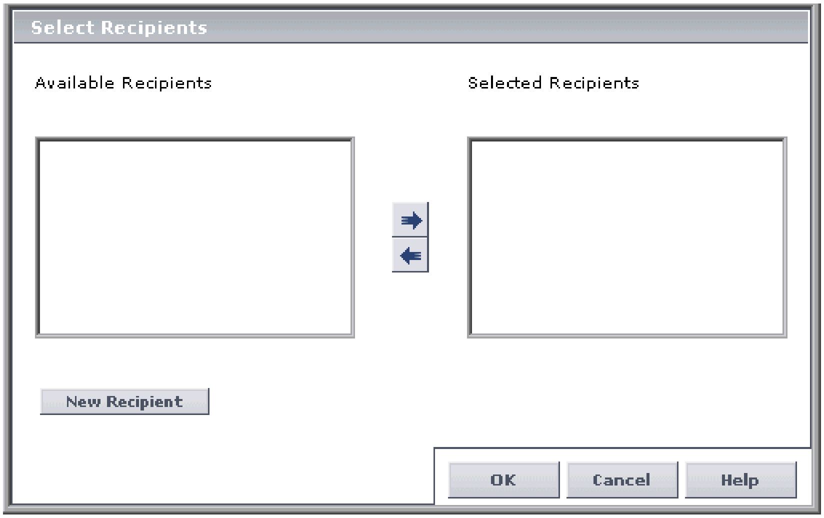
Sending an Alert to Specified Recipients

You specify the recipients that receive alert notices.

To specify recipients:

1 In the upper box, select **Send alert to specified recipients**. The action appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Send alert to**. The Select Recipients dialog box opens.



3 Select the recipient(s) to whom you want alert notifications sent from the **Available Recipients** list, and use the upper arrow to move your selection(s) to the **Selected Recipients** list. You can select multiple recipients using the CTRL key.

To define a new recipient, click **New Recipient**. For details on defining recipients, see Chapter 15, "Configuring and Selecting Recipients."

4 Click **OK** to close the Recipients dialog box.

To remove a specified recipient:

1 In the lower box, click the linked value in the sentence that begins **Send alert to**. The Select Recipients dialog box opens.

2 Select the recipients you want to remove from the **Selected Recipients** list, and use the lower arrow to remove them. You can select multiple recipients using the CTRL key.

Including a User Message in the Alert

You specify that you want to include a user message and type the message that you want Mercury Business Availability Center to include in the alert notices that recipients receive.

To include a user message:

1 In the upper box, select **Include user message**. The action appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Include the user message**. The Add User Message dialog box opens.

3 Type the required message, and click **OK**.

In addition to this message, Mercury Business Availability Center automatically sends a description of the alert to the Alert log, which can be viewed by selecting **End User Management** > **Alerts** from the Business Availability Center menu. For details, see “Alert Log” in *Using End User Management*.

Accessing a URL When the Alert Is Triggered

You specify that you want Mercury Business Availability Center to access a URL when alert trigger criteria are met. By accessing a URL, Mercury Business Availability Center can send alerts via a Web site, for example, using Active Server Pages, CGI, or Perl. The URL can activate an executable program on a Web server, report to a custom database, activate a Web-based fax service, and so forth. You can develop custom pages or use existing ones.

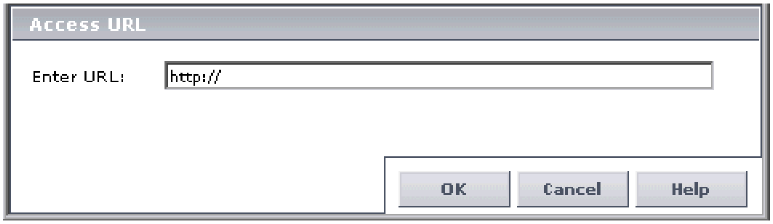
Note: Mercury Business Availability Center supports the GET method only when accessing a URL. If your Web server only supports the POST method, or if you want more information on developing custom Web pages for your server, please contact your Mercury Interactive Customer Support representative.

To access a URL:

1 In the upper box, select **Access URL(s)**. The action appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Access the URL(s)**. The Access URLs dialog box opens.

3 Click **Add URL** to add a new URL. The Access URL dialog box opens.



Access URL

Enter URL: http://

4 Type a URL in the **Enter URL** box.

For details on embedding predefined alert parameters in the URL, see “Using Custom Alert Parameters” on page 275.

5 Click **OK** to close the Access URL dialog box.

6 To add additional URLs, repeat steps 3 to 5.

7 Click **OK** to close the Access URLs dialog box.

Sending an SNMP Trap When the Alert Is Triggered

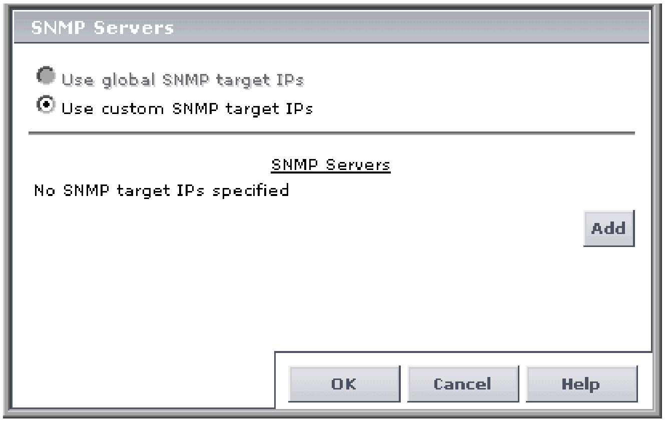
You specify that you want Mercury Business Availability Center to send an SNMP trap when alert trigger criteria are met. The alert notice can then be seen via any SNMP management console in the organization.

Note: Mercury Business Availability Center supports only SNMP V1 traps.

For details on configuring the Alerts MIB in your SNMP management console, see "Configuring the Alerts MIB" on page 285.

To send an SNMP trap:

1. In the upper box, select **Send SNMP trap**. The action appears in the lower box.
2. In the lower box, click the linked value in the sentence that begins **Send SNMP trap to**. The SNMP Servers dialog box opens.



SNMP Servers

○ Use global SNMP target IPs

● Use custom SNMP target IPs

SNMP Servers

No SNMP target IPs specified

3. Select from the following options:

➤ To use the global SNMP server IP address defined in the Alerting context of the Infrastructure Settings page (accessed from **Setup and Maintenance** > **Infrastructure Settings** in Platform Administration), select **Use global SNMP target IP**.

➤ To define a custom SNMP server IP address, select **Use Custom SNMP Target IPs**, and click **Add** to open the SNMP Target IP dialog box. Specify the required address, and click **OK**. Repeat to add multiple addresses.

Running an Executable File When the Alert is Triggered

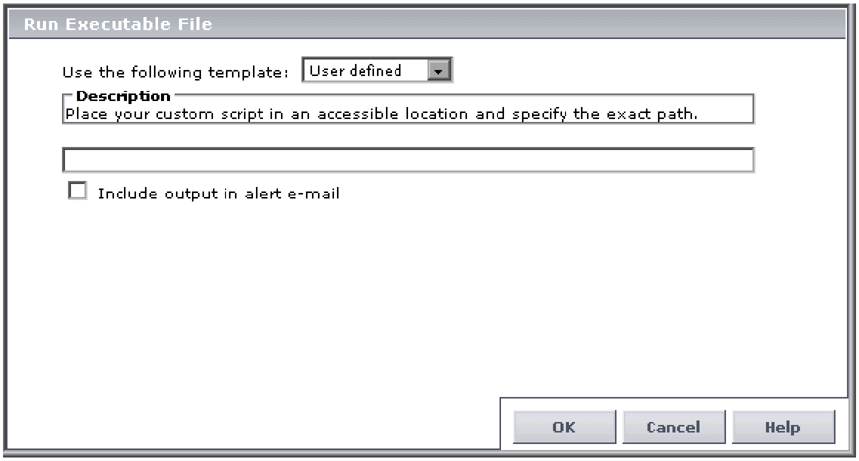
You specify that you want Mercury Business Availability Center to run an executable file (for example, an **.exe** or **.bat** file) when an alert is triggered. The executable file must not be interactive (no user response required) and should not have a user interface.

Mercury Business Availability Center can run an executable file (**.exe** or **.bat** file) when an alert is triggered—either a predefined or custom executable.

To run an executable file:

1 In the upper box, select **Run executable file**. The action appears in the lower box.

2 In the lower box, click the linked value in the sentence that begins **Run executable file**. The Run Executable File dialog box opens.



Run Executable File

Use the following template: User defined

Description
Place your custom script in an accessible location and specify the exact path.

□ Include output in alert e-mail

3 Select the type of template to use for running the file in the **Use the following template** box:

- ➤ **User defined**
- ➤ **ping**
- ➤ **Restart IIS** (not seen if the Core server is on a Solaris platform)
- ➤ **Restart server** (not seen if the Core server is on a Solaris platform)
- ➤ **Restart service** (not seen if the Core server is on a Solaris platform)

4 Type in the command line required to run the executable file.

For details on creating a user-defined command line, including command line format and options, see "Using Custom Alert Parameters" on page 275.

Note to Windows users: To use the predefined batch files that restart a service (including IIS) or server, you must provide the supervisor service running on the Core Server machine with permissions to restart a remote service or machine. To do so, open the **Windows Services** dialog box, right-click the **Mercury Business Availability Center** service, select **Properties**, click the **Log On** tab. In the Log On As section, select **This Account**, and specify the username and password of a user with administrator permissions on the Mercury Business Availability Center server machine.

In addition, if the administrative user on the Core Server is not also an administrative user on the remote machine, you must provide the Core Server machine administrator with permissions on the remote machine. To do so, on the remote machine, open the Windows User Manager, double-click **Administrators** in the Groups window to open the Local Group Properties dialog box, click **Add** to open the Add Users and Groups dialog box, and add the name of a user with administrator permissions on the Core Server.

---

5 Select **Include output in alert e-mail** to include any output that results from the running of the executable file in e-mail alerts. Mercury Business Availability Center places this output in the section of the e-mail alert containing the **Actions Result** text parameter. For details, see "Descriptions of Template Sections and Text Parameters" on page 268.

6 Click **OK**.

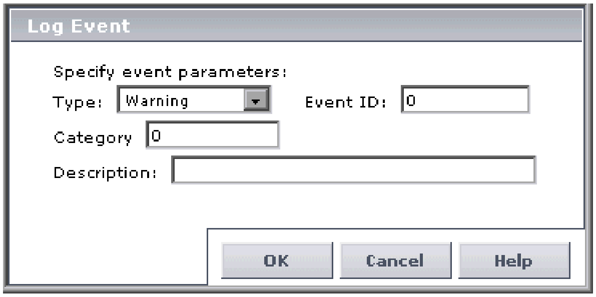
Logging an Event to the Windows Event Viewer When the Alert is Triggered

You specify that you want Mercury Business Availability Center to log an event to the Windows Event Viewer application log when an alert is triggered. You configure the event type, ID, category, and description (standard Event Viewer categories).

Note: If the Core Server is not installed on a Windows-based machine, Mercury Business Availability Center cannot execute this alert action.

To log an event to the Windows Event Viewer application log:

1. In the upper box, select **Log to Event Viewer application log**. The action appears in the lower box.
2. In the lower box, click the linked value in the sentence that begins **Log**. The Log Event dialog box opens.



Log Event

Specify event parameters:

Type: Warning

Event ID: 0

Category 0

Description:

3. Select an event type from the Type list. Event types are represented by icons to the left of the entries in the Event Viewer.
4. If required, specify a numerical event ID in the Event ID box (by default the event ID is 0). You can use event IDs, for example, to group alerts by trigger criteria, profile, transaction, or any other identifying characteristic. Using event IDs will enable you to find events in the Event Viewer.
5. If required, specify a numerical category value in the Category box (by default the category value is 0). You can use category values, for example, to group alerts by type—assign **1** to availability-related alerts and **2** to response-time related alerts. Using categories enables you to find events in the Event Viewer.
6. If required, type a description of the logged event. For example, type a description that corresponds to the characteristics of the alert scheme (alert filters being used, alert trigger criteria, and so forth).
7. Click **OK** to close the Log Event dialog box.

Defining Alert Dependency

Mercury Business Availability Center enables you to define alert dependency. You specify that you want alerts that were previously defined in a specific profile to be subordinate to the alert you are currently defining in that profile, thus making the current alert the dominant alert. If required, you can enable cross-profile dependency. This allows you to define alerts from other profiles as subordinate alerts.

When an alert defined as subordinate is triggered, Mercury Business Availability Center suppresses all actions configured for the alert if its dominant alert was previously triggered as well, and if the conditions that triggered the dominant alert remain true at the time the subordinate alert is triggered.

Further, you can define a time limit for each alert you designate as subordinate. Mercury Business Availability Center begins running the clock on the time limit from the moment the dominant alert is triggered. When a time limit is defined, the actions of the subordinate alert are suppressed as long as the conditions that triggered the dominant alert remain true—but only until the time limit expires.

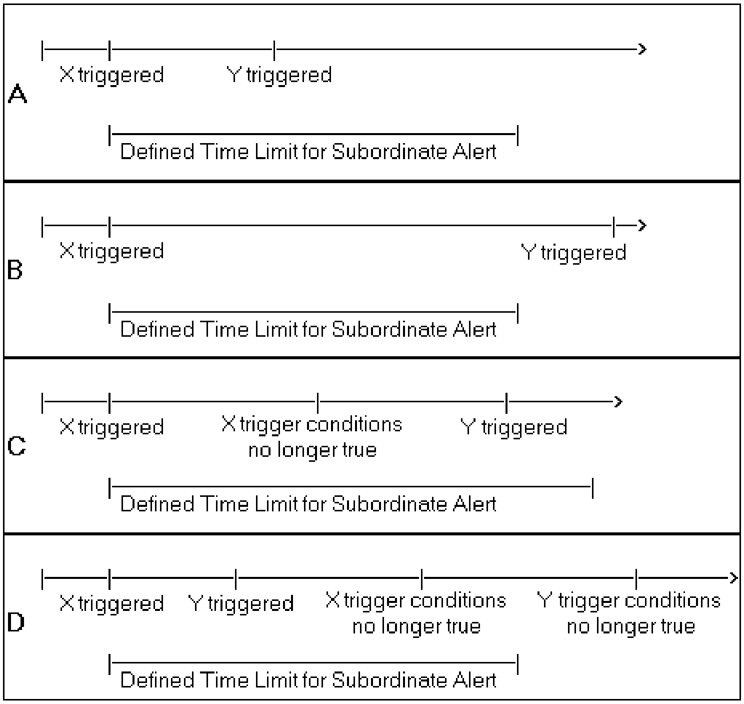
Guidelines and Tips for Configuring Alert Dependencies

- Subordinate alerts are always logged to the Alert Log.
- If a follow-up alert is defined for an alert, regardless of whether the alert is dominant or subordinate, Mercury Business Availability Center sends the follow-up alert only if the original alert was sent. Thus, if a subordinate alert is suppressed, its follow-up alert is not sent. For details on defining follow-up alerts, see “Sending a Follow-Up Alert” on page 256.
- When a group filter is defined in the alert scheme, Mercury Business Availability Center considers each grouped element separately as long as the dominant alert and subordinate alert are from the same profile and have the exact same group filter defined. When dominant and subordinate alerts are from different profiles or do not have the exact same group filters defined, Mercury Business Availability Center does not consider the group filter when determining dependency.

  For example, if a dominant alert and its subordinate alert both have the **Group by transaction** filter defined, when the dominant alert is triggered for a specific transaction, Mercury Business Availability Center will suppress only the subordinate alert instances pertaining to that transaction. However, if a dominant alert has the **Group by transaction** filter defined, and its subordinate alert has the **Group by location** filter defined, when the dominant alert is triggered for a specific transaction, Mercury Business Availability Center will suppress all subordinate alert instances, regardless of transaction or location.
- You cannot create alert loops. That is, if you have a series of dependencies, the dependency path cannot loop back on itself. For example, if Alert A is subordinate to Alert B, Alert B is subordinate to Alert C and Alert D, and Alert C is subordinate to Alert E, you cannot define Alerts B, C, D, or E to be subordinate to Alert A.
- Alert dependency is not transitive. For example, if Alert A is subordinate to Alert B, and Alert B is subordinate to Alert C, Alert A is not subordinate to Alert C.

Examples of Alert Dependency

Consider the following examples, in which alert Y is defined as being subordinate to alert X.


A
X triggered
Y triggered
Defined Time Limit for Subordinate Alert
B
X triggered
Y triggered
Defined Time Limit for Subordinate Alert
C
X triggered
X trigger conditions no longer true
Y triggered
Defined Time Limit for Subordinate Alert
D
X triggered
Y triggered
X trigger conditions no longer true
Y trigger conditions no longer true
Defined Time Limit for Subordinate Alert

- In example A, Mercury Business Availability Center suppressed alert Y's defined actions because alert X, the dominant alert, occurred before alert Y. Further, alert Y occurred during its defined time limit, and while the conditions that triggered alert X remained true.

- In example B, Mercury Business Availability Center did not suppress alert Y's defined actions (that is, alert Y behaved as defined) because—even though alert X, the dominant alert, occurred before alert Y—alert Y occurred after its defined time limit expired.

- In example C, Mercury Business Availability Center did not suppress alert Y's defined actions (that is, alert Y behaved as defined) because the conditions that triggered alert X, the dominant alert, were no longer true by the time alert Y occurred. In this case, the time limit is irrelevant.

- In example D, Mercury Business Availability Center suppressed alert Y's defined actions because alert X, the dominant alert, occurred before alert Y and because alert Y occurred during its defined time limit. In addition, assuming follow-up alerts were defined for alerts X and Y, Mercury Business Availability Center sent a follow-up alert for alert X when its trigger conditions were no longer true. A follow-up alert for alert Y was not sent when its trigger conditions were no longer true, since the original alert Y was suppressed.

Benefits of Alert Dependency

Defining subordinate alerts allows you to:

- Reduce the amount of alert traffic sent.
- Define alert dependencies that match transaction dependencies.

  For example, if you have a transaction that checks the login to your application and a transaction that checks a search in the application after login, you can define the alert that notifies you about poor search performance subordinate to the alert that notifies you about failure to log in to your application. In this case, only the dominant alert is necessary to alert staff to a problem.
- Nest alerts according to severity.

  For example, you can make alerts that are of severity Minor subordinate to alerts that are of severity Critical.
- Define alert dependencies that match alert trigger criteria.

  For example, if you define an alert to be triggered if response time is greater than 15 seconds, and another alert for response time greater than 30 seconds, if response time was 35 seconds, without dominant/subordinate alert definition, Mercury Business Availability Center would send 2 alerts. By making the "response time greater than 15 seconds" alert subordinate to the "response time greater than 30 seconds" alert, only the dominant alert would be sent if response time were greater than 30 seconds. The subordinate alert would be sent if response time were between 15 and 30 seconds.

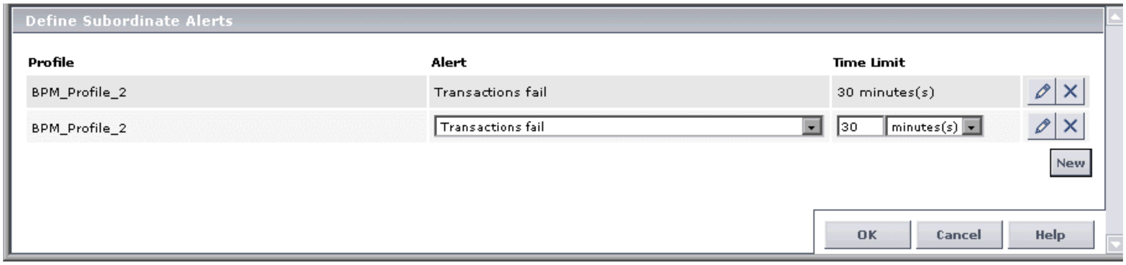
Defining Alert Dependency

To make optimal use of the alert dependency feature, it is recommended that you map out an overall picture of your monitoring and alerting strategy before defining subordinate alerts. Further, you should decide whether you need cross-profile alert dependency (once enabled, cross-profile alert dependency cannot be disabled). For details on enabling cross-profile dependency, see "Changing the Cross-Profile Alert Dependency Status" on page 253.

Once you have planned out your required alert dependencies and configured the desired cross-profile dependency setting, you can create or edit your dominant alerts to specify their subordinate alerts.

To define an alert as subordinate:

1. In the upper box, select **Make specified alerts subordinate to this alert**. The action appears in the lower box.
2. In the lower box, click the linked value in the sentence that begins **Make the following alerts subordinate to this alert**. The Define Subordinate Alerts dialog box opens.
3. Click **New**. Mercury Business Availability Center adds a row to the table and displays a list of available alerts that you can select to be subordinate to the alert you are defining. Mercury Business Availability Center also displays time limit selection lists.



Define Subordinate Alerts

Profile	Alert	Time Limit
BPM_Profile_2	Transactions fail	30 minutes(s)
BPM_Profile_2	Transactions fail	30 minutes(s)

4. If cross-profile dependency is enabled, from the Profile list select the profile in which the alert you want to define as subordinate is defined. For details on enabling cross-profile dependency, see "Changing the Cross-Profile Alert Dependency Status" on page 253.

5. From the **Alert** list, select the alert that you want to be subordinate to the alert you are defining.
6. In the **Time Limit** section, specify the required time limit. To specify no time limit, select **None**.
7. To define additional subordinate alerts, repeat steps 3-6.
8. Click **OK** to close the Define Subordinate Alerts dialog box.

To edit a line in the Define Subordinate Alerts dialog box:

1. If the line is in read-only mode, click the **Edit** button to enable editing.
2. Make the required changes.
3. Click the **Edit** button again to disable editing of the line.

To delete a line in the Define Subordinate Alerts dialog box:

Click the **Delete** button.

Reviewing Alert Dependencies

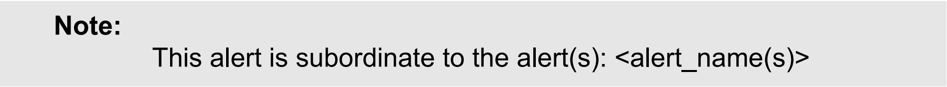
You can view an overall summary of all defined alert dependencies for all profiles. You can also determine whether a specific alert is defined as subordinate and view its dominant alert(s).

To review all defined alert dependencies:

In the Alerts and Recipients tab, select the **View Dependencies** menu item. The Alert Dependency Overview page opens and displays a table that lists all existing dominant alerts and their subordinate alerts, along with their corresponding profiles.

To verify whether an alert is defined as subordinate and view its dominant alert(s):

1. Look for the following line in the bottom window of any page in the Alert Wizard:



Note:
This alert is subordinate to the alert(s): <alert_name(s)>

2. Click the alert name to view the alert's dominant alert(s). The Dominant Alerts window opens.
3. View each dominant alert to which the current alert is subordinate, the profile to which the dominant alert belongs, and the defined time limit—the amount of time Mercury Business Availability Center suppresses instances of the current alert after the dominant alert is triggered.

Changing the Cross-Profile Alert Dependency Status

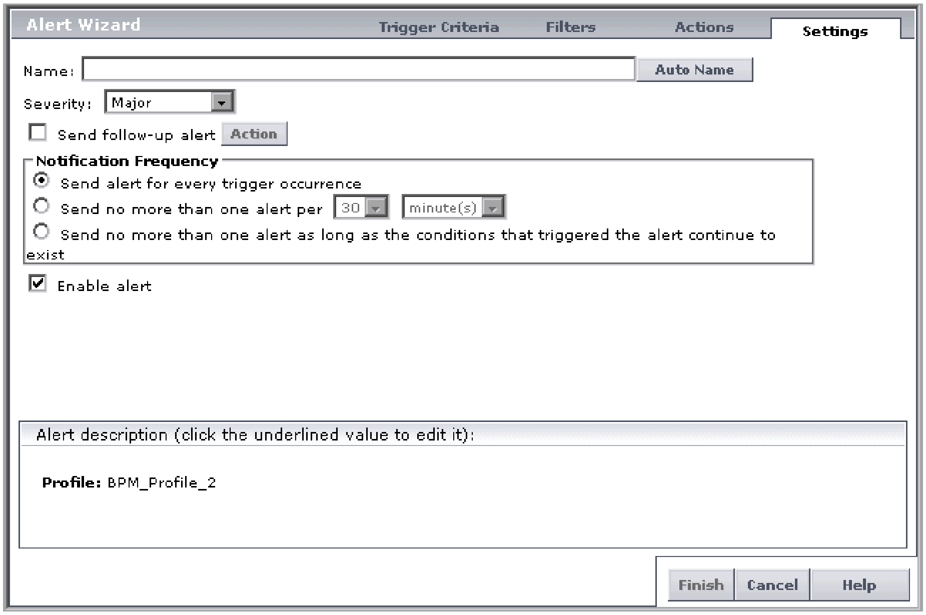
Cross-profile alert dependency is disabled by default. Enabling cross-profile alert dependency has the following implications:

- After it has been enabled, it cannot be disabled.
- With cross-profile alert dependency enabled, more complex alert dependencies can be defined. However, managing complex dependencies may require an advanced level of administration.
- When defining alert dependencies with cross-profile alert dependency enabled, users must keep in mind that they do not have permissions to modify alerts defined in profiles to which they do not have permissions. Thus, if a subordinate alert belongs to a profile to which the user does not have permissions, the user cannot unassociate it from its dominant alert, even if the dominant alert belongs to a profile to which the user does have permissions. Further, if a dominant alert belongs to a profile to which the user does not have permissions, the user cannot edit the alert at all (that is, cannot add or remove dependencies).

Configuring Additional Alert Settings

You specify additional alert settings and review your alert scheme before saving it.

You configure the additional alert settings from the Alert Settings tab of the Alert Wizard.



Name:

Severity: Major

☐ Send follow-up alert

Notification Frequency

● Send alert for every trigger occurrence

○ Send no more than one alert per 30 minute(s)

○ Send no more than one alert as long as the conditions that triggered the alert continue to exist

☑ Enable alert

Alert description (click the underlined value to edit it):

Profile: BPM_Profile_2

From the Alert Settings tab, you can:

- modify the default alert name – for details, see page 255
- select a severity label for the alert – for details, see page 255
- send a follow-up alert and run an executable file when follow-up alert is triggered – for details, see page 256
- specify the alert notification frequency – for details, see page 257
- temporarily disable the alert scheme – for details, see page 258

After selecting the required settings, you can review your alert scheme before saving it.

Modifying the Default Alert Name

The alert name appears in the alert notices that Mercury Business Availability Center sends. The default alert name is based on the alert trigger criteria you select. If you do not want Mercury Business Availability Center to use the default alert name, you can give the alert an alternative name.

To modify the alert name:

Type the required alert name in the alert name box.

To restore the default name assigned by Mercury Business Availability Center, click **Auto Name**.

Selecting a Severity Label for the Alert

You provide meaningful labels to your alerts to identify and classify them when you receive them, or when you see them in the Alert Log.

You can choose from the following alert severity labels:

- Informational
- Warning
- Minor
- Major
- Critical

When choosing the severity label, consider the priority of the alert scheme's alert trigger criteria. For example, label the alert Informational if the alert trigger criteria do not reflect a problem that affects end users. Label the alert Critical if the alert trigger criteria reflect a total site crash.

To select an alert severity label:

Select the required label from the severity label list.

Sending a Follow-Up Alert

You can instruct Mercury Business Availability Center to send a follow-up alert when the conditions that trigger the original alert are no longer true. Mercury Business Availability Center sends the follow-up alert to the same recipient(s) that received the original alert.

Mercury Business Availability Center uses the system's default, follow-up template or a user-defined, follow-up template. For details on creating a user-defined follow-up template and the conditions under which it is used, see "Configuring a Template for Follow-up Notifications" on page 273.

You can also instruct Mercury Business Availability Center to run an executable file when the follow-up alert is triggered.

Note: The follow-up alert is logged in the Alerts log with the status listed as **Informational**, regardless of the status of the original alert.

To instruct Mercury Business Availability Center to send a follow-up alert:

Select the **Send follow-up alert** check box.

To instruct Mercury Business Availability Center to run an executable file when the follow-up alert is triggered:

1. Select **Send follow-up alert**.
2. Click **Action**. The Run Executable File dialog box opens.
3. Type the command line required to run the executable file, or choose one of the predefined commands. For details, see "Running an Executable File When the Alert is Triggered" on page 243.
4. Select **Include output in alert e-mail** to instruct Mercury Business Availability Center to include any output that results from the running of the executable file in follow-up e-mail alerts. For details, see "Running an Executable File When the Alert is Triggered" on page 243.
5. Click **OK**.

Note: If the original alert sent was configured to be sent based on any alert frequency criteria other than **even once**, the executable file run based on a follow-up alert cannot include the following parameters: UserMessage, org_name, script_name, txn_err, host_name, time, actual_desc, target_host_name, mon_name, msr_name, con_name, err_msg. This is because Mercury Business Availability Center records all the data for each event that satisfies the alert criteria and sends the alert only when the defined frequency criteria was met. The follow-up alert will no longer contain these parameters. For details on alert frequency criteria, see "Defining Alert Frequency Criteria" on page 202.

Specifying the Alert Notification Frequency

You specify the frequency with which you want Mercury Business Availability Center to perform the alert actions that you select.

For example, if you specify **Send no more than one alert per 30 minutes**, even if alert trigger criteria are met several times within a 30-minute span, Mercury Business Availability Center performs the selected alert action(s) only once.

Note: Regardless of the frequency you select, each time alert trigger criteria are met, Mercury Business Availability Center logs an alert in the Alert Log. For details on viewing the alert log, see "Alert Log" in *Using End User Management*.

To specify alert notification frequency:

Choose from:

- **every trigger occurrence.** Instructs Mercury Business Availability Center to send an alert every time trigger conditions exist.

- **no more than one alert per specified time period.** Instructs Mercury Business Availability Center to send no more than one alert over each specified time period, even if alert trigger conditions continue to exist during the entire time period.

  For example, if you instruct Mercury Business Availability Center to send no more than one alert notice per 60 minutes, from the moment alert trigger conditions exist and Mercury Business Availability Center sends the alert, Mercury Business Availability Center waits 60 minutes before sending another alert. If, after the 60 minutes, the conditions that triggered the alert continue to exist, another alert is sent.

- **no more than one alert as long as the conditions that triggered the alert continue to exist.** Instructs Mercury Business Availability Center to send no more than one alert notice as long as the conditions that triggered the alert continue to exist.

  For example, if you select this option, from the moment alert trigger conditions exist and Mercury Business Availability Center sends the alert, an additional alert is not sent as long as the conditions that triggered the alert continue to exist.

  Note that, when you select this option, Mercury Business Availability Center automatically selects the **Send follow-up alert** option. If you do not want a follow-up alert to be sent when the conditions that triggered the alert no longer exist, you must manually clear the **Send follow-up alert** setting.

Temporarily Disabling the Alert Scheme

You can temporarily disable the alert scheme if you do not want Mercury Business Availability Center to send or log alerts when the trigger criteria defined in the alert scheme are met. You disable an alert scheme if, for example, you have not yet finished creating the profile related to the alert, or if you temporarily stop the profile run.

To modify the alert status:

- To temporarily disable the alert, clear the **Enable alert** check box.
- To enable the alert, select the **Enable alert** check box.

Reviewing and Saving the Alert Scheme

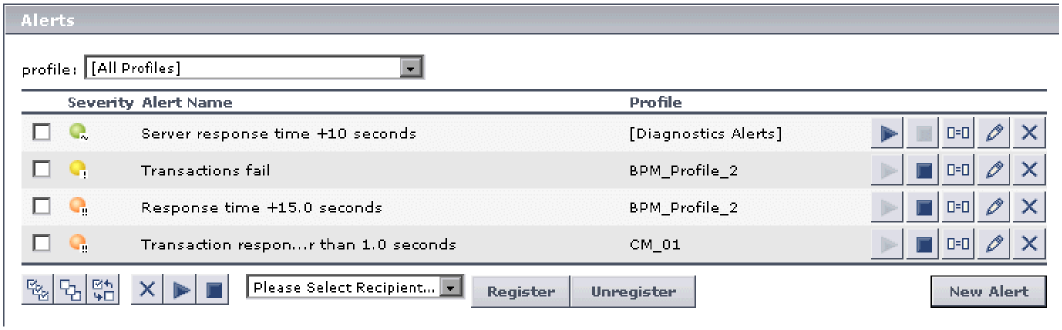
From the Alert Settings page, you can review your alert scheme before saving it.

To save the alert scheme:

Click **Finish**. Mercury Business Availability Center saves the alert scheme and closes the Alert Wizard.

Viewing an Alert Scheme

After you create an alert scheme, Mercury Business Availability Center displays it in the Alerts table. The Alerts table lists alerts by name, their severity label, and their associated profile.



Alerts

profile: [All Profiles]

	Severity	Alert Name	Profile
□	●	Server response time +10 seconds	[Diagnostics Alerts]
□	●	Transactions fail	BPM_Profile_2
□	●	Response time +15.0 seconds	BPM_Profile_2
□	●	Transaction respon...r than 1.0 seconds	CM_01

Mercury Business Availability Center indicates alert severity as follows:

Icon status	Description
●	Informational
●	Warning
●	Minor

Icon status	Description
🟠‼	Major
🔴✕	Critical

Mercury Business Availability Center indicates the status of the alert (whether it is enabled or disabled) by the status of the Enable and Disable buttons next to each alert scheme. If the Enable button is enabled, the alert is disabled and can be enabled by clicking the Enable button, and vice versa for disabled alerts.

Icon status	Description
▶	Alert scheme enabled
■	Alert scheme disabled

Managing Alert Schemes

Over time, you may find it necessary to make changes to alert schemes that you create, due to organizational changes, changes to service level monitoring contracts, and so forth. For example, if an alert recipient leaves the company, you will need to modify the alert scheme. Alternatively, if, due to a change in a service level monitoring agreement, the availability rate of a specific transaction is now expected to be at 97 percent rather than 90 percent, you may want to modify alert trigger criteria for that transaction accordingly.

You can perform the following alert management procedures directly from the Alerts page:

- edit the alert scheme
- disable/enable the alert scheme
- clone the alert scheme
- delete the alert scheme
- modify the alert recipients

To edit an alert scheme:

1. Click the **Modify Alert Properties** button beside the alert whose properties you want to modify. The Alert Wizard opens.
2. Move through the Alert Wizard and edit the alert scheme as required.
3. Click **Finish** to save the changes and close the Alert Wizard. Click **Cancel** to close the Alert Wizard without saving any changes.

To disable/enable an alert scheme:

- If an alert is enabled, click the **Disable Alert** button beside the alert to disable it. When an alert is disabled, Mercury Business Availability Center does not send an alert notice when the trigger conditions defined in the alert occur.
- If an alert is disabled, click the **Enable Alert** button beside the alert to enable it.
- To enable or disable multiple alerts simultaneously, select their check boxes in the left column and click the **Enable Selected Alert(s)** or **Disable Selected Alert(s)** button located at the bottom of the Alerts table.

Note: You can also disable or enable an alert scheme from the Alert Settings page of the Alert Wizard. For details, see "Temporarily Disabling the Alert Scheme" on page 258.

To clone an alert scheme:

1. In the profile table, select the alert scheme you want to clone.
2. Select the **Clone** button next to the alert scheme you want to clone. Mercury Business Availability Center adds a copy of the alert scheme to the profile tree, with a new name.
3. Rename and edit the alert scheme as required.

To delete an alert scheme:

- ➤ Click the **Delete Alert** button beside the alert.
- ➤ To delete multiple alerts simultaneously, select their check boxes in the left column, and click the **Delete Selected** button located at the bottom of the Alerts table.

To modify recipients registered to an alert from the Alert table:

1. Select the check box beside the alert(s) for which you want to add or remove a recipient.
2. Select the recipient to add or remove in the recipient list at the bottom of the Alerts table.
3. Click the **Register** button to add the specified recipient to the selected alert(s).

   Click the **Unregister** button to remove the specified recipient from the selected alert(s).

Note: The value that appears in the **From** field when Mercury Business Availability Center sends alerts is set when you install the Core Server. By default the value is **MercuryAM_Alert_Manager**. You can modify the value in Platform Administration by selecting **Setup and Maintenance** > **Infrastructure Settings** and the **Alerting** context. Modify the value **Email sender** or **Email sender address** (to include an email address in the From field). For details on modifying values, see “Editing Infrastructure Settings” on page 76.

17

Alert Notification Templates

Mercury Business Availability Center alerts proactively inform designated recipients when predefined performance limits are breached. To determine the contents and appearance of the alert notices, you can select pre-defined templates or configure your own template for notifications.

About Alert Notification Templates

Alert notification templates specify the information that Mercury Business Availability Center includes when it sends various types of alert notices. There are two default templates, **Long** and **Short**. These default templates are pre-configured with selected parameters for each section of the alert notice. For details on the information included in the default templates, see "Default Templates" on page 271.

You can also create custom templates to use for different alert notice delivery methods (e-mail, pager, SMS), or for different recipients, for example. A custom template is defined in the Notification Template Properties page. Each section of the alert notice includes a list of parameters from which to select. For details on the information that can be included in a custom template, see "Descriptions of Template Sections and Text Parameters" on page 268.

Note for Mercury Managed Services customers: Your list of notification templates includes those created for your use by Mercury Managed Services representatives and those created by your organization.

The **Customer Template** column in the Notification Templates page indicates whether the template listed was created specifically for your organization's use.

You select which template to use per recipient in the Recipient Properties dialog box. For details, see "Defining a Recipient" on page 182.

You use the Notification Templates page to:

- create custom templates
- modify the default Long and Short templates, if required
- manage existing templates
- create custom templates for follow-up notifications

Creating Custom Templates

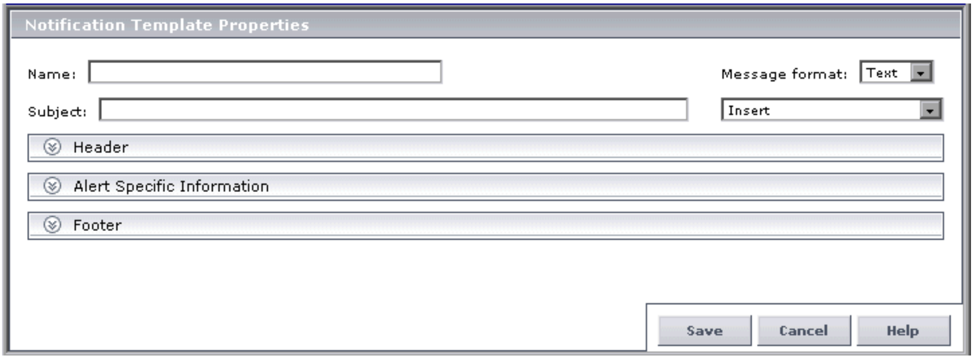
Mercury Business Availability Center gives you the flexibility to create different notification templates for the different alert schemes and recipients that are defined for your platform.

You can taylor a notification template for the specific method of delivery and for different recipients. You can create templates with just the details relevant to the recipient's position and responsibilities, for example:

- high level executives may want to know only the severity level and the location via a pager alert containing limited space
- systems administrators may need details of the data collector and the transaction via an e-mail alert
- customer support may need information on the group, location, and description of the transaction

To define a new alert notification template:

1. Select **Admin** > **Platform** > **Alerts and Recipients** > **Notification Templates**. Mercury Business Availability Center opens the Notification Templates page listing the **Long** and **Short** templates, and any custom templates that have been defined.
2. Click the **New Template** button to open the Notification Template Properties dialog box.



3. Type a name for the template in the **Template name** box.

   If possible, use a descriptive name, for example, one that includes information on the type of alert (e-mail, pager, SMS) for which you plan to use the template, or the recipient(s) who will receive alerts using this template.

Note to Mercury Managed Services customers: When creating a notification template, the Customer Template checkbox is automatically selected. The template will be listed as a Customer Template in the Notification Templates page.

4. Select the format for the message as either **Text** or **HTML** in the **Message Format** box.
5. Specify the information that you want Mercury Business Availability Center to include in the various sections of the alert notice. Select a section of the template:

- **Subject**. Same options as header and footer (e-mail only)
- **Header**. Same options as subject and footer
- **Alert Specific Information.** Includes **Transaction** parameters and text
- **Footer.** Same options as subject and header

6. Click the **Insert** button for each section, and select a text parameter to add. Repeat to add as many text parameters as you want from the list.

   For detailed descriptions of the sections and text parameters, see the table below.

7. In the section's text box, add free text before or after the text parameters. For examples, see the configurations for the long and short default templates.
8. Click **OK** to save the template.

Descriptions of Template Sections and Text Parameters

Every template is divided into sections. You specify the information that you want to appear in each section. A typical template is divided into three sections:

- **header.** Appears at top or beginning of alert notice
- **body.** Appears in middle of alert notice; includes alert-specific and transaction information
- **footer.** Appears at the bottom or end of alert notice

In addition, e-mail notices have a subject section that corresponds to an e-mail subject line.

The table below describes the text parameter options that are available in each section of the alert notification template:

Template Section	Options	Description
Subject (e-mail only), **Header**, **Footer**	Alert Name	The name of the alert, as defined in the alert scheme.
	Severity	The severity label assigned to the alert in the alert scheme.
	Mercury AM URL	The URL of the Mercury Business Availability Center Web site.
	Profile Name	The name of the profile in which the alert scheme was created.
	User Message	The user message, as specified in the alert scheme.
	Actions Result	A description of the results of the alert actions specified in the alert scheme.
	Add Hardcoded Strings Flag	Text and values that have been predefined in the system. These include the occurrence of the alert and if the alert is, or has triggered, a subordinate alert. For example, Occurrence 5, Subalert triggered (1 of 3).
Alert-Specific Information	Trigger Cause	A description of the alert trigger conditions, as specified in the alert scheme.
	Actual Details	A description of the actual conditions at the time of the alert.

Template Section	**Options**	**Description**
Transaction	Transaction Time	The date and time of the alert.
	Transaction Name	The name of the transaction related to the alert.
	Script Name	The name of the script containing the transaction related to the alert.
	Data Collector Name	The name of the data collector running the transaction related to the alert.
	Location Name	The location of the data collector running the transaction related to the alert.
	Group Name	The group defined for the data collector running the transaction related to the alert.
	Transaction Error	The error message generated by the data collector for the transaction, if a transaction error occurred at the time of the alert.
	Transaction Description	A description of the transaction, if it has been defined in Monitor Administration.

Default Templates

The tables below describe the text categories that are included in the default Long and Short templates. These templates also include added text that identifies each of the text parameters within the notification.

If you find that you want to modify these default templates, you can use the same procedures for editing any notification template. For details, see "Managing Notification Templates" on page 272.

➤ Long Template

Template Section	Included Text Categories
Subject	Alert name, Severity
Header	Profile name, Severity, Alert name
Alert-Specific Information	Trigger cause, Actual details
Transaction	Location name, Transaction time, Data collector name, Group name, Script name, Transaction name, Transaction error
Footer	User message, Mercury AM URL, Actions result

➤ Short Template

Template Section	Options
Subject	Alert name, Severity
Alert-Specific Info	Trigger cause

Managing Notification Templates

Over time, you may find it necessary to make changes to notification templates that you create, due to organizational changes, changes in notification policies, changes to service level monitoring contracts, and so forth.

You use the Notification Templates page to edit, duplicate, and delete notification templates defined in Mercury Business Availability Center.

To modify a notification template:

1. Click the **Modify** button beside the notification template you want to modify. The Notification Template Properties dialog box opens.
2. Edit the template sections as required.
3. Click **Save** to save the changes. Click **Cancel** to close the properties dialog box without saving any changes.

To clone a notification template:

1. Click the **Duplicate** button next to the notification template you want to clone. The Notification Template Properties dialog box opens.
2. Rename the notification template and edit as required.
3. Click **Save** to save the changes. Click **Cancel** to close the properties dialog box without saving any changes.

To delete a notification template:

- Click the **Delete** button beside the notification template to remove.
- To delete multiple templates simultaneously, select their check boxes in the left column, and click the **Delete Selected** button located at the bottom of the templates list.

To make your selections, use the buttons at the bottom of the page for **Select All**, **Clear All**, and **Invert Selection**.

Configuring a Template for Follow-up Notifications

When configuring alert schemes, you can instruct Mercury Business Availability Center to automatically follow up the alert by sending a follow-up notification. For details on selecting this option while creating your alert scheme, see "Sending a Follow-Up Alert" on page 256.

There is a default template for follow-up notifications that is automatically used by Mercury Business Availability Center. If you do not want Mercury Business Availability Center to use that default template, you can create your own follow-up template.

This follow-up template must be based on an existing notification template. Mercury Business Availability Center uses the follow-up notification template that you create under the following circumstances:

- An alert has been triggered.
- Notification is sent to a recipient based on an existing template (default or user-defined).
- The alert scheme has been configured to send a follow-up alert.
- The notification template selected for the recipient has a follow-up template based on the notification template's name. For details on naming a follow-up template, see the procedures below.

To create a user-defined, follow-up notification template:

1 Select the notification template to use as the basis for your follow-up template. Make your determination based on which notification templates are selected for users likely to receive a follow-up alert notification.

2 Click the **Duplicate** button next to the selected notification template. The Notification Template Properties dialog box opens.

3 In the **Name** box, delete **Copy of**, and at the end of the current name, add the following: _FOLLOWUP (all caps, one word).

For example, if you are creating a follow-up template based on the **LONG** default template, you would call the follow-up template LONG_FOLLOWUP. If the follow-up template is based on a user-defined template called MyTemplate, name the follow-up template MyTemplate_FOLLOWUP.

Note: The _FOLLOWUP string is the default string recognized by Mercury Business Availability Center as the template name for a follow-up alert message. You can change this string by selecting **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundation: Alerting**. Edit the **Followup notifications suffix** value and be sure to use the same string when creating a follow up template.

4 Edit the template details as required. It is recommended that you include in the **Subject** (for e-mails), **Header**, and/or **Alert Specific Information** that this is a follow up to an alert.

5 Click **Save** to save the new follow-up notification template.

18

Advanced Alert Procedures

Advanced alert procedures enable you to customize and control the way Mercury Business Availability Center sends alerts.

Using Custom Alert Parameters

You can embed predefined alert parameters into:

- a custom command line that runs an executable file when an alert is triggered
- a URL that is accessed when an alert is triggered

For details on configuring your alert scheme to run an executable file or access a URL when an alert is triggered, see “Configuring Alert Actions” on page 238.

For a description and listing of the different alert parameters, see “Alert Parameter Categories” on page 277.

Embedding Alert Parameters in the Command Line

When using a custom command line, the command line that runs the executable file must be in the following format:

```
<full path to program from Core Server machine> <program command line switches>
```

You embed the alert parameters—which are expanded before the command line is executed—in the **program command line switches** section of the command line statement.

The format of alert parameters is: <ParameterName>

For example:

```
C:\Bin\MyAlertReporter.exe –title “Alert <AlertName> for <ProfileName>” –Text “<UserMessage>”
```

Note: Because the server triggers the executable, the path to the executable must be available from the Core Server machine.

Embedding Alert Parameters in a URL

When embedding alert parameters in a URL, you use the following format:

```
http://<server_or_IP>?<parameters>
```

You embed the alert parameters in the **parameters** section of the URL.

The format of alert parameters is: <ParameterName>

For example:

```
http://myticketingsystem.com?name=<AlertName>&ticketID=<AlarmID>&description=<AlertDescription>
```

Alert Parameter Categories

There are different categories of parameters that can be embedded:

- **alert parameters.** Return information pertaining to the alert that Mercury Business Availability Center sends.
- **event parameters.** Return information pertaining to specific transaction events that meet alert trigger criteria, but for which an alert is not sent. Depending on the defined alert trigger criteria, a number of events might need to occur before an alert is sent. For example, for an alert defined to be sent if a transaction fails three times out of five, Mercury Business Availability Center considers each single transaction failure as one event, but only three failures out of five will trigger an actual alert.
- **group performance data parameters.** Return information as alert parameters or event parameters when Mercury Business Availability Center has been instructed to consider the performance data by transaction, by script (file containing transactions), by group, by location, or by any combination of the four. These parameters can be embedded as either alert parameters or event parameters as described above.

Note: For details on grouping performance data when creating an alert scheme, see "Grouping Performance Data" on page 232.

- **SubAlerts parameter.** Returns, in XML format, information pertaining to specific transaction events that meet alert trigger criteria, but for which an alert is not sent.

Alert Parameters

You can use the following alert parameters to return information pertaining to the Business Process Monitor alerts that Mercury Business Availability Center sends.

Parameter	Description
ProfileName	The name of the profile in which the alert scheme was created.
TriggerCause	The alert trigger criteria specified in the alert scheme.
AlertName	The alert name specified in the alert scheme.
Severity	The alert severity label specified in the alert scheme.
AlertPurpose	The type of alert, either a “regular” alert, which is sent when alert trigger conditions are true, or a “follow-up” alert, which is sent when the alert trigger conditions that triggered the earlier alert are no longer true.
UserMessage	The user message specified in the alert scheme.
AlarmID	The unique ID assigned to the alert scheme.
AlertDescription	A description of actual conditions at the time of the alert, generated by Mercury Business Availability Center.
txn_name	The transaction name specified in the script. This parameter is available to use as an alert parameter only when the alert has been grouped by transaction.
loc_name	The location of the host machine, specified during Business Process Monitor installation, that ran the transaction(s) that triggered the event. This parameter is available to use as an alert parameter only when the alert has been grouped by location.

Event Parameters

You can define alert trigger criteria in such a way that multiple conditions must be met before Mercury Business Availability Center sends an alert. For example, say you specify alert trigger criteria as follows:

Send alert if transactions fail or if transaction response time is greater than 10 seconds. Send alert if trigger conditions occur at least 3 times out of 5.

In this case, Mercury Business Availability Center considers each instance of transaction failure or response time greater than 10 seconds as one transaction event that meets alert trigger criteria. However, Mercury Business Availability Center sends an alert only if there are at least 3 such events out of 5 total events.

You use the event parameters to return specific information about each of the individual transaction events for which trigger criteria were met.

The format of event parameters is <**ValueNameEventNumber**>, where ValueName is the name of the parameter and EventNumber is the index of the triggered event. The default value for EventNumber is 1, so if EventNumber is not provided, information on the first event that meets trigger criteria will be returned. Further, if you provide an EventNumber for an event that does not occur (for example, if you specify an EventNumber of 4 and there are only 3 events), an empty string will be returned.

For example, for an alert defined to be sent if a transaction fails three times out of five, to return information on all three "transaction failed" events, you could use the following command:

```
C:\Bin\MyAlertReporter.exe –title “Event for <txn_name1>” –Time “<time1>”
–Text “<actual_desc1>” –title “Event for <txn_name2>” –Time “<time2>” –Text
“<actual_desc2>” –title “Event for <txn_name3>” –Time “<time3>” –Text
“<actual_desc3>”
```

The following table describes the individual event parameters:

Parameter	Description
txn_name	The transaction name specified in the script
org_name	The name of the organization specified during installation
loc_name	The location of the host machine, specified during Business Process Monitor installation, that ran the transaction(s) that triggered the event
script_name	The name of the script containing the transaction(s) that triggered the event
txn_err	A description of the error that the script generated, if an error occurred at the time of the event
host_name	➤ The name of the host machine that ran the transaction(s) that triggered the event ➤ For SiteScope alerts, the name of the SiteScope that ran the monitor that triggered the event (provided for backward compatibility with SiteScope alerts created in older versions of Topaz)
time	The time at which the event was triggered
actual_desc	A description of actual conditions at the time of the event
target_host_name	The name of the monitored server specified in the profile (provided for backward compatibility with SiteScope alerts created in older versions of Topaz)
mon_name	The name of the SiteScope monitor for which the event was triggered (provided for backward compatibility with SiteScope alerts created in older versions of Topaz)
msr_name	The measurement instance that triggered the event (provided for backward compatibility with SiteScope alerts created in older versions of Topaz)

Parameter	Description
con_name	The title of the SiteScope monitor for which the event was triggered (provided for backward compatibility with SiteScope alerts created in older versions of Topaz)
err_msg	A description of the error that the monitor generated, if an error occurred (provided for backward compatibility with SiteScope alerts created in older versions of Topaz)

Group Performance Data Parameters

You can use this category of parameters as either alert parameters or event parameters. They can be embedded only if the alert scheme was defined with performance data grouped by one of the parameters or a combination of the four.

Parameter	Description
transaction	The transaction name specified in the script. Can be used only when performance data has been grouped by transaction.
location	The location of the host machine, specified during Business Process Monitor installation, that ran the transaction(s) that triggered the event. Can be used only when performance data has been grouped by location.
group	The group name of the host machine that ran the transaction(s) that triggered the alert and/or event. Can be used only when performance data has been grouped by group.
transaction file	The name of the script containing the transaction(s) that triggered the alert and/or event. Can be used only when performance data has been grouped by script.

The SubAlerts Parameter

You can use the **SubAlerts** parameter to return complete details of all the transaction events related to the alert, as a string in XML format. For a description of transaction events, see “Event Parameters” above. For details on the returns XML string, see “XML String for Business Process Profile Alerts” below.

The SubAlerts parameter contains the following sections:

➤ <**Sub_Alert Index**="**x**">

Each section in the XML string beginning with this tag contains the transaction events related to one defined alert trigger criterion. The “x” indicates the order in which alert trigger criteria occur.

➤ <**Sub_Alert_Instance Index**="**x**">

This tag nests under the <**Sub_Alert Index**="**x**"> section and its contents relate to the alert trigger criterion for that section.

Each section in the XML string beginning with the <**Sub_Alert_Instance Index**="**x**"> tag contains the transaction events for one specific member of a group, as defined in the **Group By** filter in the Alert Wizard. For example, if you specify Group By Location, and transaction events occur at 2 locations, Mercury Business Availability Center lists one instance of the <**Sub_Alert_Instance Index**="**x**"> parameter for each location. If there are no defined **group by** criteria, all events are listed under <**Sub_Alert_Instance Index**="**1**">. The “x” represents the order in which the events occur.

➤ <**Transaction_Event Index**="**x**">

This tag nests under the <**Sub_Alert Index**="**x**"> and <**Sub_Alert_Instance Index**="**x**"> sections and its contents relate to the alert trigger criterion for those sections.

Each section in the XML string beginning with the <**Transaction_Event Index**="**x**"> tag contains information on one specific transaction event. The “x” represents the order in which the events occur.

When the executable parses the XML string, it should run until there are no more events to read.

Understanding the XML String Returned by the SubAlerts Parameter

You can use the information in the XML file returned by the SubAlerts parameter to understand the circumstances that triggered the alert, and thus take the appropriate corrective action, for example, restart a service or notify another utility.

XML String for Business Process Profile Alerts

For alerts generated through a Business Process profile, the SubAlerts parameter returns an XML string containing the following information:

Sub_Alert Tags

Tag	Description
Trigger_Cause	The alert trigger criteria that triggered the alert
Actual_Description	A description of actual conditions at the time of the alert

Transaction_Event Tags

Tag	Description
Transaction_Name	The transaction name specified in the script
Organization	The name of the organization specified during installation
Host	The name of the host machine that ran the transaction(s) that triggered the alert
Location	The location of the host machine specified during Business Process Monitor installation
Script	The name of the script containing the transaction(s) that triggered the alert

Tag	Description
Time	The time at which the alert was triggered
Actual_Description	A description of actual conditions at the time of the alert
Transaction_Error_Msg	A description of the error that the script generated, if an error occurred

For example:

```
<Sub_Alerts>
    <Sub_Alert Index="1">
        <Sub_Alert_Instance Index="1">
            <Trigger_Cause>Response time for 2 out of 3 transactions greater
              than 0.01 seconds.</Trigger_Cause>
            <Actual_Description>Response time for 2 out of 2 transactions
              was greater than 0.01 seconds.</Actual_Description>
            <Transaction_Event Index="1">
                <Transaction_Name>MyHomepage</Transaction_Name>
                <Organization>MyCompany</Organization>
                <Host>Agent1</Host>
                <Location>Location1</Location>
                <Script>TransFile1</Script>
                <Time>Monday, September 10, 2001 09:24:00</Time>
                <Actual_Description>Response time was 0.20
                  seconds.</Actual_Description>
            </Transaction_Event>
            <Transaction_Event Index="2">
                <Transaction_Name>MyHomepage</Transaction_Name>
                <Organization>MyCompany</Organization>
                <Host>Agent1</Host>
                <Location>Location1</Location>
                <Script>TransFile1</Script>
                <Time>Monday, September 10, 2001 09:29:00</Time>
                <Actual_Description>Response time was 0.18
                  seconds.</Actual_Description>
            </Transaction_Event>
        </Sub_Alert_Instance>
    </Sub_Alert>
</Sub_Alerts>
```

Configuring the Alerts MIB

If you enabled alerts via SNMP trap in your alert schemes, it is recommended that you configure your SNMP management console to read the Alerts MIB. This enables you to see names, rather than OIDs, when working in the management console.

Note: Mercury Business Availability Center uses the AM alerts MIB 5.0 by default.

To configure the alerts MIB in your SNMP management console:

1. Copy the Alerts MIB file **amAlerts5.mib** into your SNMP management console. The file is on the Mercury Business Availability Center Documentation and Utilities CD-ROM in **tools_and_utilities\SNMP_MIBS**.
2. To view the Alerts varbinds, use your SNMP management console’s MIB browser. See “Alerts MIB Varbinds” on page 287 for a list of varbinds and their descriptions.
3. Using your SNMP management console’s event configuration utility, configure the notification content and method for the various alert types. See SNMP-Specific Codes below for a list of alert types and their corresponding SNMP-specific codes.

Note: If you need to use a MIB from a previous version of Mercury Business Availability Center, follow the procedure in step 1 above for copying the appropriate MIB file. The files are numbered according to the version number of Mercury Business Availability Center.

Set Mercury Business Availability Center to use the appropriate MIB in the Alerting context of the Infrastructure Settings page by selecting **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings.** Choose **Foundations** and select **Alerting**. Change the **Use SNMP trap MIB of AM version** setting to use the appropriate MIB.

SNMP-Specific Codes

The following table lists the alert types and their SNMP-specific codes. Use these codes when configuring alert notification events in your SNMP management console.

SNMP-Specific Code	Alert Type
1	Transaction response time Alert Frequency: Even once
2	Transaction failure Alert Frequency: Even once
3	Transaction availability
4	Average transaction response time
5	Measurement value Alert Frequency: Even once
6	Average measurement value
7	Real User Monitor alert
8	Transaction response time for specified percentage of transactions
9	Transaction response time Alert Frequency: X out of Y
10	Transaction failure Alert Frequency: X out of Y
11	Measurement failure Alert Frequency: Even once

SNMP-Specific Code	Alert Type
12	Measurement value for specified percentage of measurements
13	Measurement availability
14	Measurement value Alert Frequency: X out of Y
15	Measurement failure Alert Frequency: X out of Y
100	Complex alert (contains more than one subalert)

Alerts MIB Varbinds

The tables below list the varbinds used in the Alerts MIB.

Object Identifier	MIB Label	Description
1.3.6.1.4.1.5233	mercuryInteractive	Company name
1.3.6.1.4.1.5233.4	topazAlerts4	Subject
1.3.6.1.4.1.5233.4.1	profileName	Profile name
1.3.6.1.4.1.5233.4.2	alertName	Alert name (for example, "Response time of any transaction < 10.00 sec")
1.3.6.1.4.1.5233.4.3	alertType	Alert type: regular or follow-up
1.3.6.1.4.1.5233.4.4	alarmID	Unique alert ID
1.3.6.1.4.1.5233.4.5	alertSeverity	Alert severity: informational -10, warning - 20, minor - 30, major - 40,critical - 50
1.3.6.1.4.1.5233.4.6	alertTriggerCause	Defined alert trigger conditions (for example, "Response time less than 10 seconds")

Object Identifier	**MIB Label**	**Description**
1.3.6.1.4.1.5233.4.7	alertActualDescripti on	Actual conditions at time of alert (for example, “Current response time is 3.00 seconds”)
1.3.6.1.4.1.5233.4.8	alertUserMessage	User message for this alert
1.3.6.1.4.1.5233.4.9	subAlertsTable	Start of Subalerts table. Subalerts trigger alerts (listed in Events table below)
1.3.6.1.4.1.5233.4.9.1	subAlertsEntry	Start of subalert entry
1.3.6.1.4.1.5233.4.9.1.1	subAlertIndex	Index of the subalert within subalert list
1.3.6.1.4.1.5233.4.10	subAlertInstances Table	Start of subalert instance table
1.3.6.1.4.1.5233.4.9.10.1	subAlertInstances Entry	Start of subalert instance entry
1.3.6.1.4.1.5233.4.9.10.1.1	subAlertInstances Index	Index of the subalert instance
1.3.6.1.4.1.5233.4.9.10.1.2	subAlertOwner	Index of subalert owner
1.3.6.1.4.1.5233.4.9.10.1.3	subAlertInstance TriggerCause	Defined alert trigger conditions for subalert instance
1.3.6.1.4.1.5233.4.9.10.1.4	subAlertInstance ActualDesc	Actual conditions at time of subalert instance
1.3.6.1.4.1.5233.4.11	alertEvents	Start of Events table
1.3.6.1.4.1.5233.4.11.1	transactionalEvents Table	Start of alerts table
1.3.6.1.4.1.5233.4.11.1.1	transEventEntry	Start of alert entry
1.3.6.1.4.1.5233.4.11.1.1.1	transEventIndex	Index of the event within event list

Object Identifier	MIB Label	Description
1.3.6.1.4.1.5233.4.11.1.1.2	txnSubAlertInstance Owner	Index of the subalert instance owner from the subalert instance table
1.3.6.1.4.1.5233.4.11.1.1.3	transactionName	Transaction name
1.3.6.1.4.1.5233.4.11.1.1.4	organization	Group name
1.3.6.1.4.1.5233.4.11.1.1.5	host	Host name
1.3.6.1.4.1.5233.4.11.1.1.6	location	Location name
1.3.6.1.4.1.5233.4.11.1.1.7	script	script name
1.3.6.1.4.1.5233.4.11.1.1.8	eventTime	Event time
1.3.6.1.4.1.5233.4.11.1.1.9	eventActualDescript ion	Description of event (for example, “Response time 3.00 seconds”)
1.3.6.1.4.1.5233.4.11.1.1.1 0	txnErrorMessage	Error message generated during a script run

Configuring SMTP Mails

You can send e-mail alerts and scheduled reports via a configured SMTP server or via the Microsoft SMTP Service.

Note: UNIX uses the **sendmail** application for sending SMTP e-mails and, therefore, SMTP settings are not needed for Unix systems. Contact your system administrator to configure sending e-mails correctly for Unix systems.

You can configure a primary SMTP server and an alternate SMTP server. Mercury Business Availability Center uses the primary server and only if the primary server fails to send the message, attempts to use the alternate server.

The primary and alternate SMTP servers are setting values that are configured in Infrastructure Settings. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Alerting**, and locate the entry in the Alerting-Triggered alerts table.

Both the primary and alternate SMTP server can be defined as either:

➤ a designated server with a defined port number

Enter a server name for sending SMTP e-mails as the value in the **SMTP server** or **Alternate SMTP server** field and enter a port number for the server in the **SMTP server port** or **Alternate SMTP server** field.

➤ Microsoft's SMTP services

Enter <SMTPSVC> as the value in the **SMTP server** or **Alternate SMTP server** field. There is no need to enter a port number when using Microsoft SMTP services.

Note: If you use the Microsoft SMTP service to send e-mail alerts, Mercury Business Availability Center cannot send the e-mail-based Performance Update report (which you configure in Scheduled Reports) in HTML format. The report must be sent as an HTML, MHT, CSV, or PDF attachment.

Adding a Custom Pager or SMS Service Provider

If you are configuring pager or SMS alerts and your pager or SMS service provider does not appear on the default provider list and the provider uses an e-mail gateway, you can manually add your provider to Mercury Business Availability Center. After doing so, your provider appears on the list.

Provider Uses E-mail Gateway

To add a provider that uses an e-mail gateway, manually add the gateway information to the management database. If necessary, ask your database administrator for assistance.

To add a provider that uses an e-mail gateway:

1. Open the **NOTIFICATION_PROVIDERS** table in the management database.
2. In the **NP_NOTIFICATION_PROVIDER_NAME** column, add the name of the provider to the bottom of the list. Add the name exactly as you want it to appear in the provider list that opens in the Recipient Properties dialog box of the Recipients page in Platform Administration.

   Note the ID number that is automatically assigned to the provider.
3. Close the **NOTIFICATION_PROVIDERS** table, and open the **NOTIFPROVIDER_NOTIFTYPE** table.
4. In the **NN_NOTIF_PROVIDER_ID** column, add the ID number that was assigned to the new provider in step 2.
5. In the **NN_NOTIF_TYPE_ID** column, assign the provider one of the following notification types:
   - ➤ **102** – for pager service provider
   - ➤ **101** – for SMS service provider
6. Close the **NOTIFPROVIDER_NOTIFTYPE** table, and open the **NOTIFICATION_PROVIDER_PROP** table.
7. In the **NPP_NOTIFICATION_PROVIDER_ID** column, add the ID number that was assigned to the new provider in step 2. Note that you add the ID number to two consecutive rows.

8 In the **NPP_NPROVIDER_PROP_NAME** and **NPP_NPROVIDER_PROP_VALUE** columns, add the following new property names and values for the provider, one beneath the other (for examples, see existing entries):

Property Name	Property Value	Description
EMAIL_SUFFIX	<email_suffix>	The gateway's e-mail suffix. For example, if the gateway e-mail address is 12345@xyz.com, enter xyz.com as the property value for EMAIL_SUFFIX.
EMAIL_MAX_LEN	<max_length>	The maximum message length, in characters, of the body of the e-mail message. For example, 500. When determining this value, take into consideration the maximum length limit imposed by your service provider, as well as limitations to your pager or mobile phone.

9 In the **NPP_NPROVIDER_PROP_DATATYPE_ID** column, specify an ID value as follows:

- for EMAIL_SUFFIX, specify: 1
- for EMAIL_MAX_LEN, specify: 2

10 Restart the Mercury Business Availability Center service.

Generating Tickets in Help Desk Systems

Mercury Business Availability Center alerts can automatically generate new tickets in popular help desk systems (Remedy Action Request System and Blue Ocean Track-It!). The alerts can then be managed, escalated, and so forth, in the help desk application.

Integrating Mercury Business Availability Center with Remedy Action Request Help Desk version 4.0 or Later

When an alert is triggered, Mercury Business Availability Center sends e-mail to the Remedy Mail Service. The service generates a ticket in the Remedy Action Request help desk system.

Remedy accepts only e-mails that have a specific structure in the body of the mail. This structure is specific to each site and changes from customer to customer. The alert that you create in Mercury Business Availability Center, therefore, must be of this same structure.

The following procedure explains how to find the format in the Remedy management application, and how to copy it to an e-mail alert recipient.

In Remedy, perform the following steps:

1. Log into the Action Request System's Administrative Tool as the administrator.
2. Select **Tools** > **Export Mail Template**. Remedy opens the Export Mail Templates dialog box.
3. Export the form you would like to connect to the alerts. It should contain all of the required fields for generating a ticket. Save the file.
4. Open the exported file in a text editor. You will copy the contents of this file into the notification template in the next procedure.
5. Install the Remedy Mail Server service (if not yet installed), and configure it to start automatically on startup.
6. Create a dedicated e-mail profile and e-mail box and configure the mail server to work with them. If the service is already running, open the **<remedy installation directory>\conf\ar.cfg** file and note the mailbox being used for the service. You will need this address when defining the alert recipient.

In Alerts Management, perform the following steps:

1 In Platform Administration, select **Alerts and Recipients** > **Notification Templates**. Mercury Business Availability Center opens the Template Manager. Click the **New Template** button to open the New Template Properties dialog box.

2 In the **Name** field, enter Remedy.

3 Copy the contents of the file you exported in Remedy into the **Alert Specific Information** table.

Note: Do not make any changes to these contents, as Remedy relies on this format and will reject any modified formats. You can, however, add fields from another section of the Properties dialog box. For example, the line
Description !240000007!:
could be replaced with
Description !240000007!: <Alert Name>

4 Click **Save** to save the template.

5 Select **Alerts and Recipients** > **Recipients**. The Recipients dialog box opens.

6 Click **New Recipient** to open the Recipient Properties dialog box.

7 Create a new alert notification recipient and enter the Remedy mailbox as the e-mail address. In the General tab, choose the Remedy template. Click **Save** to save the recipient.

8 For each alert that you want to send to Remedy, add the Remedy recipient as one of the recipients of that alert.

Integrating Mercury Business Availability Center with Blue Ocean Track-It! Version 4.1

When an alert is triggered, an alert e-mail is sent to the Track-It Receive module, which generates a ticket in the Track-It! Help Desk – Work Orders module.

To implement the integration:

If a dedicated e-mail profile for the help desk system does not exist, you must create one.

1. Open the **tirecv.exe** file from the Track-It! installation directory. Add this application to the startup directory of your computer.
2. Select **Options** > **Configure E-mail**. The Configure Mapi Mail dialog box opens.
3. Select the help desk e-mail profile you created in step 1.
4. Choose the frequency with which you want alert e-mails to be monitored in the Track-It Receive application, in the time interval slot.
5. In the Track-It! main window, select **File** > **Administration** > **Configure Track-It!** and choose the **Notify** tab.
6. Set your e-mail preferences in the Configure Track-It Notify dialog box.
7. Configure the help desk as a recipient. For details about creating alert recipients, see “Configuring and Selecting Recipients” on page 181. Enter the e-mail address you created in step 1 as the recipient's e-mail address.
8. Add this recipient to any alert definition you want to forward to Track-It!

Part IV

Scheduled Reports

19

Scheduled Reports

You can configure Mercury Business Availability Center to send reports at predefined times to specific users.

About Scheduled Reports

You configure scheduled reports to enable specific recipients to automatically receive performance reports, via e-mail, at regularly defined intervals. You configure scheduled reports in the Platform Administration area of the Administration Console.

You can schedule the following reports to be sent:

- **user report.** A report based on one of the user reports (custom or trend report) defined in the End User Management, Service Level Management, or System Availability Management applications. For details on configuring user reports, see “Configuring and Viewing User Reports” in *Working with Applications*.
- **Performance Update report.** A summary report of key performance data for a specified Business Process profile. For details on the Performance Update report, see “The Performance Update Report” on page 307.

Note: By default, the value that appears in the "From" field in the e-mail containing the scheduled report is **MercuryAM_Alert_Manager@<Mercury Business Availability Center server name>**. You can modify the value by selecting **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and the **Scheduled Reports** context. Modify the value **Email sender** or **Scheduled Reports email sender address** (to include an e-mail address in the From field). For details on modifying values, see "Editing Infrastructure Settings" on page 76.

Scheduling User Reports or the Performance Update Report

You configure scheduled reports by defining which type of report to send, the frequency with which the report is sent, to whom the report is sent, and in what format the generated report is delivered.

For details on managing scheduled reports, see "Managing Scheduled Reports" on page 304.

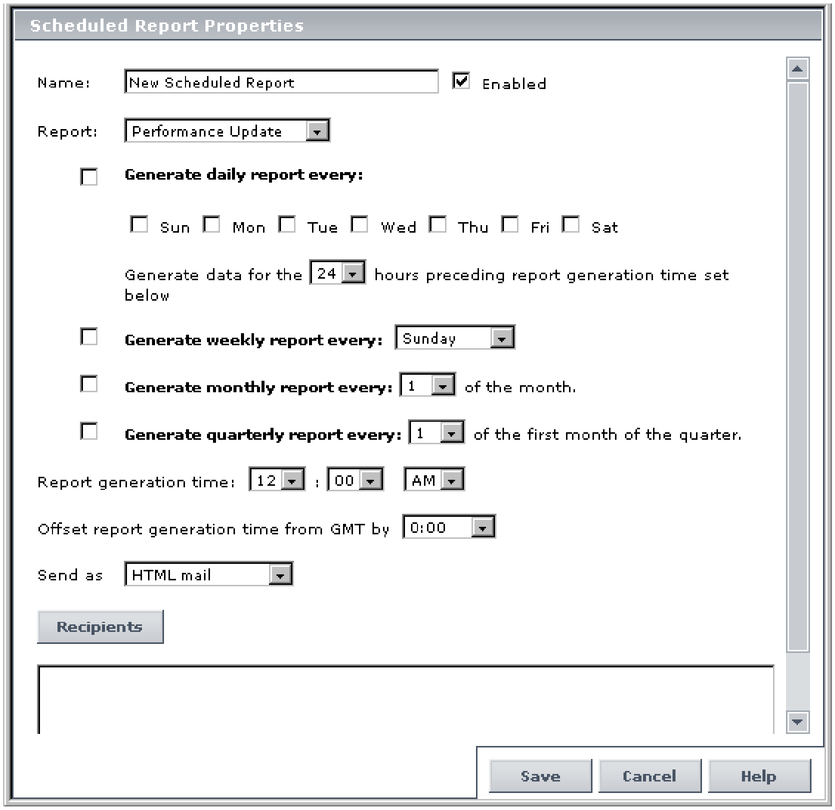
Note: To correctly view scheduled reports received in Microsoft Outlook 2003, in **Tools** > **Options** > **Security** > **Zone Settings**, select **Internet**; click Custom Level and specify the following settings in the Security Settings dialog box: **Download signed ActiveX control** = **Prompt, Run ActiveX controls and plug-ins** = **Enable, Script ActiveX controls marked safe for scripting** = **Enable**; in the **Reset to** list, select **Medium**.

To schedule a user-defined report or Performance Update report:

1. Select **Admin** > **Platform** > **Scheduled Reports**.
2. Select **User-Defined Reports** to schedule a user-defined report or the Performance Update report.
3. If you are scheduling a Performance Update report, select the profile upon which you want to base the scheduled report.

If you are scheduling a user-defined report (custom or trend report), select a profile to which the scheduled report is assigned for internal management purposes. You can choose any profile, but keep in mind that if you later delete that profile, the scheduled report will not be sent.

4 Click **New Scheduled Report** to open the Scheduled Report Properties dialog box.



Scheduled Report Properties

Name: New Scheduled Report ☑ Enabled

Report: Performance Update

□ **Generate daily report every:**

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Generate data for the 24 hours preceding report generation time set below

□ **Generate weekly report every:** Sunday

□ **Generate monthly report every:** 1 of the month.

□ **Generate quarterly report every:** 1 of the first month of the quarter.

Report generation time: 12 : 00 AM

Offset report generation time from GMT by 0:00

Send as HTML mail

5 In the Name box, specify a name for the report, for example, “Kim’s daily update of MyProfile.”

6 In the Report list, if you selected the **User-Defined Reports** menu item, select either Performance Update or one of the listed user-defined reports. If no user-defined reports exist, only the Performance Update is listed.

Note: If you choose a user-defined report that is later deleted, after report deletion, the scheduled report will not be sent.

7 Select a schedule for the report. You can choose from any of the following options (you must choose at least one):

- To send a report on a daily basis, select **Generate daily report every** and the days of the week on which the report should be sent.

  You can also select how many hours of data will appear in the report. The number of hours of data you indicate will be the hours directly preceding the **Report generation time** set. The default is 24 hours of data.

- To send a report on a weekly basis, select **Generate weekly report every** and the day of the week on which the report should be sent.
- To send a report on a monthly basis, select **Generate monthly report every** and the day of the month on which the report should be sent. Note that, when necessary, months with less than 31 days are rounded down.
- To send a report on a quarterly basis, select **Generate quarterly report every** and the day of the first month of the quarter on which the report should be sent. Note that, when necessary, months with less than 31 days are rounded down.

8 From the **Report generation time** lists, select the time of day at which the report should be sent.

9 In the **Offset report generation time from GMT by** box, specify the time zone, relative to GMT, by which you want to offset the time at which the report is sent. For example, to specify Eastern Standard Time, type -5 since EST is equivalent to GMT -5:00.

For a reference list of GMT time zones for locations throughout the world, see “GMT Time Zones” in *Reference Information*.

10 Specify whether to send the report as:

- **HTML mail.** The report is displayed in the e-mail client (the e-mail client must support, and be configured to display, HTML). All report resources (for example, graphics) are located on Mercury Business Availability Center servers. A network connection to Mercury Business Availability Center is required to view the report.

- **HTML attachment.** The report is displayed in a browser. All report resources (for example, graphics) are located on Mercury Business Availability Center servers. A network connection to Mercury Business Availability Center is required to view the report.
- **MHTML mail.** The report is displayed in the e-mail client (the e-mail client must support, and be configured to display, HTML). All report resources (for example, graphics) are included in the mail.
- **MHT attachment.** The report is displayed in a browser (the browser must support the MHT format—Microsoft Internet Explorer supports MHT format, for example). All report resources (for example, graphics) are included in the mail. Select **Zipped attachment** to send the report as a zipped attachment.
- **CSV mail.** The report is displayed in the e-mail client (the e-mail client must support, and be configured to display, HTML). All report resources (for example, graphics) are included in the mail.
- **CSV attachment.** The report is displayed in a program capable of displaying CSV format files (for example, Microsoft Excel). The report includes only tabular data and no graphics resources.
- **PDF attachment.** The report is displayed in PDF format in a new browser window. Select **Zipped attachment** to send the report as a zipped attachment.

Note: If you choose to use the HTML/MHTML mail option (which displays the report content in the e-mail client), make sure that the e-mail client does not employ security restrictions which prevent the running of scripts contained in HTML mail. E-mail clients that do employ such restrictions may be unable to properly display all report content.

11 Specify the report recipients by clicking the **Recipients** button and selecting the required recipients in the Select Recipients window. Click **OK** to save the settings and return to Scheduled Report Properties dialog box.

For details on configuring recipients, see “Configuring and Selecting Recipients” on page 181.

12 Click **Save** to save settings and close the Scheduled Report Properties window. The scheduled report is added to the list.

Managing Scheduled Reports

You can edit scheduled reports, disable or enable them, duplicate them, e-mail them on demand, and delete them.

To edit a scheduled report:

1. Click the **Modify Scheduled Report** button to open the Scheduled Report Properties window.
2. Modify settings as required, and click **Save**.

To duplicate a scheduled report:

1. Click the **Duplicate Scheduled Report** button to open the Scheduled Report Properties window.
2. Specify a new name for the report, and modify report properties as required.
3. Click **Save**. The report is added to the report list.

Note: If the scheduled report is configured for a custom report that no longer exists, the report is not sent.

To enable a scheduled report:

1. Select one or more reports to enable them to be sent to recipients.
2. Click the **Enable scheduled report** button at the bottom or side of the report list. Confirm that you want to enable the scheduled report(s).
3. Click **OK** in the dialog box.

To disable a scheduled report:

1 Select one or more reports to disable them, that is, they will not be sent to recipients.

2 Click the **Disable scheduled report** button at the bottom or side of the report list. Confirm that you want to disable the scheduled report(s).

3 Click **OK** in the dialog box.

To delete a scheduled report:

1 Select one or more scheduled reports to delete.

2 Click the **Delete Scheduled Report(s)** button at the bottom or side of the report list. Confirm that you want to delete the scheduled report(s).

To e-mail a scheduled report:

1 Select one or more reports report to e-mail.

2 Click the **E-mail Scheduled Report(s)** button at the bottom of the report list to open the Send Scheduled Report Now window.

3 For each selected report, modify the recipients and report time frame, or accept the default values.

4 Click **Send** to send the report.

20

The Performance Update Report

The Performance Update report is a summary report of key performance data for the transactions in a specific profile. The Performance Update report is a scheduled report sent via e-mail.

About the Performance Update Report

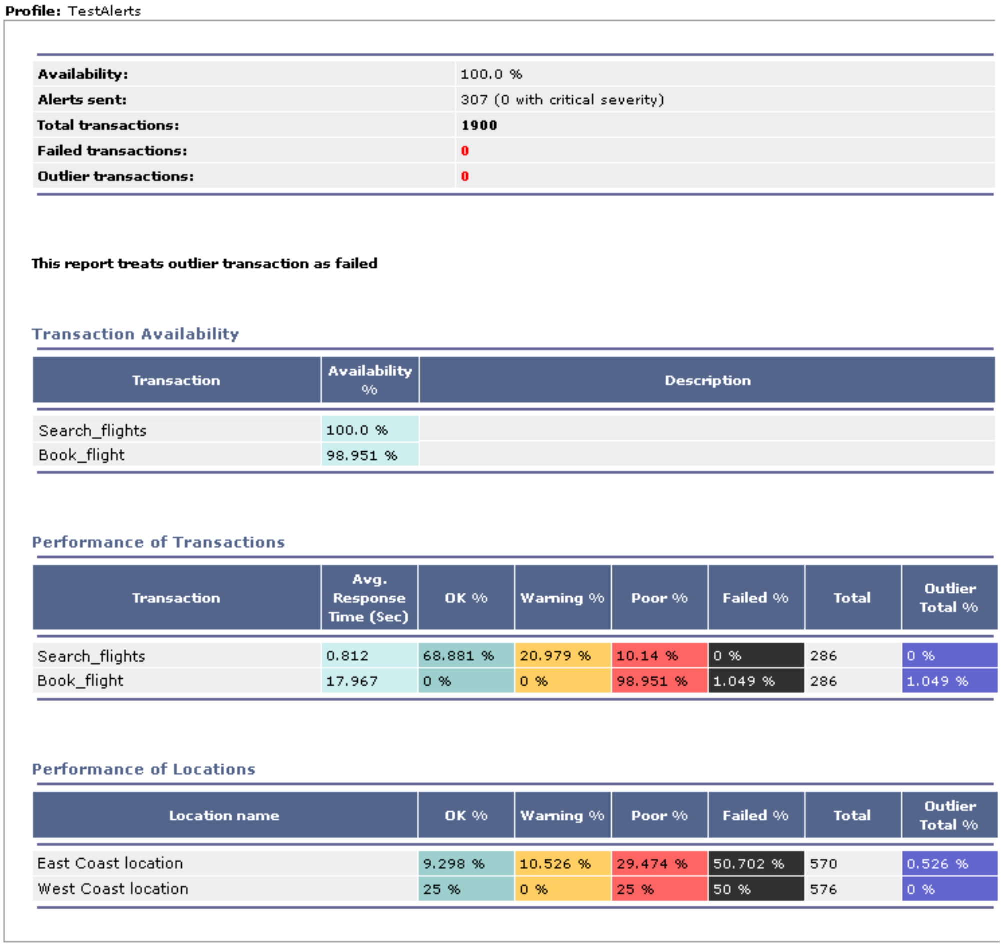
The Performance Update report is a scheduled report that is configured to be sent to specified recipients, via e-mail, on a periodic basis. The report includes key metrics on the performance of the transactions and locations defined in a specific profile.

For details on scheduling the Performance Update report, see “Scheduling User Reports or the Performance Update Report” on page 300.

You can also add components of the Performance Update report to custom reports. For details, see “Configuring and Viewing User Reports” in *Working with Applications*.

Viewing the Performance Update Report

You view the Performance Update report either in your e-mail client or in a Web browser.



Profile: TestAlerts

Availability:	100.0 %
Alerts sent:	307 (0 with critical severity)
Total transactions:	**1900**
Failed transactions:	**0**
Outlier transactions:	**0**

This report treats outlier transaction as failed

Transaction Availability

Transaction	Availability %	Description
Search_flights	100.0 %	
Book_flight	98.951 %	

Performance of Transactions

Transaction	Avg. Response Time (Sec)	OK %	Warning %	Poor %	Failed %	Total	Outlier Total %
Search_flights	0.812	68.881 %	20.979 %	10.14 %	0 %	286	0 %
Book_flight	17.967	0 %	0 %	98.951 %	1.049 %	286	1.049 %

Performance of Locations

Location name	OK %	Warning %	Poor %	Failed %	Total	Outlier Total %
East Coast location	9.298 %	10.526 %	29.474 %	50.702 %	570	0.526 %
West Coast location	25 %	0 %	25 %	50 %	576	0 %

You view the following information in the Performance Update report:

- **Report title and frequency.** Displays the title of the report, and in parentheses the report frequency.

  Time zone and time frame for report. Displays the configured time zone relative to GMT, as well as the time frame of the report (for a reference list of GMT time zones for locations throughout the world, see "GMT Time Zones" on page 19 in *Reference Information*).

- **Profile name.** Displays the Business Process profile upon which the report is based.
- **Availability.** Displays the percentage of transactions that succeeded (did not fail) during the measured period.
- **Alerts sent.** Displays the total number of alerts sent, including the number of critical severity alerts, for the measured period.
- **Total transactions.** Displays the total number of transactions run during the measured period.
- **Failed transactions.** Displays the total number of failed transactions for the measured period.
- **Outlier transactions.** Displays the total number of outlier transactions for the measured period.
- **Outlier transaction reporting status.** Describes whether Mercury Business Availability Center ignores outlier transactions in reports, or treats them as failed transactions (this setting is defined during profile definition in Monitor Administration).
- **Transaction Availability.** Displays the availability rate for each transaction in the profile, for the measured period. If a description of the transaction is set, the description is also displayed (this setting is defined during transaction monitor configuration in Monitor Administration).

- **Performance of Transactions.** Displays, for the measured period and for each transaction, average transaction response time, the percentage of transaction instances that fell into each defined transaction threshold range, (OK, Minor, and Critical), the percentage of failed transaction instances, the total number of transaction instances, and the percentage of outlier transaction instances.
- **Performance of Locations.** Displays, for the measured period and for each location, the percentage of transactions that fell into each defined transaction threshold range, (OK, Minor, and Critical), the percentage of failed transaction instances, the total number of transactions, and the percentage of outlier transactions.

  You define transaction thresholds—to specify the OK, Minor, and Critical range for each transaction—when you create a profile. You can also modify the transaction threshold ranges, as well as the default outlier value of 45 seconds, from Monitor Administration. For details, see “Transaction Threshold Settings” on page 54 in *End User Management Data Collector Configuration*.

Part V

Users and Permissions

21

User and User Group Management

Mercury Business Availability Center enables you to create users, groups of users, and groups of groups (nested groups) for increased flexibility in managing accessibility to the platform.

User Management

You define and manage Mercury Business Availability Center users in the User Management page under the Users and Permissions tab of Platform Administration.

User Management includes:

- Defining New Users – for details see page 314
- Managing Users – for details see page 317

Once you have created users, you can create groups for those users. For details, see “User Group Management” on page 320. You can also apply detailed permissions scenarios to the users and groups defined in your platform. For details, see “Configuring User Permissions” on page 329.

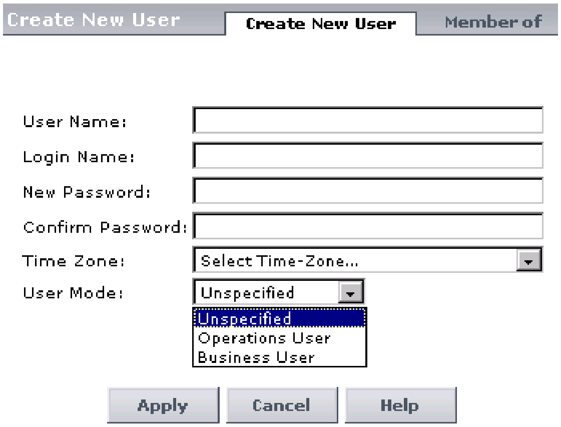
Defining New Users

You define new users by assigning them a user name, a login name, and a password. The login name is the unique identifier for the user.

To define a new user:

1 Select **Admin** > **Platform** > **Users and Permissions** > **User Management**. The User Management page opens, displaying all existing users.

2 Click the **New User** button to open the Create New User dialog box.



User Name:

Login Name:

New Password:

Confirm Password:

Time Zone: Select Time-Zone...

User Mode: Unspecified

3 Type a user name in the **User name** box.

Note: For both the user name and login name, all special characters are allowed except the following: “ \ / [ ] : | < > + = ; , ? *

4 Type a login name for the user in the **Login name** box. The user must use the assigned login name whenever accessing Mercury Business Availability Center.

5 Type a password in the **New Password** box, and retype it in the **Confirm Password** box to verify it.

6 Select the appropriate time zone for the user from the **Time Zone** list.

7 Select the **User Mode** for the user. Mercury Business Availability Center enables you to work with two user modes, operations and business, and different versions of Dashboard KPIs can be defined for each mode. Users see the KPI version appropriate for their user mode. For details, see "KPIs for User Modes" in *Application Administration*.

Select from the following options:

- ➤ **Unspecified.** Leaves the user without a particular mode. Select this option if:
  - Mercury Business Availability Center is working with user modes and you want this user to see KPIs for both modes in Dashboard views.
  - Your system is not working with user modes.
- ➤ **Operations User.** Enables the user to view the operations version of KPIs.
- ➤ **Business User.** Enables the user to view the business version of KPIs.

8 Click **Apply**. Mercury Business Availability Center adds the user name and properties to the existing users list.

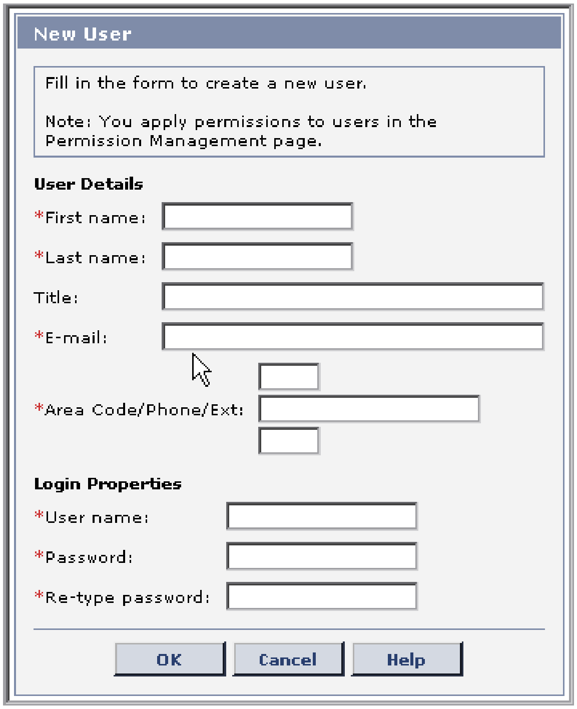
Click **Cancel** to close the dialog box without saving settings.

9 To create additional users, repeat steps 2-9. Create as many new users as you need.

To define new Mercury Managed Services users:

1. In Platform Administration, select **Users and Permissions** > **User Management**. The User Management page opens, displaying all existing users.

2. Click the **New User** button to open the New User dialog box.



New User

Fill in the form to create a new user.

Note: You apply permissions to users in the Permission Management page.

User Details

*First name:

*Last name:

Title:

*E-mail:

*Area Code/Phone/Ext:

Login Properties

*User name:

*Password:

*Re-type password:

3. Enter the user details. Those marked with a red asterisk are required fields.

4. Enter the login properties. Those marked with a red asterisk are required fields.

Note: For the user name, all special characters are allowed except the following: “ \ / [ ] : | < > + = ; , ? *

The login properties are used to login to mms.mercury.com.

5 Click **OK**. Mercury Managed Services adds the user name and properties to the existing users list.

Click **Cancel** to close the dialog box without saving.

6 To create additional users, repeat steps 2-5. Create as many new users as you need.

Managing Users

Once you have created users, you can use the User Management page to perform the following tasks:

- Rename a user – for details, see page 318
- Modify the user time zone – for details, see page 318
- Change a user's password – for details, see page 319
- Delete a user – for details, see page 319

Note: One superuser is defined for every installation of Mercury Business Availability Center. This superuser's default login name and password are admin, admin. This original superuser is not listed among the users in User Management and, therefore, this user's password can be changed only in the Change Password page under Personal Settings (**Admin** menu > **Personal Settings**). For details, see "Changing the User Password" on page 387.

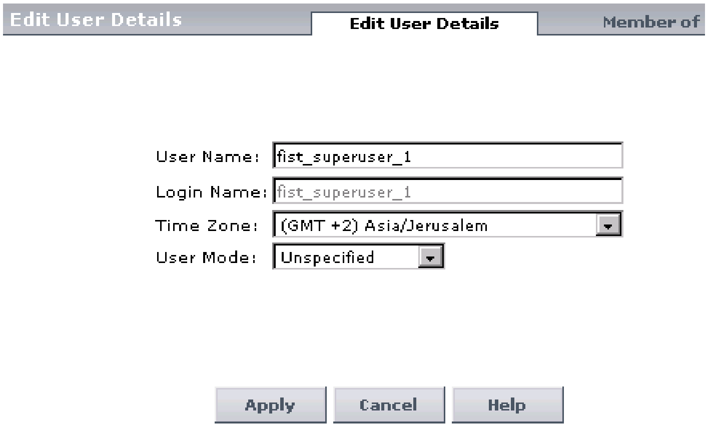
The superuser permissions role can be applied to other users in the system. These users with superuser permissions are listed, and can be modified, in User Management. For details on applying permissions, see "Configuring User Permissions" on page 329.

To modify the user name, time zone, or user mode of an existing user:

Note: This option is not available to Mercury Managed Services customers. Customers can change the user name and time zone settings from the Personal Settings area.

---

1. In Platform Administration, select the **Users and Permissions** tab > **User Management**. The User Management page opens, displaying the list of existing users.
2. Select the user whose name and/or time zone you want to modify.
3. Click the **Edit user details** button to open the Edit User Details dialog box and display the user's current user name, login name and time zone.



User Name: fist_superuser_1

Login Name: fist_superuser_1

Time Zone: (GMT +2) Asia/Jerusalem

User Mode: Unspecified

4. Modify the user name in the **User name** box and/or time zone in the **Time zone** box as required. Note that the login name is not editable.
5. Click **Apply** to save the changes.

   Click **Cancel** to close the dialog box without saving settings.

To change an existing user's password:

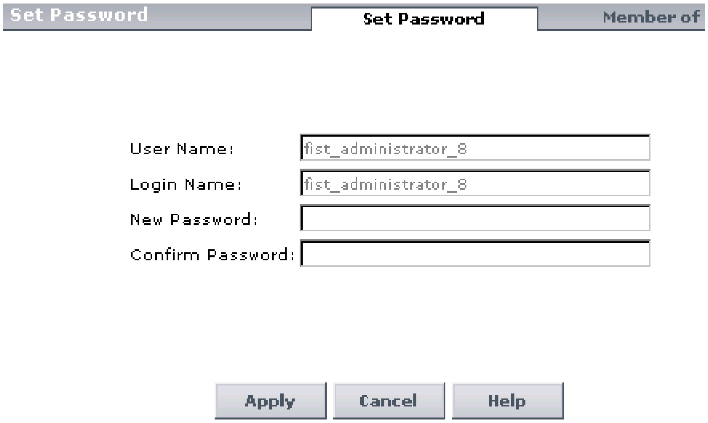
Note: This option is not available to Mercury Managed Services customers. Customers can change passwords from the Personal Settings area.

---

1 In Platform Administration, select the **Users and Permissions** tab > **User Management**. The User Management page opens, displaying the list of existing users.

2 Select the user whose password you want to modify.

3 Click the **Set user password** button to open the Set Password dialog box and display the user's current user name and login name.



User Name: fist_administrator_8
Login Name: fist_administrator_8
New Password:
Confirm Password:

4 Enter the new password in the **New Password** box and retype it into the **Confirm Password** box.

5 Click **Apply** to save the changes.

Click **Cancel** to close the dialog box without saving settings.

To delete an existing user:

1 In Platform Administration, select the **Users and Permissions** tab > **User Management**. The User Management page opens, displaying the list of existing users.

2. Select the check box next to the user you want to delete.

   To make your selections, you can also use the buttons at the bottom left of the page for, **Select All**, **Clear All**, and **Invert Selection.**

3. Click the **Delete** button and click **OK** to confirm that you want to delete the user. Mercury Business Availability Center deletes the user.

User Group Management

You group users to make managing user permissions more efficient. Instead of assigning access permissions to each user one at a time, you can group users who are assigned the same permissions levels on the same resources. You use the Permissions Management page to specify the access permissions on the group. For details, see "Configuring User Permissions" on page 329.

You may want to create different groups based on how users access the different resources in Mercury Business Availability Center. Examples of criteria for grouping users that are relevant to your organization may be:

- tasks within the organization:
  - customer service representatives
  - system administrators
  - high-level management
- locations and territories:
  - users working in different sales territories
  - users based on geographical location
  - users accessing network servers in different locations

User Group Management includes:

- Defining New User Groups – for details see page 321
- Managing User Groups – for details see page 323

Defining New User Groups

You define and manage user groups in Platform Administration. You group users to make it easier to manage their access permissions. The access permissions are inherited by the users of the group.

The group name is the unique identifier for the user group.

To define a new user group:

1. Select **Admin** > **Platform** > **Users and Permissions** tab > **User Group Management**. The User Group Management page opens, displaying the list of existing user groups.

2. Click the **New Group** button. The Create New Group dialog box opens and displays the **General** tab.

3. Type a group name in the **Group name** box.

Note: For the group name, all special characters are allowed except the following: “ \ / [ ] : | < > + = ; , ? *

---

4. Type a description for the group in the **Group description** box.

5. You can then either click the **Users** tab to assign the users to the group, or you can save the group and assign the users to the group at a later time. For more details, see below.

6. Click **Apply** to save the changes.

   Click **Cancel** to close the dialog box without saving the group.

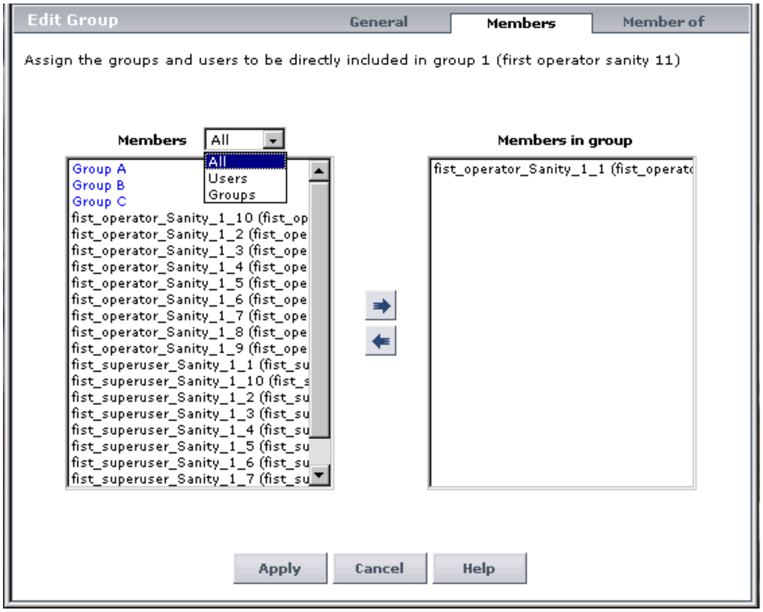
To assign users to a user group:

1. Select **Admin** > **Platform** > **Users and Permissions** tab > **User Group Management**. The User Group Management page opens, displaying the list of existing user groups.

2. Access the Users tab:

   ➤ If you are adding users to an existing group, select the group to which you want to add users and click the **Edit** button. The Edit Group page opens. Click the **Members** tab to open the page where you can assign users to the group.

➤ If you are adding users while you are creating a new group, click the **Members** tab to open the page where you can assign users to the group.



Assign the groups and users to be directly included in group 1 (first operator sanity 11)

Members: All

Group A
Group B
Group C
fist_operator_Sanity_1_10 (fist_op
fist_operator_Sanity_1_2 (fist_ope
fist_operator_Sanity_1_3 (fist_ope
fist_operator_Sanity_1_4 (fist_ope
fist_operator_Sanity_1_5 (fist_ope
fist_operator_Sanity_1_6 (fist_ope
fist_operator_Sanity_1_7 (fist_ope
fist_operator_Sanity_1_8 (fist_ope
fist_operator_Sanity_1_9 (fist_ope
fist_superuser_Sanity_1_1 (fist_su
fist_superuser_Sanity_1_10 (fist_s
fist_superuser_Sanity_1_2 (fist_su
fist_superuser_Sanity_1_3 (fist_su
fist_superuser_Sanity_1_4 (fist_su
fist_superuser_Sanity_1_5 (fist_su
fist_superuser_Sanity_1_6 (fist_su
fist_superuser_Sanity_1_7 (fist_su

Members in group:

fist_operator_Sanity_1_1 (fist_operato

3 Select the user in the **Members** box, and click the left-to-right arrow to move the user to the **Members in group** box. Repeat as needed for each user.

4 Click **Apply** to save the changes or click **Cancel** to close the dialog box without saving the changes.

Managing User Groups

You can change the name or description of a user group, and you can assign new users to a group or unassign existing users from an existing group.

To change the name and/or description of an existing user group:

1. Select **Admin** > **Platform** > **Users and Permissions** tab > **User Group Management**. The User Group Management page opens, displaying the list of existing user groups.
2. Select the group and click the **Edit** button. The Edit Group dialog box opens and displays the **General** tab.
3. Edit the group name and/or a group description in the **Group name** box.
4. Click **Apply** to save the changes or click **Cancel** to close the dialog box without saving the settings.

To assign or unassign users to the group:

1. Select **Admin** > **Platform** > **Users and Permissions** tab > **User Group Management**. The User Group Management page opens, displaying the list of existing user groups.
2. Select the group and click the **Edit** button. The Edit Group dialog box opens and displays the **General** tab.
3. In the **Edit Group** page, click the **Members** tab to open the page where you assign users to the group.
4. Assign users by selecting the user in the **Members** box, and clicking on the left-to-right arrow to move the user to the **Members in group**.

   Unassign users by selecting the user in the **Members in group** box, and clicking on the right-to-left arrow to move the user to the **Members** box.
5. Click **Apply** to save the changes.

   Click **Cancel** to close the dialog box without saving settings.

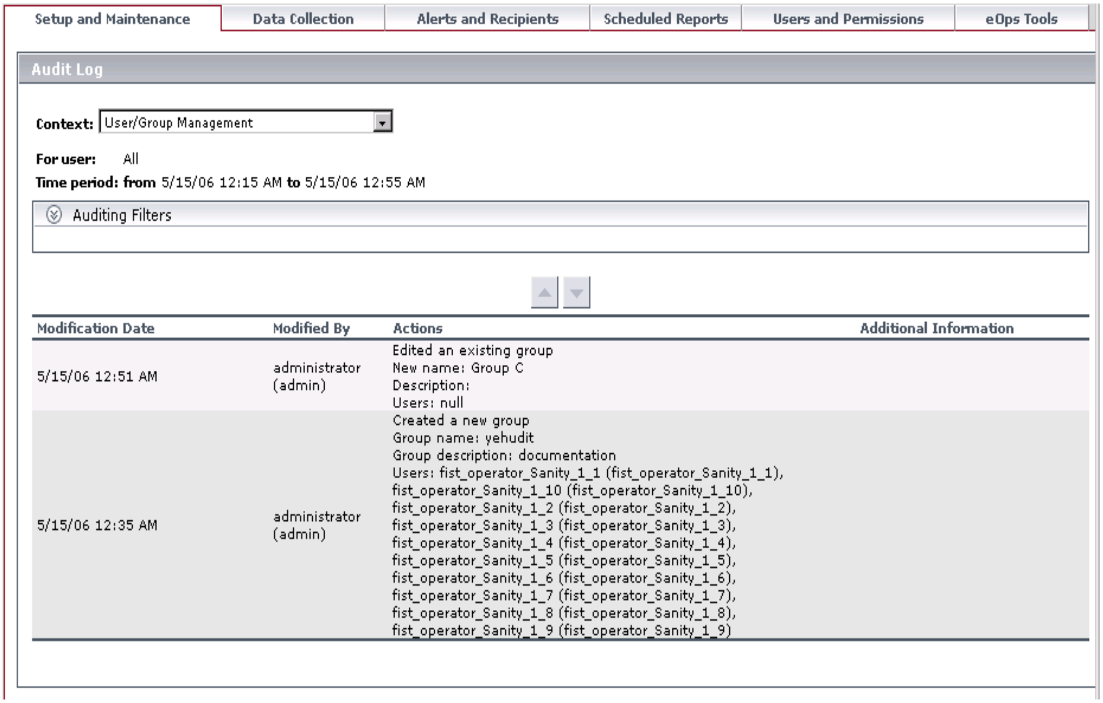
To delete existing user groups:

1. Select **Admin** > **Platform** > **Users and Permissions** tab > **User Group Management**. The User Group Management page opens, displaying the list of existing user groups.
2. Select the user group you want to delete.

   To make your selections, you can also use the buttons at the bottom left of the page: **Select All**, **Select None, Invert Selected** and **Delete Selected.**
3. Click the **Delete** button and click **OK** to confirm the deletion. Mercury Business Availability Center deletes the user group.

To check user and group activity in the audit log:

The Audit Log contains information about all user and group activity. For details, see “Using the Audit Log” on page 94.



Context: User/Group Management

For user: All

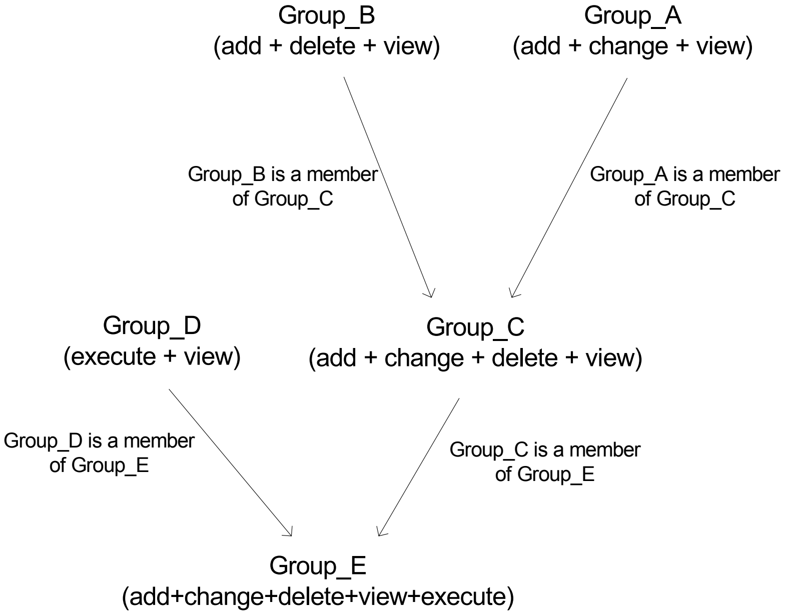
Time period: from 5/15/06 12:15 AM **to** 5/15/06 12:55 AM

Modification Date	Modified By	Actions	Additional Information
5/15/06 12:51 AM	administrator (admin)	Edited an existing group New name: Group C Description: Users: null	
5/15/06 12:35 AM	administrator (admin)	Created a new group Group name: yehudit Group description: documentation Users: fist_operator_Sanity_1_1 (fist_operator_Sanity_1_1), fist_operator_Sanity_1_10 (fist_operator_Sanity_1_10), fist_operator_Sanity_1_2 (fist_operator_Sanity_1_2), fist_operator_Sanity_1_3 (fist_operator_Sanity_1_3), fist_operator_Sanity_1_4 (fist_operator_Sanity_1_4), fist_operator_Sanity_1_5 (fist_operator_Sanity_1_5), fist_operator_Sanity_1_6 (fist_operator_Sanity_1_6), fist_operator_Sanity_1_7 (fist_operator_Sanity_1_7), fist_operator_Sanity_1_8 (fist_operator_Sanity_1_8), fist_operator_Sanity_1_9 (fist_operator_Sanity_1_9)	

Nested Groups Management

You can nest groups to make managing user and group permissions easier. Instead of assigning access permissions to each group one at a time, you can nest a group to inherit the permissions of its direct parent.

In the example below, Group_A and Group_B are nested members of Group_C. Group_C inherits the combined permissions of both groups. Group_C and Group_D are nested members of Group_E. Group_E directly inherits the permissions of Group_C and Group_D, and indirectly inherits the permissions of Group_A and Group_B.


Group_B
(add + delete + view)
Group_A
(add + change + view)
Group_B is a member of Group_C
Group_A is a member of Group_C
Group_D
(execute + view)
Group_C
(add + change + delete + view)
Group_D is a member of Group_E
Group_C is a member of Group_E
Group_E
(add+change+delete+view+execute)

When permissions are added to, or removed from, a nested group, the changes are automatically implemented in the nested group's immediate parent and continue to propagate onward. For example, if delete permission in Group_B is removed, Group_C's permissions become add + change + view. Group_E's permissions become add + change + view + execute.

Nested Group Management includes:

- Notes and Limitations – for details see page 326
- Setting Up Nested Groups – for details see page 326
- Removing a Nested Group from Its Parent – for details see page 327

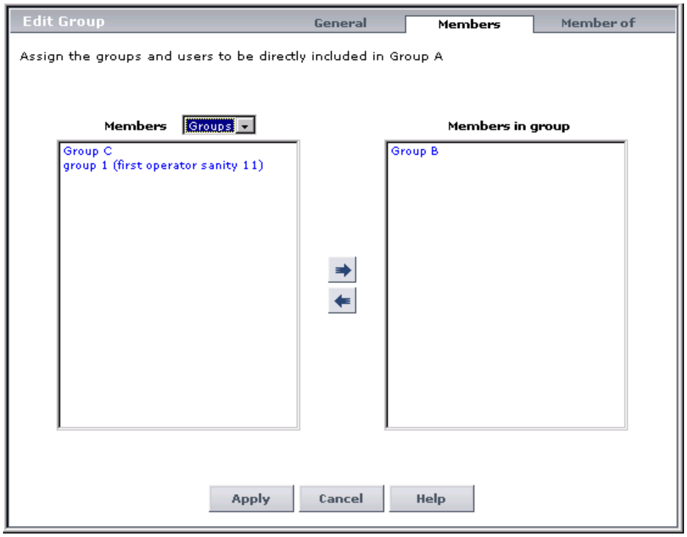
Notes and Limitations

- A group can be a member of several groups.
- A circle of nested groups is not permitted. For example, Group_A is a member of Group_B, and Group_B is a member of Group_C. Group_C can not be a member of Group_A.
- Permissions are assigned to nested groups in the same way as for regular, not nested, groups. Changes in nested group permissions take effect at the user's next login.
- There is no maximum number of levels of nested groups.

Setting Up Nested Groups

1. Select **Admin** > **Platform** > **Users and Permissions** > **User Group Management**. The User Group Management page opens.
2. Click the **Edit** button of the group to contain the nested group. The Edit Group dialog box opens.

3 Click the **Members** tab. A list of users and groups that can be assigned as members of your selection is displayed in the **Members** column. Users and groups already assigned as members are displayed in the **Members in group** column. Groups are listed in blue. Members that are already a part of the group, and members that are direct parents are not listed.



Assign the groups and users to be directly included in Group A

Members: Groups

Group C
group 1 (first operator sanity 11)

Members in group:

Group B

4 Use the right and left arrow buttons to assign or remove groups from your selection.

5 Click the **Members of** tab to view a list of the groups that include your selection.

6 Click **Apply** to save the changes or click **Cancel** to close the dialog box without saving the changes.

Removing a Nested Group from Its Parent

A nested group can be removed from its parent. The group itself is not deleted.

1 Select **Admin** > **Platform** > **Users and Permissions** > **User Group Management**. The User Group Management page opens.

2 Click the **Edit** button of the parent group that contains the group to be removed. The Edit Group dialog box opens.

3. Click the **Members** tab. Users and groups already assigned as members are in the **Members in group** column. Groups are listed in blue.
4. Use the arrow button to remove the group from your selection.
5. Click **Apply** to save the changes or click **Cancel** to close the dialog box without saving the changes.

22

Configuring User Permissions

Mercury Business Availability Center enables you to apply permissions to users and user groups for specific resources and instances of those resources that are defined in the system.

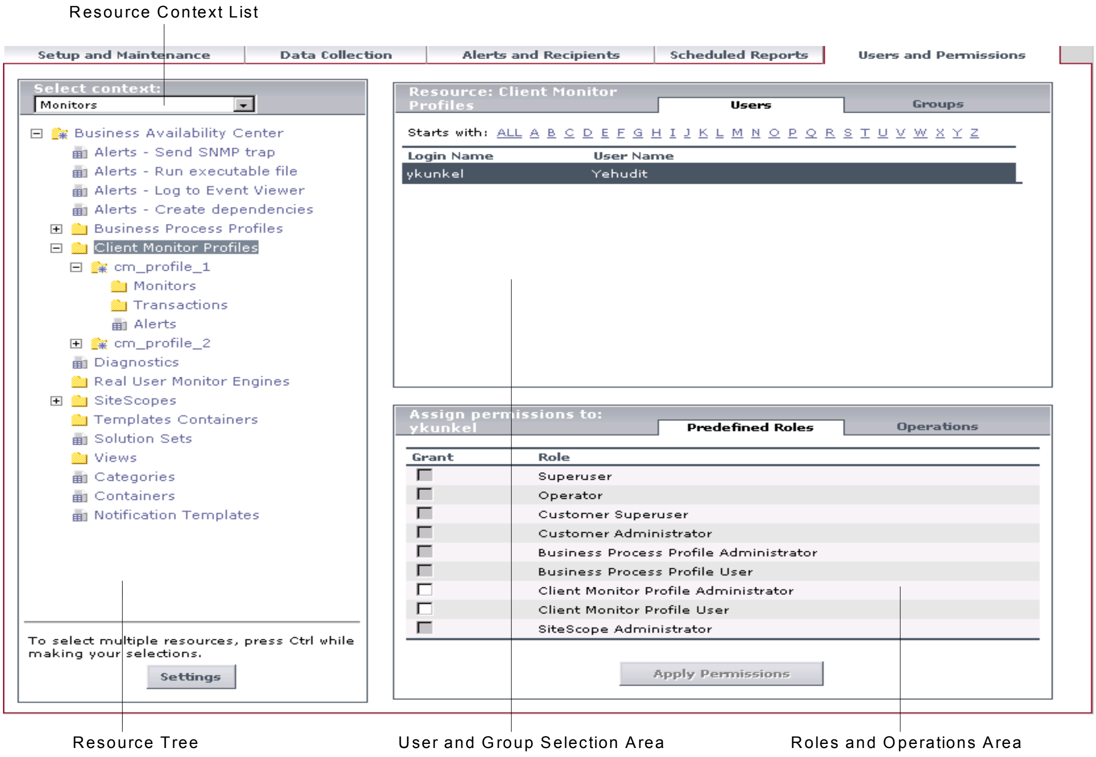
About User Permissions

You can enable sophisticated and detailed permissions scenarios for the users and user groups defined in your Mercury Business Availability Center platform. Permissions are based on both the user who is granted the permission and the resource on which the permission is granted.

Granting permissions has three components: the resource, the user, and the operation or role being granted. Each of these is represented by a different section in the Permissions Management page.

The Permissions Management page is divided into three main areas:

- resource tree area on the left side of the page– for details see "Understanding Permissions Resources" on page 331
- user and group selection area in the upper right-hand side of the page – for details see "Selecting Users and User Groups" on page 334
- roles and operations area on the bottom right-hand side of the page – for details see "Understanding Operations and Roles" on page 335



Select context: Monitors

- Business Availability Center
  - Alerts - Send SNMP trap
  - Alerts - Run executable file
  - Alerts - Log to Event Viewer
  - Alerts - Create dependencies
  - Business Process Profiles
  - Client Monitor Profiles
    - cm_profile_1
      - Monitors
      - Transactions
      - Alerts
    - cm_profile_2
  - Diagnostics
  - Real User Monitor Engines
  - SiteScopes
  - Templates Containers
  - Solution Sets
  - Views
  - Categories
  - Containers
  - Notification Templates

To select multiple resources, press Ctrl while making your selections.

Starts with: ALL A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Login Name	User Name
ykunkel	Yehudit

Grant	Role
□	Superuser
□	Operator
□	Customer Superuser
□	Customer Administrator
□	Business Process Profile Administrator
□	Business Process Profile User
□	Client Monitor Profile Administrator
□	Client Monitor Profile User
□	SiteScope Administrator

To grant or remove permissions, you must select a resource, select a user or user group, and check the operations or roles to apply. For details, see "Granting and Removing Permissions" on page 377.

Note: If you have upgraded from a previous version of Mercury Business Availability Center and had specific users and security levels defined, those users and security levels are mapped to the new roles functionality in Permissions Management. For details, see "Roles" on page 359.

You cannot specify profile or group permissions for the Event Log (for details, see "The Event Log" in *Using System Availability Management*). If SiteScope is configured to display events (for details, see the Mercury BAC Logging Settings in "Adding SiteScope Monitors to the Monitor Tree" in *Managing SiteScope*), a user without the appropriate SiteScope permission is able to view all SiteScope event data in the Event Log (by selecting **All Profiles** in the Profile box in the SiteScope Filters dialog box). If the user selects one of the profiles in the **Profile** list (the list is filtered for the user profile and group permissions) then the event data that is displayed by the Event log corresponds to event data filtered for that user profile or group permissions.

Understanding Permissions Resources

Mercury Business Availability Center enables you to finely tune your permissions management by applying permissions at the resource level. All of the resources on which permissions can be applied have been identified and categorized in a hierarchical tree, representing the Mercury Business Availability Center platform.

The resources and instances of those resources are organized according to logical groupings called contexts. These contexts make it easier to identify and select the area of the platform on which you want to apply permissions.

Resource Contexts

The resources are divided according to the context in which they function within the platform and not necessarily where they are found in the user interface.

While applying permissions, you select resources from the following contexts:

- **CMDB.** Includes the view resources for the CMDB in IT Universe
- **Monitors.** Includes all the resources relating to data collection and monitoring
- **Platform.** Includes all the resources for administering the platform
- **Production Analysis.** Includes all the resources relating to application performance lifecycle (APL)
- **Service Level Management.** Includes the SLA resource
- **User Defined Reports.** Includes the custom report, trend report, custom link, and Excel report resources
- **My BAC.** Includes resources needed to administer modules and portlet definitions.

For a detailed table, divided by context, describing how each operation is applied to each resource within each context, see "Operations" on page 336.

Resources and Resource Instances

There are three types of resources in Permissions Management and each is represented by a different icon in the resource tree:

- resource collection (a resource that can have instances)
- instance of a resource
- resource that cannot have instances in the permissions resource tree

An instance of a resource is displayed only if it has been defined in the platform. The instance of a resource appears as a child object of the resource in the tree with the name as it has been defined in the application. Once instances of a resource are defined in the system, the resource collection acts as the parent resource for those instances.

There are some resources, such as the different data collector profiles, that contain other resources within them in the resource tree hierarchy. Some of these subresource types appear only if there are instances of the resource defined in your platform, such as Monitor and Transaction resources within a profile resource.

Examples of Resources and Instances

An example of how resources and instances are displayed in the permissions hierarchy is the Business Process Profile resource within the Monitors context. The Business Process Profile resource includes instances only if there have been Business Process profiles defined in the system. If there are profiles defined in the system, each of those appears as an instance of the Business Process Profile resource with the name defined for the profile in Monitor Administration.

Because monitors, transactions, and alerts are defined in your platform per profile, the Monitors, Transactions, and Alerts resources appear under each of the instances of the profile resource. Monitors and Transactions are resource collections and can have their own instances, but Alerts is a resource that cannot have instances.

You can apply permissions to the Business Process Profile resource level. This enables the user access to all Business Process profiles created in the system. If you want to restrict a user’s access to only specific Business Process profiles that relate to the user’s tasks, you can apply permissions to a specific Business Process profile or to the Monitors resource or to any instance of monitors that have been defined under the profile.

Guidelines for Working with Resources

- The Business Availability Center resource refers to all contexts in Mercury Business Availability Center.
- Only roles and not operations can be applied to the Business Availability Center resource. For details, see “Roles” on page 359.
- To manage the permissions on a subresource, you must provide the user with at least **View** permissions on the selected resource's parent.

- You cannot grant **Add** permission on an instance of a resource, only on the resource itself.
- When a user defines or creates an instance of a resource, for example creates a Business Process profile, that user has **Full Control** permission on that resource instance and all of its child resources.
- Resources that cannot have instances in the permissions tree are divided into the following two types:
  - Resources that are functions or options within the system that do not have any other instances or types.

    For example, the outlier value resource determines whether the user can edit the outlier threshold value. It has no instances.
  - Resources that do have instances but permissions can be applied only on the resource type and affect all instances of the resource.

    For example, the category resource includes all categories defined in Monitor Administration. Change permissions granted on the categories resource enables a user to modify all the categories defined in the system. You cannot grant or remove permissions for specific categories, only for every category defined in Monitor Administration.

Selecting Users and User Groups

The users and user groups that appear in the Permissions Management page (upper right-hand area) are those users and user groups that have been created in your platform. For details on creating, editing, and managing users and user groups, see “User and User Group Management” on page 315.

You can choose to grant permissions to users or to user groups by selecting the appropriate tab in the user selection area. All of the users or user groups appear in an alphabetical listing.

When working with users, you can manipulate the list by selecting one of the letter links above the list to display only those users beginning with that letter. By default, all of the users are displayed. If you select a letter and want to revert to the complete list, you can select **ALL**.

Guidelines for Selecting Users Versus User Groups

When granting permission to users on the resources in Permissions Management, keep the following in mind:

- You can grant permission to only one user or user group at a time.
- If you have many users for whom you have to grant permissions, it is recommended that you organize your users into logical groups using the User Group Management page (for details, see “User Group Management” on page 322).

To assign permissions by group:

1. Create logical user groups based on groups of users that will likely have the same sets of permissions granted to them. These groups can be organized by department, task, location, project, and so forth.
2. Add the appropriate users to the groups. Note that users can be added to more than one user group.
3. Apply permissions based on the groups, rather than individual users.

Understanding Operations and Roles

You can grant permissions to users by selecting one of the two tabs in the roles and operations area of the Permissions Management page:

- **Operations.** Use to apply specific operations on a resource for a user or user group. For a detailed table of what each operation enables as it is applied to each resource, see below. When assigning operations, you can see the descriptions listed below as tooltips under the operations area. They appear when a resource is highlighted and you move your cursor over an operation.
- **Predefined Roles.** Use to apply a collection of operations that have been predefined for various resources. For a detailed description of each role, including which operations are applied to what resources, see “Roles” on page 359.

Operations

When working with operations, keep the following in mind:

- All of the operations that can be applied to a resource collection can also be applied to any instance of that resource. The one exception is the **Add** operation which cannot be applied to an instance of a resource.
- The **Full Control** operation automatically includes all the other operations available on the resource. When selected, the other operations will also be automatically selected.
- When the **Full Control** operation is applied to any resource, the user also has permissions to grant and remove permissions on that resource, or resource instance, for other users or user groups.
- When the **View** operation is one of the resource's available operations and you select one of the other available operations, the **View** operation will also automatically be selected.

Within each context listed below is a table listing every resource, which operations can be applied to that resource, and a description of what the operation enables.

CMDB

The **CMDB** context enables you to define the operations permitted for the views defined in IT Universe Administration and viewed in the View Explorer, Dashboard, and Service Level Management.

Resources	Operation	Description
Views	Add	Enables adding and cloning views in the View Manager
	Change	Enables adding a configuration item or relationship to a view; editing the view in the View Manager; and if user is the creator of the view, removing configuration items or relationships from the view
	View	Enables viewing the configured views in read-only mode
	Delete	Enables deleting views from the View Manager
	Full Control	Enables performing all available operations on the views in the view Manager and IT Universe Admin, viewing all views in the applications, and granting and removing permissions for those operations

Tip: If a user has permissions on a view in CMDB, all the profiles that are in that view are visible to the user, even if the user does not have permissions on the profile. To prevent a user from viewing profiles for which the user does not have permissions while enabling the user to access a view, create a view for the user including only those configuration items for which you want the user to have permissions and grant the user permission on that view.

Monitors

The **Monitors** context includes all those resources that relate to data collection and monitoring. These resources can be found in Monitor Administration, Platform Administration, and End User Management Administration.

The various profile resources (Business Process, Client Monitor, and SiteScope) determine the permissions level of the user in all areas of the platform where you must select a profile to access the page or perform the action. These include most areas of Monitor Administration, Alert Management, Downtime/Event Scheduling, Transaction Ordering, Transaction Coloring, and various Reports.

Some of the resources listed appear only when instances of the parent resource have been defined in the platform. For example, the Monitors and Transactions resources appear only as child objects of an instance of a Business Process Profile or Client Monitor Profile.

Resources	Operation	Description
Alerts - Send SNMP Trap	Change	Enables selecting the option to send SNMP traps on alert, editing SNMP trap addresses, and clearing the option to send SNMP traps on alert
	Full Control	Enables performing all available operations on sending SNMP traps on alerts, and granting and removing permissions for those operations
Alerts - Run Executable File	Change	Enables selecting the option to run an executable file on alert, selecting and editing executable files to run on alert, and clearing the option to run an executable file on alert
	Full Control	Enables performing all available operations on running an executable file on alert, and granting and removing permissions for those operations

Resources	Operation	Description
Alerts - Log to Event Viewer	Change	Enables selecting whether alerts should be logged in the Windows Event Viewer which is accessed from Windows Administrative Tools
	Full Control	Enables selecting whether alerts should be logged in the Windows Event Viewer, and granting and removing permissions on that operation
Alerts - Create Dependencies	Change	Enables creating and removing dependencies between alerts
	Full Control	Enables creating and removing alert dependencies, and granting and removing permissions for those operations

Resources	Operation	Description
Business Process Profiles	Add	Enables creating Business Process profiles
	Change	Enables renaming Business Process profiles and modifying profile properties
	View	Enables viewing the Business Process profile details in Monitor Administration, and the Business Process profile in any application that lists the profiles, such as Alert Management, Service Level Management, Downtime/Event Scheduling, Analytics, and reports
	Delete	Enables deleting Business Process profiles
	Execute	Enables running and stopping Business Process profiles
	Full Control	Enables performing all available operations on Business Process profiles, and granting and removing permissions for those operations

Resources	Operation	Description
Monitors (under Business Process Profile instance)	Add	Enables adding transaction monitors, WebTrace monitors, and single URL monitors (Managed Services only) to Business Process profiles
	Change	Enables editing transaction monitor, WebTrace monitor, and single URL monitor (Managed Services only) properties
	View	Enables viewing transaction monitor, WebTrace monitor, and single URL monitor (Managed Services only) properties
	Delete	Enables deleting transaction monitors, WebTrace monitors, and single URL monitors (Managed Services only) from the profile
	Full Control	Enables performing all available operations on transaction monitors, WebTrace monitors, and single URL monitors (Managed Services only), and granting and removing permissions for those operations
Transactions (under Business Process Profile)	Change	Enables editing transaction descriptions and threshold settings
	View	Enables viewing transaction details
	Full Control	Enables performing all available operations on transactions, and granting and removing permissions for those operations

Resources	**Operation**	**Description**
Outlier Value (under Business Process Profile > Transaction instance)	Change	Enables setting a transaction's outlier value
	Full Control	Enables setting the transaction's outlier value, and granting and removing permissions for that operation
Alerts (under Business Process Profile instance)	Add	Enables adding alerts to the Business Process profile
	Change	Enables editing details of alerts associated with the Business Process profile
	View	Enables viewing alerts in the Business Process profile and viewing alert details in Alerts Management
	Delete	Enables deleting alerts associated with the Business Process profile
	Full Control	Enables performing all available operations on the alerts in the Business Process profile, and granting and removing permissions for those operations

Resources	Operation	Description
Client Monitor Profiles	Add	Enables adding Client Monitor profiles
	Change	Enables renaming Client Monitor profiles and editing the profile properties
	View	Enables viewing the Client Monitor profile details in Monitor Administration, and the Client Monitor profile in any application that lists the profiles, such as Alerts Management, Service Level Management, Downtime/Event Scheduling, and reports
	Delete	Enables deleting Client Monitor profiles
	Execute	Enables running and stopping Client Monitor profiles
	Full Control	Enables performing all available operations on Client Monitor profiles, and granting and removing permissions for those operations

Resources	Operation	Description
Monitors (under Client Monitor Profile instance)	Add	Enables adding transaction monitors and traceroute monitors to Client Monitor profiles
	Change	Enables editing transaction monitor and traceroute monitor properties
	View	Enables viewing transaction monitor and traceroute monitor properties
	Delete	Enables deleting a transaction monitor or traceroute monitor from a Client Monitor profile
	Full Control	Enables performing all available operations on transaction monitors and traceroute monitors in a Client Monitor profile, and granting and removing permissions for those operations
Transactions (under Client Monitor Profile instance)	Change	Enables editing a transaction's description and threshold settings
	View	Enables viewing a transaction in a Client Monitor profile
	Full Control	Enables performing all available operations on a transaction in a Client Monitor profile, and granting and removing permissions for those operations

Resources	Operation	Description
Alerts (under Client Monitor Profile instance)	Add	Enables adding alerts to the Client Monitor profile
	Change	Enables editing details of alerts associated with the Client Monitor profile
	View	Enables viewing alerts in the Client Monitor profile
	Delete	Enables deleting alerts associated with the Client Monitor profile
	Full Control	Enables performing all available operations on the alerts in the Client Monitor profile, and granting and removing permissions for those operations
Diagnostics	Change	Enables viewing Diagnostics administration and configuring the Diagnostics settings
	View	Enables viewing the Diagnostics application when accessing Diagnostics from the Business Application Center
	Execute	Enables starting, stopping, and getting the status of a capture on a Deep Diagnostics server
	Full Control	Enables performing all operations on Diagnostics, and granting and removing permissions for those operations

Resources	Operation	Description
Real User Monitor Engines	Add	Enables adding Real User Monitor engines to Monitor Administration
	Change	Enables editing Real User Monitor engine details
	View	Enables viewing Real User Monitor engine details
	Delete	Enables removing Real User Monitor engines from Monitor Administration
	Full Control	Enables performing all available operations on Real User Monitor engines, and granting and removing permissions for those operations
Domains (under Real User Monitor Engine instance)	Add	Enables adding the Real User Monitor to general settings
	Change	Enables editing the Real User Monitor general settings
	View	Enables viewing the general settings of a Real User Monitor engine
	Full Control	Enables performing all available operations on Real User Monitor general settings, and granting and removing permissions for those operations

Resources	Operation	Description
RUM Applications (under Real User Monitor Engine instance)	Add	Enables adding applications to a Real User Monitor engine, and pages and transactions to an application
	Change	Enables editing the Real User Monitor application, page, and transaction details
	View	Enables viewing the Real User Monitor application, page, and transaction
	Delete	Enables deleting a page or transaction from a Real User Monitor application or a Real User Monitor application from a container or RUM engine instance
	Full Control	Enables performing all available operations on a Real User Monitor application, page, and transaction, and granting and removing permissions for those operations
Alerts (under Real User Monitor Engine instance)	Add	Enables adding alerts to a Real User Monitor engine
	Change	Enables editing Real User Monitor alert properties
	View	Enables viewing the properties of a Real User Monitor alert
	Delete	Enables deleting an alert from a Real User Monitor engine
	Full Control	Enables performing all available operations on Real User Monitor alerts, and granting and removing permissions for those operations

Resources	**Operation**	**Description**
SiteScope	Add	Enables adding SiteScopes and SiteScope profiles to Monitor Administration
	Change	Enables modifying SiteScope and SiteScope profile properties and attaching a SiteScope to, or detaching it from, Monitor Administration
	View	Enables viewing SiteScope or SiteScope profile properties
	Delete	Enables deleting a SiteScope profile from Monitor Administration
	Full Control	Enables performing all available operations on SiteScopes and SiteScope profiles, and granting and removing permissions for those operations
Content (under SiteScope instance)	Add	Enables adding a SiteScope group, monitor, report or alert to the SiteScope or to any of its subgroups
	Change	Enables modifying the SiteScope group, monitor, report, or alert and all the objects contained within them
	View	Enables viewing the SiteScope group, monitor, report, or alert and all the objects contained within them
	Delete	Enables deleting a SiteScope group, monitor, or alert and all the objects contained within them
	Full Control	Enables performing all available operations on the SiteScope group, monitor, or alert, and granting and removing permissions for those operations

Resources	Operation	Description
SiteScope Preferences (under SiteScope instance)	Add	Enables adding SiteScope preferences to Monitor Administration
	Change	Enables editing SiteScope preferences
	View	Enables viewing SiteScope preferences
	Delete	Enables deleting SiteScope preferences
	Full Control	Enables performing all available operations on SiteScope preferences, and granting and removing permissions for those operations
Template Containers	Add	Enables adding a container for templates to the Monitor Administration enterprise
	Change	Enables modifying template container properties
	View	Enables viewing template container properties in Monitor Administration
	Delete	Enables deleting a template container from the Monitor Administration enterprise
	Full Control	Enables all available operations on template containers, and granting and removing permissions for those operations
Solution Sets	Change	Enables editing the Solution Set container, and adding, editing, and deleting Solution Set template objects
	Full Control	Enables all operations on Solution Sets, and granting and removing permissions for those operations

Resources	Operation	Description
Views	Add	Enables creating view filters in Monitor Administration
	Change	Enables editing view filter definitions in Monitor Administration
	View	Enables viewing view filter definitions in Monitor Administration
	Delete	Enables deleting view filters from Monitor Administration
	Full Control	Enables performing all available operations on view filters, and granting and removing permissions for those operations
Categories	Add	Enables creating a category in Monitor Administration
	Change	Enables editing Monitor Administration category definitions
	Delete	Enables deleting categories from Monitor Administration
	Full Control	Enables performing all available operations on Monitor Administration categories, and granting and removing permissions for those operations

Resources	**Operation**	**Description**
Containers	Add	Enables adding a container to the Monitor Administration enterprise
	Change	Enables renaming and modifying the properties of a container
	Delete	Enables deleting a container from Monitor Administration
	Full Control	Enables performing all available operations on a Monitor Administration container, and granting and removing permissions for those operations
Solution Sets	Change	Enables editing the Solution Set container, and adding, editing, and deleting Solution Set template objects
	Full Control	Enables all operations on Solution Sets, and granting and removing permissions for those operations
Customer Notification Templates (Mercury Managed Services only)	Add	Enables creating and cloning a customer-specific notification template
	Change	Enables editing the properties of a customer-specific notification template
	View	Enables viewing the properties of a customer-specific notification template
	Delete	Enables deleting a customer-specific notification template
	Full Control	Enables performing all available operations on a customer-specific notification template, and granting and removing permissions for those operations

Resources	Operation	Description
Notification Templates	Add	Enables creating and cloning notification templates
	Change	Enables editing notification template properties
	View	Enables viewing notification template properties
	Delete	Enables deleting a notification template
	Full Control	Enables performing all available operations on notification templates, and granting and removing permissions for those operations

Platform

The Platform context includes all the resources related to administering the platform.

Note: Some of the resources listed are available for Mercury Managed Services customers only and are marked as such.

Resources	Operation	Description
Audit Log	View	Enables viewing the audit log
	Full Control	Enables viewing the audit log, and granting and removing permission to view the audit log

Resources	Operation	Description
Users	Add	Enables adding users to the system
	Change	Enables modifying user details
	View	Enables viewing user details
	Delete	Enables deleting users from the system
	Full Control	Enables performing all available operations on users, and granting and removing permissions for those operations
User Groups	Add	Enables adding user groups to the system
	Change	Enables modifying user group details
	View	Enables viewing user group details
	Delete	Enables deleting user groups
	Full Control	Enables performing all available operations on user groups, and granting and removing permissions for those operations
Data Collectors	Change	Enables performing remote upgrades, remote uninstalls, and settings updates (Client Monitor) on data collectors in Data Collector Maintenance
	View	Enables viewing the data collectors in Data Collector Maintenance
	Delete	Enables removing data collector instances
	Full Control	Enables performing all available operations in Data Collector Maintenance, and granting and removing permissions for those operations

Resources	**Operation**	**Description**
Central Scripts Repository	Full Control	Enables working in the Script Repository, including creating, deleting, and renaming folders; uploading, downloading, checking in, and checking out scripts
Scheduled Reports	Add	Enables creating new scheduled reports
	Change	Enables modifying scheduled reports
	View	Enables viewing scheduled reports
	Delete	Enables deleting scheduled reports
	Full Control	Enables performing all available operations on scheduled reports, and granting and removing permissions for those operations
Recipients	Add	Enables adding recipients to the platform
	Change	Enables editing recipient details
	View	Enables viewing recipients and recipient details
	Delete	Enables deleting recipients from the platform
	Full Control	Enables performing all available operations on recipients, and granting and removing permissions for those operations

Resources	Operation	Description
Custom Data Types	Add	Enables full access permissions to Measurement Filters page
	Change	Enables full access permissions to Measurement Filters page
	View	Enables full access permissions to Measurement Filters page
	Delete	Enables full access permissions to Measurement Filters page
	Full Control	Enables full access permissions to Measurement Filters page, and granting and removing permissions for those permissions
Databases	Add	Enables adding profile databases to the system
	Change	Enables modifying profile database details in database management
	View	Enables viewing profile database management details
	Delete	Enables deleting profile databases from the system
	Full Control	Enables performing all available operations on profile databases in database management, working with the purging manager, and granting and removing permissions for those operations

Resources	**Operation**	**Description**
Script Repository (Mercury Managed Services only)	Add	Enables uploading new scripts to the repository
	Change	Enables modifying scripts in the repository
	View	Enables viewing the script repository
	Remove	Enables deleting a script from the script repository.
	Execute	Enables subscribing to script verification and verifying scripts for private POP only
	Full Control	Enables performing all available operations on scripts in the scripts repository, and granting and removing permissions for those operations
Package Information (Mercury Managed Services only)	Change	Enables modifying package locations, renaming packages, and selecting recipients for package notifications
	View	Enables viewing package information
	Full Control	Enables performing all available operations on package information, and granting and removing permissions for those operations
System Tickets (Mercury Managed Services only)	View	Enables viewing system ticket details
	Execute	Enables registering system notifications
	Full Control	Enables performing all available operations on system tickets, and granting and removing permissions for those tickets

Production Analysis

Use the Production Analysis context to assign permissions to access the Production Analysis reports generating from the Application Performance Lifecycle application. These reports enable users to extract real-user transaction data to be used in Performance Center load tests and to create Virtual User Generator (VuGen) script templates, based on real-user activity.

Resources	Operation	Description
Production Analysis	Full Control	Enables accessing and downloading Production Analysis reports generated by Application Performance Lifecycle

Service Level Management

Use the Service Level Management context to assign permissions to all SLAs or specific instances.

Resources	Operation	Description
SLAs	Add	Enables adding SLAs
	Change	Enables renaming SLAs, adding descriptions to SLAs, viewing SLA configuration in administration pages, and changing SLA configurations
	View	Enables generating and viewing reports and custom reports on SLAs
	Delete	Enables deleting SLAs
	Full Control	Enables performing all available operations on SLAs, and granting and removing permissions for those operations

User Defined Reports

Use the User Defined Reports context to assign permissions to the various types of user-defined reports and related settings.

Resources	Operation	Description
Custom Reports	Change	Enables creating, editing, and deleting custom reports
	View	Enables viewing custom reports
	Full Control	Enables performing all available operations on custom reports, and granting and removing permissions for those operations
Trend Reports	Change	Enables creating, editing, and deleting trend reports
	View	Enables viewing trend reports
	Full Control	Enables performing all available operations on trend reports, and granting and removing permissions for those operations
Custom Links	Change	Enables creating and deleting custom links
	View	Enables viewing custom links
	Full Control	Enables performing all available operations on custom links, and granting and removing permissions for those operations
Excel Reports	Change	Enables adding, deleting, and updating Excel open API reports
	View	Enables viewing Excel open API reports
	Full Control	Enables performing all available operations on Excel open API reports, and granting and removing permissions for those operations

Resources	Operation	Description
Default Header/Footer	Change	Enables modifying the default header and footer for custom and trend reports
	Full Control	Enables modifying, and granting and removing permissions to modify, the default header and footer for custom and trend reports

My BAC

Use the My BAC context to assign permissions to work with the module and portlet definition pages in My BAC Administration.

Resources	Operation	Description
Modules	Full Control	Enables creating, editing, deleting, and performing all operations on the Manage Modules page.
Portlet definitions	Full Control	Enables creating, editing, deleting, and performing all operations on the Manage Portlet Definitions page.

Roles

Mercury Business Availability Center enables you to apply permissions using pre-defined roles for specific users or user groups in your organization. These roles include a pre-configured collection of resources and a set of operations that apply to those resources.

Each role defined appears below with a table, listing by context which resources and which operations have been preconfigured and included in the role.

Roles can be applied only to specific resources:

- Roles that include resources from several contexts can be applied only to the Business Availability Center resource. Business Availability Center appears as the first resource collection in every context.

- Roles whose resources are all within one context can be applied to specific resources within that context.

  Details of the resources on which roles can be applied appear within the description of each role below. Some of the resources are applicable to Mercury Managed Services customers only and are listed as such.

Note to users of previous versions of Mercury Business Availability Center: If you had users and permission levels defined in your previous version, those users and some of the applicable permissions levels have been upgraded to the current version and mapped to the roles in Mercury Business Availability Center. Under each role listed below is a note indicating the corresponding permission level from Topaz 4.5 Feature Pack 2 or earlier.

Superuser

The superuser role can be applied only to the Business Availability Center resource.

This role includes all available operations on all the resources in all the contexts. Only a superuser can apply the superuser role to another user.

This role is mapped from Superuser security level in Topaz version 4.x.

Administrator

The administrator role can be applied only to the Business Availability Center resource.

An administrator has a collection of permissions that enable adding profiles to the system, and managing the resources related to those profiles. Once a profile is added, the administrator has full control privileges on all resources within that profile instance.

This role is mapped from the Administrator security level in Topaz version 4.x.

Context	**Resource**	**Operation**
CMDB	Views	Full Control
Monitors	Client Monitor Profile	Add
	Categories	Add
	Containers	Full Control
	Filters	Add
	Template Containers	Add
	Template	Add
	Diagnostics	Full Control
	Business Process Profile	Add
	Real User Monitor	Add
	SiteScope	Add
	SiteScope Group	Add
	SiteScope Preferences	Add
	Solution Sets	Full Control
Platform	Audit Log	Full Control
	Database	Full Control
	Data Collectors	Change
		View
	Recipients	Full Control
	Scheduled Reports	Full Control
	Users	Full Control
	User Group	Full Control
Service Level Management	SLAs	Full Control

Context	Resource	Operation
User Defined Reports	Custom Links	Full Control
	Custom Reports	Full Control
	Default Header/footer	Full Control
	Excel Reports	Full Control
	Trend Reports	Full Control
My BAC	Manage Modules page	Full Control
	Manage Portlet Definitions page	Full Control

System Modifier

The system modifier role can be applied only to the Business Availability Center resource.

A system modifier can view and change any and all of the resources within Mercury Business Availability Center. There are some resources on which the view or the change operation is not applicable. A system modifier has permissions for only those operations that are available in Mercury Business Availability Center.

A system modifier does not have full control privileges on any resource and, therefore, cannot grant or remove permissions for other users.

Context	Resource	Operation
CMDB	Views	View
		Change

Context	Resource	Operation
Monitors	Alerts (Business Process)	View
		Change
	Alerts - Create Dependency	Change
	Alerts - Log Event	Change
	Alerts - Run Executable File	Change
	Alerts - SNMP	Change
	Alert (Client Monitor)	View
		Change
	Monitors (Client Monitor)	View
		Change
	Client Monitor Profile	View
		Change
	Outlier Value (Client Monitor)	Change
	Transaction (Client Monitor)	View
		Change
	Monitors (Business Process)	View
		Change
	Categories	View
		Change
	Containers	Change

Context	Resource	Operation
Monitors	Filters	View
		Change
	Template Containers	View
		Change
	Template	View
		Change
	Diagnostics	View
		Change
	Business Process Profile	View
		Change
	Real User Monitor Engines	View
		Change
	Alerts (Real User Monitor)	View
		Change
	End User (Real User Monitor)	View
		Change
	Engine Settings (Real User Monitor)	View
		Change
	Pages (Real User Monitor)	View
		Change
	Transactions (Real User Monitor)	View
		Change
	SiteScope	View
		Change
	SiteScope Group	View
		Change

Context	Resource	Operation
Monitors	SiteScope Preferences	View
		Change
	Solution Sets	Change
	Notification Templates	View
		Change
	Outlier Value (Business Process)	Change
	Transactions (Business Process)	View
		Change
Platform	Audit Log	View
	Databases	Change
		View
	Data Collectors	View
		Change
	Recipients	View
		Change
	Sample Type	Change
		View
	Scheduled Reports	Change
		View
	Users	Change
		View
	User Group	Change
		View
Service Level Management	SLAs	Change
		View

Context	Resource	Operation
User Defined Reports	Custom Links	View
		Change
	Custom Reports	View
		Change
	Default Header/footer	Change
	Excel Reports	View
		Change
	Trend Reports	View
		Change

System Viewer

The system viewer role can be applied only to the Business Availability Center resource.

A system viewer can only view resources within Mercury Business Availability Center and has no permissions to change, add, or delete any resources or resource instances. There are some resources on which the view operation is not applicable. A system viewer has no access to those resources.

Context	Resource	Operation
CMDB	Views	View

Context	**Resource**	**Operation**
Monitors	Alerts (Business Process)	View
	Alerts (Client Monitor)	View
	Monitors (Client Monitor)	View
	Client Monitor Profile	View
	Transactions (Client Monitor)	View
	Monitors (Business Process)	View
	Categories	View
	Filters	View
	Template Containers	View
	Templates	View
	Diagnostics	View
	Business Process Profile	View
	Real User Monitor Engines	View
	Alerts (Real User Monitor)	View
	End User (Real User Monitor)	View
	Engine Settings (Real User Monitor)	View
	Pages (Real User Monitor)	View
	Transactions (Real User Monitor)	View
	SiteScope	View
	SiteScope Group	View
	SiteScope Preferences	View
	Notification Templates	View
	Transactions (Business Process)	View

Context	Resource	Operation
Platform	Audit Log	View
	Database	View
	Data Collectors	View
	Recipients	View
	Sample Types	View
	Scheduled Reports	View
	Users	View
	User Group	View
Service Level Management	SLAs	View
User Defined Reports	Custom Links	View
	Custom Reports	View
	Excel Reports	View
	Trend Reports	View

Business Process Profile Administrator

The Business Process profile administrator role can be applied to only the Business Process Profile resource or specific instances of the profile resource.

When granted this role at the resource collection level, the Business Process profile administrator can manage all of the platform's Business Process profiles, including permissions on all the profiles. When granted this role at the instance level, the administrator can manage only those resources associated with the specific Business Process profile instance.

This role is mapped from Administrator security level in Topaz version 4.x. Any administrator who was added as a user on a specific Business Process profile in the previous version is upgraded to the Business Process profile administrator role for that profile. This is in addition to being assigned the administrator role as described above (for details, see "Administrator" on page 360).

Context	Resource	Allowed Operations
Monitors	Business Process Profile	Full Control
	Monitor	Full Control
	Transaction	Full Control
	Alert	Full Control

Business Process Profile User

The Business Process profile user role can be applied to only the Business Process Profile resource or specific instances of the profile resource.

These users have viewing permissions, but can modify transaction threshold settings and transaction descriptions.

This role is mapped from Regular User security level in Topaz version 4.x. Any regular user who was added as a user on a specific Business Process profile in the previous version is upgraded to the Business Process profile user role for that profile.

Context	Resource	Allowed Operations
Monitors	Business Process Profile	View
	Monitor	View
	Transaction	View
		Change
	Alert	View

Client Monitor Profile Administrator

The Client Monitor profile administrator role can be applied to only the Client Monitor Profile resource or specific instances of the profile resource.

When granted this role at the resource collection level, the Client Monitor profile administrator can manage all of the platform's Client Monitor profiles, including permissions on all the profiles. When granted this role at the instance level, the administrator can manage only those resources associated with the specific profile instance.

This role is mapped from Administrator security level in Topaz version 4.x. Any administrator who was added as a user on a specific Client Monitor profile in the previous version is upgraded to the Client Monitor profile administrator role for that profile. This is in addition to being assigned the administrator role as described above (for details, see "Administrator" on page 360).

Context	Resource	Allowed Operation
Monitors	Client Monitor Profile	Full Control
	Monitor	Full Control
	Transactions	Full Control
	Alerts	Full Control

Client Monitor Profile User

The Client Monitor profile user role can be applied to only the Client Monitor Profile resource or specific instances of the profile resource.

These users have only viewing permissions, but can also modify transaction threshold settings and transaction descriptions.

This role is mapped from Regular User security level in Topaz version 4.x. Any regular user who was added as a user on a specific Client Monitor profile in the previous version is upgraded to the Client Monitor profile user role for that profile.

Context	Resource	Allowed Operation
Monitors	Client Monitor Profile	View
	Monitors	View
	Transactions	View
		Change
	Alerts	View

SiteScope Administrator

The SiteScope administrator role can be applied to only the SiteScope resource or specific instances of the resource.

When granted this role at the resource collection level, the SiteScope administrator can manage all of the platform's SiteScopes, including permissions on the SiteScopes. When granted this role at the instance level, the administrator can manage only those resources associated with the specific SiteScope instance.

This role is mapped from Administrator security level in Topaz version 4.x. Any administrator who was added as a user on a specific SiteScope in the previous version is upgraded to the SiteScope administrator role for that SiteScope.

Context	Resource	Allowed Operation
Monitors	SiteScopes	Full Control
	Groups (SiteScope)	Full Control
	SiteScope Preferences	Full Control

Customer Superuser

Note: This role can be applied to Mercury Managed Services customers only.

The customer superuser role can be applied to only a specific instance of the customer resource. The customer resource is available only to Mercury Managed Services customers and represents the customer level in the permissions resource tree. It is available in all contexts and applies to all contexts (like the Business Availability Center resource). The customer superuser is granted full control on all the resources and instances that belong to that customer. These includes all resources, instances of those resources, and child resources under the customer resource.

Context	Resource	Allowed Operation
CMDB	Views	Full Control

Context	Resource	Allowed Operation
Monitors	Alerts	Full Control
	Alert - Create Dependency	Full Control
	Alerts (Client Monitor)	Full Control
	Monitors (Client Monitor)	Full Control
	Client Monitor Profile	Full Control
	Outlier Value (Client Monitor)	Full Control
	Transactions (Client Monitor)	Full Control
	Notification Templates	Full Control
	Diagnostics	Full Control
	Monitors (Business Process)	Full Control
	Categories	Full Control
	Containers	Full Control
	Filters	Full Control
	Template Containers	Full Control
	Template	Full Control
	Business Process Profile	Full Control
	Real User Monitor Engines	Full Control
	Alerts (Real User Monitor)	Full Control
	End User (Real User Monitor)	Full Control
	Engine Settings (Real User Monitor)	Full Control
	Pages (Real User Monitor)	Full Control
	Transactions (Real User Monitor)	Full Control
	SiteScope	Full Control
	Groups (SiteScope)	Full Control
	SiteScope Preferences	Full Control
	Solution Sets	Full Control

Context	Resource	Allowed Operation
Platform	Audit Log	Full Control
	Hosts	Full Control
	Package Information	Full Control
	Recipients	Full Control
	Scheduled Reports	Full Control
	Script Repository	Full Control
	System Tickets	Full Control
	Users	Full Control
	User Groups	Full Control
Service Level Management	SLAs	Full Control
User Defined Reports	Custom Links	Full Control
	Custom Reports	Full Control
	Default Header/Footer	Full Control
	Excel Reports	Full Control
	Trend Reports	Full Control
My BAC	Manage Modules page	Full Control
	Manage Portlet Definitions page	Full Control

Customer Administrator

Note: This role can be applied to Mercury Managed Services customers only.

The customer administrator role can be applied to only a specific instance of the customer resource. The customer resource is available only to Mercury Managed Services customers and represents the customer level in the permissions resource tree. It is available in all contexts and applies to all contexts (like the Business Availability Center resource).

The customer administrator is granted full control on a selection of resources, and view and/or execute on other resources. This user can add profiles of any type, and has full control on the created profile. However, the user is not granted permissions for profiles that were created by other users, even if these profiles are for the same customer. In the case of the My BAC resources, any user with this role can make changes to resources defined by other users.

This role is mapped from Customer Administrator security level in Topaz Managed Services version 4.5.

Context	Resource	Allowed Operation
CMDB	Views	Full Control
Monitors	Alerts	View
	Client Monitor Profile	Add
	Diagnostics	View
		Execute
	Categories	Add
	Containers	Full Control
	Filters	Add
	Template Containers	Add
	Templates	Add
	Business Process Profile	Add
	RUM	Add
	SiteScope	Add
	Groups (SiteScope)	Add
	SiteScope Preferences	Add
	Solution Sets	Full Control

Context	Resource	Allowed Operation
Platform	Audit Log	Full Control
	Package Information	Full Control
	Recipients	Full Control
	Scheduled Reports	Full Control
	Script Repository	Full Control
	System Tickets	Full Control
Service Level Management	SLAs	Full Control
User Defined Reports	Custom Links	Full Control
	Custom Reports	Full Control
	Default Header/Footer	Full Control
	Excel Reports	Full Control
	Trend Reports	Full Control
My BAC	Manage Modules page	Full Control
	Manage Portlet Definitions page	Full Control

Note: Customer administrators whose permissions role was mapped from Topaz version 4.5 or earlier have full control permission for all the above plus the users resource in the platform context. New customer administrators will not have this resource included in their permissions.

Operator

Note: This role can be applied to Mercury Managed Services customers only.

The operator is granted full control on one or both of the resources. Moreover, any user with this role has full control over modules and portlet definitions defined by other users.

Context	Resource	Allowed Operation
My BAC	Manage Modules page	Full Control
	Manage Portlet Definitions page	Full Control

Granting and Removing Permissions

Before granting and/or removing permissions on the resources in Mercury Business Availability Center, you should:

- understand the various contexts and resources available in Mercury Business Availability Center (for details, see "Understanding Permissions Resources" on page 331)
- determine for which users or user groups you will be applying permissions (for details, see "Selecting Users and User Groups" on page 334)
- select whether you will be applying operations or roles to the users and/or user groups (for details, see "Understanding Operations and Roles" on page 335)

Note: For the applied permissions to take effect, the user for whom permission has been granted or removed must log out and log in again to Mercury Business Availability Center.

To apply permissions:

1 In Platform Administration, select **Users and Permissions** > **Permissions Management**. The Permissions Management page opens.

2 Optionally, click **Settings** at the bottom of the left-hand resource tree. The Apply Permissions Settings dialog box opens and you can configure the settings for this session of applying permissions. For details, see the procedure on page 379.

3 Select a context from the context list at the top of the resource tree on the left-hand side of the page. The resource tree displays the resources included in the selected context.

Note: The Business Availability Center resource appears as the top level of every context and can have only roles applied to it.

4 Highlight the resources on which you want to apply permissions. You can press CTRL to make multiple selections in the resource tree.

5 Select a user or user group in the user selection area on the upper right-hand area of the page.

By default, all the users are listed. To filter your selection, click one of the letter links above the list to display only those users beginning with that letter. To revert to the complete list, click **ALL**.

6 Select the **Operations** tab or the **Predefined Roles** tab in the lower right-hand area of the page.

7 If you are applying operations, select from the available operations for the highlighted resources. Depending on the resources highlighted, you can select the **Inherit** check box for the operation to be inherited to all the child resources within the selected resource.

Note: The **Granted from Group/Role/Parent** column displays those permissions that have been granted from either a user group, a predefined role, or a parent resource. You cannot remove any of these permissions individually but you can grant additional permissions. If you want to remove permissions that are granted from a group, role, or parent resource, you must make the change at the group, role, or parent resource level.

If you are applying pre-defined roles, select the applicable role for the highlighted resource.

8. If in step 2 of configuring settings, you chose to apply permissions automatically when selecting another resource, select another resource or click **Apply Permissions**. If not, click **Apply Permissions**. Repeat as necessary for other resources and users.

To configure settings for this session of applying permissions:

1. In Permissions Management, click **Settings** at the bottom of the left-hand resource tree. The Apply Permissions Settings dialog box opens.
2. Select from the following options to change the settings by which Permissions Management functions:
   - **Apply permissions automatically when selecting another resource** – Selecting this option removes the necessity for clicking the **Apply Permissions** button after each operation. If this option is not selected, you must click **Apply Permissions** before going on to the next operation.
   - **Do not display warning message when revoking VIEW from resource** – When the view operation is removed from a resource for a user, that user has no access to the resource or to any of its child resources or instances. Therefore, by default, a warning message appears when removing view permissions. Selecting this option will disable that warning message.

Note: When you select the settings for applying permissions, the options selected apply only to the current Mercury Business Availability Center session.

3 Click **Close** to save your settings and continue applying permissions.

Part VI

Personal Settings

23

Configuring Personal Settings

Personal settings enable customization of the way Mercury Business Availability Center presents information to individual users.

About Configuring Personal Settings

Individual users can configure personal settings to customize specific user-related behavior of Mercury Business Availability Center.

Users can configure the following personal settings:

- Refresh rate of reports – for details, see page 384
- Time zone used when displaying reports – for details, see page 384
- User mode for viewing KPIs in Dashboard – for details, see page 384
- Default page displayed when logging into Mercury Business Availability Center – for details, see page 385
- Default page displayed for each different Mercury Business Availability Center context – for details, see page 385

- Display of menu items – for details, see page 386
- Password used when logging into Mercury Business Availability Center – for details, see page 387

Configuring Refresh Rate, Time Zone, and User Mode

On the General Settings page, you configure refresh rate settings, time zone settings and user mode.

Mercury Business Availability Center saves these settings per defined user. Any changes you make remain in effect for all future Web sessions for only that user.

To configure refresh rate and time zone settings:

1. Select **Admin** > **Personal Settings** > **General Settings** to open the General Settings page.
2. In the Refresh Settings section, select the rate at which you want Mercury Business Availability Center to automatically refresh the browser and load the most up-to-date data from the database. Auto-refresh is only active when in the **Past day** or **Past hour** time resolution.

   Note that, when viewing reports in the **Past day** or **Past hour** time resolution, or in the **day** or **hour** time resolution, for a period within the past 24 hours, the auto-refresh feature also automatically moves the time range of the report forward by the selected refresh period.
3. In the Time Zone Settings section, select the time zone in which you want reports to be displayed. For a reference list of GMT time zones for locations throughout the world, see "GMT Time Zones" in *Reference Information*.

   Note that the time zone automatically takes Daylight Saving Time into account. Therefore, you should select your GMT time zone in Standard Time and not in Daylight Saving Time.
4. In the User Mode section, select the **User Mode**. Mercury Business Availability Center enables you to work with two user modes, operations and business, and different versions of Dashboard KPIs can be defined for each mode. You can see the KPI version appropriate for your user mode. For details, see "KPIs for User Modes" in *Application Administration*.

Select from the following options:

- **Unspecified.** This leaves you without a particular mode. Select this option if:
  - Mercury Business Availability Center is working with user modes and you want to see KPIs for both modes in Dashboard views.
  - Your system is not working with user modes.
- **Operations User**. This enables you to view the operations version of KPIs.
- **Business User.** This enables you to view the business version of KPIs.

5 Click **Apply** to save your settings.

Setting Default Pages

On the Default Page Settings page, you can specify the default context and page that Mercury Business Availability Center opens when a specific user logs in, and specify the default page for each context.

To set default pages:

1 Select **Admin** > **Personal Settings** > **Default Page Settings** to open the Default Page Settings page.

2 From the **User** list, select the user whose settings you want to modify. Only names of users whom the current user has permission to administer appear in the list.

3 From the **Context** list, select a context whose default page you want to set. The **Available menu items** tree updates according to the chosen context.

Note that the context options are based on the customer license.

4 To set the selected context as the context that opens by default when the specified user logs in, select **Set as default context**.

5 In the **Available menu items** tree, select the page that opens by default when the specified user accesses the chosen context.

To instruct Mercury Business Availability Center to open with only a menu heading selected and splash page in the info area, select a root item in the

Available menu items tree. Root items have expand (+) or collapse (-) symbols beside them.

Note that the menu choices reflect the users permissions.

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

Customizing the Menus

On the Menu Customization page, you can customize the menu items that are displayed in different contexts.

To customize menu items:

1 Select **Admin** > **Personal Settings** > **Menu Customization** to open the Menu Customization page.

2 From the **User** list, select the user whose settings you want to modify. Only names of users who the current user has permissions to administer appear in the list.

3 From the **Context** list, select a context whose menu settings you want to customize. The **Available menu items** tree updates according to the chosen context.

Note that the context options are based on the customer license.

4 In the **Available menu items** tree, select the menu items to be displayed when the specified user accesses the chosen context.

Use the buttons at the bottom to select or clear all items.

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

Changing the User Password

Note to Mercury Managed Services customers: This menu item is called Change User Information and includes the option to change information such as user name, e-mail address, and password. Any change made here updates the login parameters for mms.mercury.com.

On the Change User Password page, the current user can change the password used to log into Mercury Business Availability Center.

To change the user password:

1 Select **Admin** > **Personal Settings** > **Change Password** to open the Change User Password page.

2 Type the old password in the **Old password** box.

3 Type a new password in the **New password** box, and retype the password in the **Retype new password** box.

4 Click **OK**.

Part VII

Report Administration

24

Customizing Reports

Mercury Business Availability Center enables you to generate reports automatically or manually and to specify a header and a footer for a report.

About Customizing Reports

Mercury Business Availability Center enables you to customize reports by:

- **generating reports automatically.** For details, see “Configuring Report Generation Settings” on page 392.
- **specifying a header and a footer for reports.** For details, see “Configuring a Report Header and Footer” on page 393.

Note: Mercury Business Availability Center also enables you to customize the look and layout of specific reports (customizable reports). Contact Mercury Customer Support to assist you in performing this type of report customization.

Configuring Report Generation Settings

You can configure Mercury Business Availability Center to generate reports automatically after selecting the report from the menu or only generate reports on demand from within the report.

To configure these settings, users with appropriate administrative privileges should perform the changes described in the procedure below.

Note: You must log in again for the changes to take effect.

To configure report generation settings for reports:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations**.
2. Select **Reporting** to open the Reporting-Display area.
3. Click the **Edit** button next to the **Generate Reports Automatically** setting to open the Generate Reports Automatically dialog box.
4. Set the property value as required:
   - ➤ select **true** to enable automatic report generation
   - ➤ select **false** to disable automatic report generation
5. Click **Save**.

   To remove automatic report generation, set the property back to **false**.

   For more information on the Infrastructure Settings Manager, see “Infrastructure Settings” in *Platform Administration*.

Configuring a Report Header and Footer

You can add a header and a footer to a report. You can also modify an existing header and footer or return to the default header and footer (blank).

The technique used to customize reports is different for different reports. The reports can be split into two different groups:

- **customizable reports**
  - **all Service Level Management reports.** For details, see *Using Service Level Management.*
  - **all Dashboard reports.** For details, see “Working with Dashboard Reports” in *Using Dashboard.*
  - **selected Real User Monitor reports.** The following reports are included: Session Analyzer, Session Details, Page Details, Event Count over Time, Event Summary, and Event Log. For details, see “Real User Monitor Reports” in *Using End User Management.*
  - **all Application Lifecycle reports.** For details, see “Working with Application Performance Lifecycle Reports” in *Using Application Performance Lifecycle.*
- **legacy reports**
  - **End User Management reports.** For details, see *Using End User Management.*
  - **System Availability Management reports.** For details, see *Using System Availability Management.*
  - **selected Real User Monitor reports.** The following reports are included: Global Statistics, Page Summary, Transaction Summary, End User Summary, and Server Summary. For details about these reports, see “Real User Monitor Reports” in *Using End User Management.*

This section includes the following topics:

- “Adding a Header and a Footer to a Legacy Report” on page 394
- “Adding a Header and a Footer to a Customizable Report” on page 394

Adding a Header and a Footer to a Legacy Report

To add a header and a footer to a legacy report, create a custom report using the Custom Report Manager, specify a header and a footer for the custom report, and include the legacy report in the custom report. For details, see "Defining a Header and Footer for a Custom Report" in *Working with Applications*.

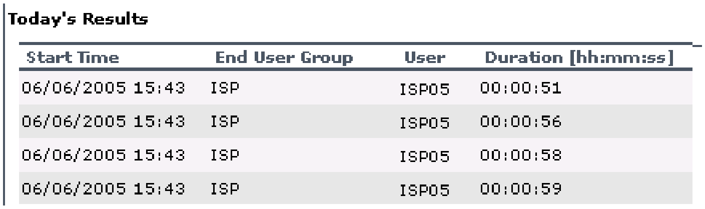
Adding a Header and a Footer to a Customizable Report

To add a header and a footer to a customizable report specify the header and/or footer in the Report Header/Footer setting as explained below.

A customizable report header/footer has the following characteristics:

- The text of the header/footer has to be valid HTML.
- The changes take effect immediately.
- The change is applied to all the customizable reports.
- The header/footer is static. It remains displayed on the page while you scroll the report lines.
- If you added a report header/footer to a customizable report using the Report Header/Footer setting, and you include the customizable report in a custom report built using the Custom Report Manager, then the custom report header/footer overrides the customizable report header/footer.

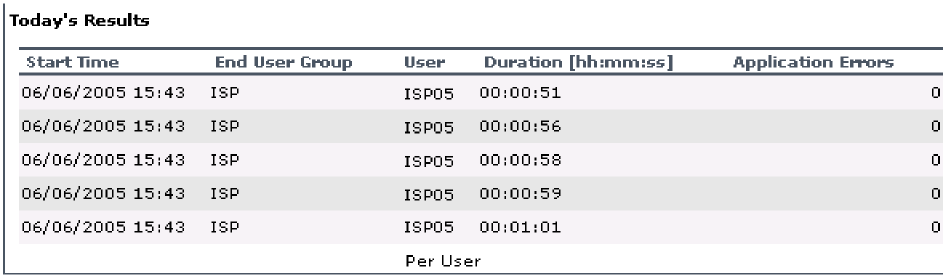
For example, if you specify the header <b>Today's Results</b>, the header appears with a bold font.



Today's Results

Start Time	End User Group	User	Duration [hh:mm:ss]
06/06/2005 15:43	ISP	ISP05	00:00:51
06/06/2005 15:43	ISP	ISP05	00:00:56
06/06/2005 15:43	ISP	ISP05	00:00:58
06/06/2005 15:43	ISP	ISP05	00:00:59

As another example, if you specify the footer <center>Per User</center> the report shows the footer aligned to the center of the report.



Today's Results

Start Time	End User Group	User	Duration [hh:mm:ss]	Application Errors
06/06/2005 15:43	ISP	ISP05	00:00:51	0
06/06/2005 15:43	ISP	ISP05	00:00:56	0
06/06/2005 15:43	ISP	ISP05	00:00:58	0
06/06/2005 15:43	ISP	ISP05	00:00:59	0
06/06/2005 15:43	ISP	ISP05	00:01:01	0

Per User

To add a header and a footer to a new report:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations**.
2. Select **Reporting** to open the Reporting - Display area.
3. To specify a header:
   a. Click the **Edit** button next to the **Display static report header** setting to open the Display static report header dialog box.
   b. In the **Value** box, enter the text of the header.
   c. Click **Save** to save the changes.
4. To specify a footer:
   a. Click the **Edit** button next to the **Display static report footer** setting to open the Display static report footer dialog box.
   b. In the **Value** box, enter the text of the footer.
   c. Click **Save** to save the changes.

25

Reports Log

Mercury Business Availability Center logs all activities related to reports as well as errors that occur when generating reports. Such activities include: creating a new report, generating a report, modifying report filter(s), drilling down in reports, and so forth.

Overview of Reports Log

Mercury Business Availability Center records all activities related to specific reports in a reports log. The activities that are logged are:

- any error related to a report – for details, see “Logging Errors” on page 400
- any other activity performed on the report – for details, see “Logging Activities” on page 400

Each error and activity is recorded using a specific format – for details about the reports log format, see “Reports Log Structure” on page 401.

This section includes the following topics:

Customizable Reports

The reports log records activities for:

- **all Service Level Management reports.** For details, see *Using Service Level Management*.
- **all Dashboard reports.** For details, see "Working with Dashboard Reports" in *Using Dashboard*.
- **selected Real User Monitor reports.** The following reports are included: Session Analyzer, Session Details, Page Details, Event Count over Time, Event Summary, and Event Log. For details, see "Real User Monitor Reports" in *Using End User Management*.
- **all Application Lifecycle reports.** For details, see "Working with Application Performance Lifecycle Reports" in *Using Application Performance Lifecycle*.

Reports Log Location

The reports log is located at **MercuryAM\log\EJBContainer\reports.log.**

Setting the Reports Log Level

Depending on the log level you specify, the following information can be recorded in the reports log:

- debugging information
- activities performed on reports
- warning messages
- error messages
- fatal errors

The log levels have the following hierarchy: **DEBUG**, **INFO**, **WARN**, **ERROR**, and **FATAL**, where **DEBUG** represents the lowest level and **FATAL** the highest level. The default level is **ERROR**.

The log level hierarchy means that if you select one of the levels, the report includes all the information related to that level and the levels above it, as follows:

Level	Reports log
DEBUG	Includes debugging information, activities performed on reports, warning messages, error messages, and fatal errors.
INFO	Includes activities performed on reports, warning messages, error messages, and fatal errors.
WARN	Includes warning messages, error messages, and fatal errors.
ERROR	Includes error messages, and fatal errors.
FATAL	Includes fatal errors.

To set the Reports Log level:

1. Open the **\MercuryAM\conf\core\Tools\log4j\EJB\topaz.properties** file with a text editor.
2. Search for the following line:
   log4j.category.com.mercury.am.bac.core.reports= ${<loglevel>}, reports.appender
3. Change **<loglevel>** to **DEBUG, INFO, WARN, ERROR**, or **FATAL**.
4. Save the file.

Logging Errors

Logging occurs for any error during:

- report initialization
- report customization – for more information, see “Customizing Reports” on page 391
- rendering (creating the report display)

For details about the reports log structure, see “Reports Log Structure” on page 401.

Logging Activities

Logging occurs for any action related to reports. The actions that are logged are:

- creating a new report
- generating a report
- updating the filter of a report that is included in a custom report
- drilling down in a report and between reports
- updating the filter of a report
- printing a generated report, exporting it using e-mail, or opening it in Microsoft Excel file format or in PDF format – for more information about these activities, see “Sharing and Storing Reports” in *Working with Applications*

Reports Log Structure

The reports log includes entries for each activity or error. Each entry has the following structure:

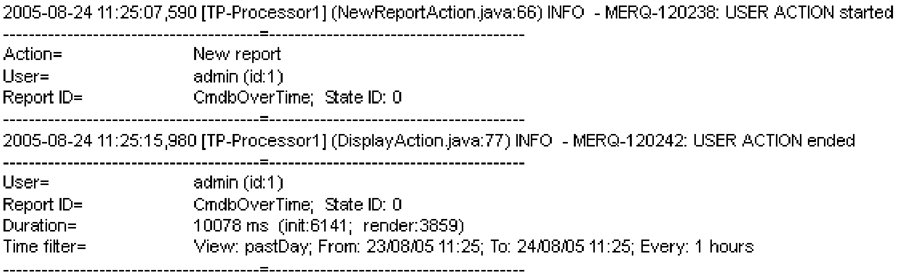
```
2005-08-24 11:25:07,590 [TP-Processor1] (NewReportAction.java:66)
<loglevel> - MERQ-120238: USER ACTION started
--------------------------------------=---------------------------------------
Action=                    <action>
User=                      <user> (id:<id>)
Report ID=                 <report_id>;  State ID: <state_id>
--------------------------------------=---------------------------------------
2005-08-24 11:25:15,980 [TP-Processor1] (DisplayAction.java:77)
<loglevel> - MERQ-120242: USER ACTION ended
--------------------------------------=---------------------------------------
User=                      <user> (id:<id>)
Report ID=                 <report_id>;  State ID: <state_id>
Duration=                  <duration> ms  (init:6141;  render:3859)
Time filter=               View: <view>; From:<from_day_time>; To:
<to_day_time>; Every: <periodicity>
--------------------------------------=---------------------------------------
```

where:

- <**log_level**> represents the level that you selected – for more details about the log level, see “Setting the Reports Log Level” on page 398.
- <**action**> is the type of activity that has been logged:
  - **New report.** The user created a new report from a menu.
  - **Generate.** The user clicked the **Generate** button.
  - **CustomSaveFilter.** The user clicked **OK** in the filter of new reports when creating a custom report.
  - **Update filter.** The user modified the filter in one of the reports.
  - **Navigate.** The user drilled down in a report or between reports.
  - **Export.** The user exported a report to Excel, .PDF, .CSV, or e-mail formats.
- <**user**> is the login name.

- <**id**> is for internal use.
- <**report_id**> is the report requested by the user action.
- <**state_id**> is for internal use.
- <**duration**> is the number of milliseconds the server took to perform the user action.
- The time filter that was used in the activity includes the following information:
  - <**view**> indicates the filter that was selected. This information is for internal use.
  - <**from_day_time**> indicates when the activity started. This information is for internal use.
  - <**to_day_time**> indicates when the activity ended.
  - <**periodicity**> indicates the sampling periodicity. This information is for internal use.

For example, the following entry specifies that a new report CMDBOverTime has been created by the admin user:



```
2005-08-24 11:25:07,590 [TP-Processor1] (NewReportAction.java:66) INFO  - MERQ-120238: USER ACTION started
----------------------------------------=----------------------------------------
Action=                    New report
User=                      admin (id:1)
Report ID=                 CmdbOverTime;  State ID: 0
----------------------------------------=----------------------------------------
2005-08-24 11:25:15,980 [TP-Processor1] (DisplayAction.java:77) INFO  - MERQ-120242: USER ACTION ended
----------------------------------------=----------------------------------------
User=                      admin (id:1)
Report ID=                 CmdbOverTime;  State ID: 0
Duration=                  10078 ms  (init:6141;  render:3859)
Time filter=               View: pastDay; From: 23/08/05 11:25; To: 24/08/05 11:25; Every: 1 hours
----------------------------------------=----------------------------------------
```

Part VIII

Authentication

26

Authentication Strategies

This chapter explains how to set up authentication strategies, such as LDAP, for Mercury Business Availability Center.

Note to Mercury Managed Services customers: This chapter is not relevant to Mercury Managed Services customers, who log in via my.mercury.com.

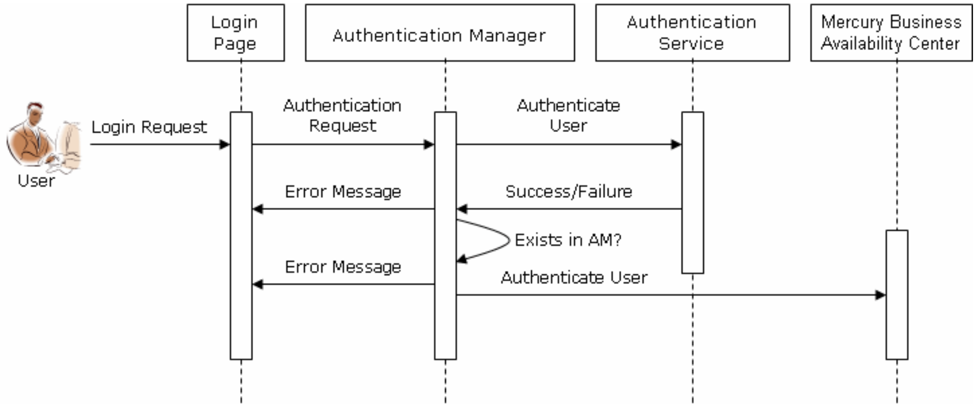
Authentication for Mercury Business Availability Center

Mercury Business Availability Center authentication is based on a concept of "authentication strategies." Each strategy handles authentication against an authentication service such as the internal Mercury Business Availability Center service, Lightweight Directory Access Protocol (LDAP), Single sign-on (SSO), or any other option enabled on the specific Mercury Business Availability Center installation.

When a login request is initiated, a strategy is invoked by a request for authentication using a specific context appropriate for that strategy.

Mercury Business Availability Center Login Workflow

This section describes a typical authentication flow in Mercury Business Availability Center:



- ➤ A user accesses the Mercury Business Availability Center login page. The login page is returned to the Web browser and includes a hidden key that specifies which authentication strategy to follow.
- ➤ The user enters a principal (in this case, user name) and credentials (in this case, password) and submits the login request (in this case, clicks **Log In**).
- ➤ The request is transferred to the Mercury Business Availability Center Authentication Manager together with the strategy name, principal, and credentials.

- The Authentication Manager reads the strategy name and dispatches the request to the relevant authentication strategy to validate the user.
- The relevant authentication strategy accepts the request and tries to authenticate the user against the authentication service in question.
- If authentication is approved, Mercury Business Availability Center verifies whether the user is defined in Mercury Business Availability Center.

Note: When creating users in Mercury Business Availability Center, make sure that user names match the user names in the relevant strategy database. A user can not login to Mercury Business Availability Center if the name does not match.

- If the user passes the previous steps, they are considered an authenticated user. The Mercury Business Availability Center Site Map page is displayed in the Web browser (or whichever page has been defined as the default page).

  If any of the steps fail, the user is notified (a page and error message are sent back to the Web browser). The page and error message depend on which strategy you are implementing.

Setting Up an Authentication Strategy

The default authentication strategy is the internal Mercury Business Availability Center service. If you use the default, you do not have to make any changes to the system.

If you want to use LDAP or SSO authentication strategy, you must configure the appropriate authentication strategy:

- To define an LDAP authentication strategy, see the next section.
- To define an SSO authentication strategy, see “Defining a Single Sign-on Authentication Strategy”.

Note: For the procedure for defining other authentication strategies, contact Mercury Customer Support.

Defining an LDAP Authentication Strategy

You can define an LDAP authentication strategy for a Mercury Business Availability Center system.

This section contains the following topics:

Setting the LDAP Authentication Strategy

This section explains how to set an LDAP authentication strategy in Mercury Business Availability Center.

To set the LDAP authentication strategy:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**. Select the **Foundations** context and choose **LDAP Authentication** from the list.

2 In the **LDAP Authentication - LDAP Server Settings** table, access the LDAP Server URL dialog box by clicking the **Edit** button.

3 Enter the LDAP URL value, using the format ldap://<ldapHost>[:<port>]/[<baseDN>][??scope]

For example, ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub)

4 Click **Save** to save the new value, **Default** to replace the entry with the default value (a blank URL), or **Cancel** to close the dialog box without changing the value.

5 The default protocol used to communicate with the LDAP server is TCP, but you can change the protocol to SSL. For details, see the next section.

6 By default, Mercury Business Availability Center does not resolve user IDs. You can, however, change this setting. For details, see “Resolving a Distinguished Name (DN) from a User ID” on page 410.

The next stage in setting the LDAP authentication strategy is to enable the strategy in Mercury Business Availability Center. For details, see “Enabling an LDAP Authentication Strategy” on page 411.

Setting a Secure Connection with the SSL (Secure Sockets Layer) Protocol

Since the login process involves the passing of confidential information between Mercury Business Availability Center and the LDAP server, you can apply a certain level of security to the content. You do this by enabling SSL communication on the LDAP server and configuring Mercury Business Availability Center to work using SSL.

Mercury Business Availability Center supports SSL that uses a certificate issued by a trusted Certification Authority (CA). This CA is included with the Java runtime environment.

Most LDAP servers, including Active Directory, can expose a secure port for an SSL based connection. If you are using Active Directory with a private CA, you may need to add your CA to the trusted CAs in Java.

For details of configuring the Mercury Business Availability Center platform to support communication using SSL, see “Using SSL in Mercury Business Availability Center” in *Hardening the Platform*.

To add a CA to trusted CAs to expose a secure port for an SSL based connection:

1 Export a certificate from your CA and import it into the JVM that is used by Mercury Business Availability Center.

2 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**. Select the **Foundations** context and choose **LDAP Authentication** from the list.

3 In the **LDAP Authentication - LDAP Server Settings** table, access the Security Protocol dialog box by clicking the **Edit** button.

4 Change the value to **ssl**.

5 Click **Save** to save the new value, **Default** to replace the entry with the default value (internal Mercury Business Availability Center service), or **Cancel** to close the dialog box without changing the value.

Resolving a Distinguished Name (DN) from a User ID

In most Directory Services, a user must log in with a complete distinguished name to be authenticated. This DN is usually a very long string such as: cn=John Smith, cn=Users, ou=Sales, dc=USA, dc=MyCompany, dc=COM. Typing this long string is both annoying and error prone. It is very common, therefore, for applications that integrate with a Directory Service to translate the user's unique ID (for example, the login name) into a complete DN before trying to bind it to the authentication strategy. Mercury Business Availability Center supports this feature.

You can enable Mercury Business Availability Center to search the LDAP server with a named or anonymous user.

The user ID is resolved as follows:

- Mercury Business Availability Center takes the user's unique ID (the user name).
- Mercury Business Availability Center performs a search in the Directory for the user by looking for either uid or sAMAccountName (the LDAP and Active Directory attribute names that hold the user's unique ID, respectively).
- If the search retrieves one (and only one) result, the user's DN is taken from the result and used instead of the login name in the bind operation. If the search retrieves zero or more than one result, the login fails.

To enable Mercury Business Availability Center to resolve user IDs:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**. Select the **Foundations** context and choose **LDAP Authentication** from the list.
2. In the **LDAP Authentication - LDAP UID Search** table, access the Distinguished Name (DN) Resolution dialog box by clicking the **Edit** button.
3. Change the value to **true**.
4. Click **Save** to save the new value, **Default** to replace the entry with the default value (the default is **false**), or **Cancel** to close the dialog box without changing the value.

5 Enter the DN of a user entitled to perform searches in the LDAP database: Access the Distinguished Name of Search-Entitled User dialog box by clicking the **Edit** button. Enter the DN in the Value field.

To enable anonymous login to the LDAP server, leave this field blank. Note, however, that the anonymous user must have permissions to search the LDAP database.

6 Click **Save** to save the new value, **Default** to replace the entry with the default value (the default is **false**), or **Cancel** to close the dialog box without changing the value.

7 Enter the password of a user entitled to perform searches in the LDAP database. Access the Password of Search-Entitled User dialog box by clicking the **Edit** button. Enter the password in the Value field.

If you defined an anonymous user (in step 5), leave this field blank.

8 Click **Save** to save the new value, **Default** to replace the entry with the default value (the default is **false**), or **Cancel** to close the dialog box without changing the value.

Enabling an LDAP Authentication Strategy

This section explains how to enable an LDAP authentication strategy in Mercury Business Availability Center.

To enable an LDAP authentication strategy:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**. Select the **Foundations** context and choose **Business Availability Center Interface** from the list.

2 In the **Business Availability Center Interface – Authentication** table, access the Login Authentication Method dialog box by clicking the **Edit** button.

3 Enter the appropriate strategy name in the Value field. Note that this field is case sensitive. Enter **LDAP**.

4 Click **Save** to save the new value, **Default** to replace the entry with the default value (the default is **false**), or **Cancel** to close the dialog box without changing the value.

Defining a Single Sign-on Authentication Strategy

This section contains the following topics:

About Single Sign-On Authentication Support

HTTP Single Sign-On Authentication provides support for single sign-on over HTTP. Single sign-on (SSO) requires a central login server for a group of applications.

The SSO authentication server authenticates users, and applications inside the group trust the authentication. You do not need further authentication when moving from one application to another.

All requests to client applications are channeled through the SSO authentication server. The internal applications only need to know the name of the authenticated user. That name is passed by the SSO authentication server as the value of an HTTP request header.

The following section explains the procedure for installing SSO authentication support in Mercury Business Availability Center.

Note: SSO support is available from Mercury Business Availability Center 6.1 Service Pack 1.

Implementing Single Sign-On Authentication Support

To implement SSO authentication support, perform the following steps:

1 Stop Mercury Business Availability Center Centers Server and Core Server.

2 Add a new key **HttpSSOAuthenticationLoginHandler.headerName** to the **SYSTEM** table in the management database. The value of the key must be the HTTP header name that the SSO server sends to Mercury Business Availability Center.

```
SQL> INSERT INTO System VALUES
('HttpSSOAuthenticationLoginHandler.headerName','HTTP_header_name');
```

3 In <**Mercury Business Availability Center root directory**>**conf****security.xml**, the following code should be present right after the <authentication> tag:

```
<strategy domain="UserNameOnly"
class="com.mercury.security.authentication.UserNameOnly.UserNameOnlyAuth
enticationStrategy" ></strategy>
```

Add the above code if it is not present.

4 Change the default Mercury Business Availability Center URL to **http://<Mercury Business Availability Center server>/topaz/HttpSSOlogin.jsp**. This can be done in one of two ways:

➤ Redirect requests from the SSO login page to **http://<Mercury Business Availability Center server>/topaz/HttpSSOlogin.jsp**.

➤ In <**Mercury Business Availability Center root directory**>**AppServer****webapps****site.war****index.html**, change **src** to **/topaz/HttpSSOlogin.jsp**.

5 (Optional) By default, logging out of Mercury Business Availability Center returns you to the main login page. You can change the logout page to a different URL by adding a new key **LOGOUT_URL** to the **SYSTEM** table:

```
SQL> INSERT INTO System VALUES ('LOGOUT_URL', 'your_logout_url');
```

6 Restart Mercury Business Availability Center Centers Server and Core Server.

Index