OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

End User Management Data Collector Configuration

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

End User Management Data Collector Configuration

Version 6.2

Document Release Date: June 20, 2006

MERCURY™

Mercury Business Availability Center, Version 6.2
End User Management Data Collector Configuration

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_EUMDCC6.2/01

Table of Contents

Welcome to End User Management Data Collector Configuration

This guide provides instructions on how to create Business Process and Client Monitor profiles and configure the Real User Monitor in Monitor Administration.

How This Guide Is Organized

The guide contains the following chapters:

Chapter 1 Creating Business Process Profiles

Describes how to use the Business Process Profile wizard to create profiles and monitors to collect performance and available data for virtual users.

Chapter 2 Managing Business Process Profiles and Creating Client Monitor Profiles

Describes how to create Business Process profiles that emulate end users performing typical business processes in your applications and create Client Monitor profiles to enable Client Monitor to collect data in Monitor Administration.

Chapter 3 Configuring the Real User Monitor

Describes how to configure the Real User Monitor in Monitor Administration in order to begin the monitoring process after you install a Mercury Real User Monitor engine and probes. This involves adding the Real User Monitor engine to the enterprise tree, adding one or more probes to the engine, defining server names and host aliases, configuring the POST parameters to be monitored, and configuring the Real User Monitor to report specific page, transaction, and end-user data.

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 data collector administrators

Readers of this guide should be knowledgeable about enterprise system administration, infrastructure monitoring systems, and Mercury Business Availability Center data collectors (Business Process Monitor, Client Monitor, Real User Monitor), and have familiarity with the systems being set up for monitoring.

Getting More Information

For information on using and updating the Mercury Business Availability Center 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*.

1

Creating Business Process Profiles

The Business Process Monitor collects data by running Business Process profiles. You create Business Process profiles in Monitor Administration using a wizard to create the profile, add monitors, and configure settings.

About Creating Business Process Profiles and Monitors

The Business Process Monitor collects availability and performance data from various points throughout the infrastructure, as well as from external locations, as defined in the Business Process profiles created using Monitor Administration. The profiles run transactions which perform the business processes you want to monitor and WebTrace monitors to collect server/network performance data.

Before creating profiles for the Business Process Monitor to run, it is important to establish a monitoring strategy for the organization. This includes following some basic profile planning guidelines as well as setting up your data collectors and platform. For details, see "Planning Profiles" on page 2.

Once you have planned out your profiles, you begin the process of creating the profiles and their monitors in Monitor Administration. You create profiles and monitors, and configure their settings using the Business Process Profile wizard. For details, see "Using the Business Process Profile Wizard" on page 4.

Planning Profiles

You should consider how to most effectively manage application performance before creating and running profiles. The information described below can assist you with effective profile planning.

Establish a Baseline

Measuring your baseline is essential for knowing the normal performance of your application. For example, your company may have a service level agreement to deliver transactions in eight seconds or less, 99% of the time. Having a baseline helps you know how your site typically performs and determine whether a performance problem is an isolated incident or a sign of a significant downward performance trend. One way to collect baseline data is to create an initial set of profiles that obtain data continuously over a predefined time period.

Monitor Essential Transactions

The Business Process Monitor emulates real user actions using specific URLs or pre-recorded transactions that perform typical business processes in your application. Consider the following when determining the type of transactions to use:

- Establish the main applications or lines of business whose performance you want to monitor.
- Determine the business functions whose failure could cause harm to your company, for example, transactions that have significant impact on the business (such as purchases), heavy throughput transactions (such as home page download), or transactions integrated with legacy systems, since these integrations increase the risk for application failures.
- Identify transactions that hit the different components within your application infrastructure (servers and physical devices), for example, transactions high in database I/O (such as search requests), since those tend to stress the system.
- Monitor transactions that affect typical end-user experience, for example, links that users commonly follow or transactions associated with new promotions.
- Select transactions that enable you to verify and reinforce service level agreements, for example, mission-critical transactions that typically exhibit heavy throughput, high impact on the system and high database I/O, or transactions describing increased user actions (such as clicking on many links or visiting many parts of your site).

  Record transactions that interact with specific parts of your network infrastructure. For example, define a transaction that exercises just the Web server, another that interacts with the Web server and application server, and a third that interacts with the Web server, application server, and database server.

Monitor from Different Locations

To obtain an accurate assessment of end-user experience, you should monitor from a variety of locations. If possible, select locations where customers are located. Monitoring from a variety of locations also enables you to better track and compare network performance from different Internet backbone locations and service providers.

Before You Begin

Before you begin profile creation, make sure you:

- Start the Business Process Monitor on the host machines designated to run Business Process profiles – for details, see "Working with Business Process Monitor" in *Business Process Monitor Administration*.
- Record scripts which are added to create transaction monitors for Business Process profiles – for details, see "Developing Vuser Scripts" in *Using Mercury Virtual User Generator* and "QuickTest Professional Recording Tips" in *Script Recording Tips*.
- Add the recorded scripts to the Script Repository either while saving in your scripting tool or using Platform Administration – for details, see "Script Repository" in *Platform Administration*.
- Configure required administration settings, including database connections and permissions – for details, see "Database Administration" and "Configuring User Permissions" in *Platform Administration*.

Using the Business Process Profile Wizard

Monitor Administration presents monitor objects in the monitor tree in hierarchy form and uses containers to organize configuration data for profiles and monitors. A Business Process profile can be added directly to the enterprise node or into a container. For details, see "Understanding Monitor Tree Objects" and "Managing Containers in the Monitor Tree" in *Working with Monitor Administration*.

Business Process profiles and transactions monitors can be added to the monitor tree only by running the Business Profile wizard. Once these monitor objects are added to the monitor tree, you can edit their properties using the right-click menu in the menu tree or the Contents tab. For details, see "Navigating and Performing Actions in the Contents Tab and the Monitor Tree" in *Working with Monitor Administration*.

You use the Business Process Profile wizard to:

- create Business Process profiles
- add transaction monitors to profiles

You can perform the following actions either during profile creation using the wizard or after profile creation by editing properties in Monitor Administration:

- set transaction thresholds
- add WebTrace monitors to profiles
- select data collectors to run the monitors
- configure data collector settings (group name, schedule, advanced settings)

Once a profile is created or transactions are added to a profile, you can modify them using the monitor tree, Contents tab and Properties tab in Monitor Administration. For details, see "Managing Business Process Profiles and Creating Client Monitor Profiles" on page 29.

Launching the Business Process Profile Wizard

You launch the Business Process profile wizard when you create Business Process profiles and add transaction monitors to profiles. You can perform these actions only by using the Business Process Profile wizard.

Launching the Wizard to Create Business Process Profiles

You can create an empty profile and at a later stage add transaction or WebTrace monitors to it.

To begin creating Business Process profiles:

Access Monitor Administration by selecting **Monitors** in the Admin menu. Select from the following options:

- In the monitor tree, right-click the enterprise node or container into which you want to add a new Business Process profile and choose **New Business Process Profile** in the container's menu.
- In the Contents tab, highlight the container into which you want to add the profile and click the **New Business Process Profile** button at the top of the page.

The Business Process Profile Wizard opens to the Define Profile Properties page.

Launching the Wizard to Add Monitors to Profiles

When you add transaction monitors to an existing profile, you do so using the Business Profile Wizard.

To add transaction or WebTrace monitors to an existing profile:

Access Monitor Administration by selecting **Monitors** in the Admin menu. Select from the following options:

- In the monitor tree, right-click the Business Process profile to which you want to add a new transaction monitor and choose **New Transaction Monitor** in the profile's menu.
- In the Contents tab highlight the appropriate profile in the monitor tree, and click **New Transaction Monitor**.

The Add Transaction Monitor page of the wizard opens.

Defining Profile Properties

The first page that opens in the Business Process Profile wizard is the Define Profile Properties page. To create a profile and to continue in the wizard, you must enter the mandatory information required in this page. Mandatory fields are marked with a red asterisk.

To create a Business Process profile:

1 Enter the following fields:

- **Profile name.** Enter a descriptive name that will assist in identifying the profile in the monitor tree, in the Dashboard, and in reports.
- **Profile description.** The profile description appears in reports as the tooltip for the profile name. For details on entering meaningful descriptions, see "Adding Descriptions for Reports" on page 55.

2 Select a **Profile database** for storing this profile's information. The list includes all the profile databases defined for this Mercury Business Availability Center installation.

If you want to create a new profile database, click the **Database Management** link which will take you to the page in Platform Administration where you can create a new profile database.

For details on creating a profile database, see "Database Management" in *Platform Administration*.

Note to Mercury Managed Services customers: In this step, you must select a **Package Name**, rather than a profile database. If no package exists, a message appears at the top of the page with a link to the Customer Policy dialog box where you can create a package. If a package exists and you want to modify it or create a new one, you can use the **Customer Policy** link below the package field to open the Customer Policy dialog box. For details, see "Package Information" in *Platform Administration*.

---

3 Select a **GMT offset**—the time zone, in relation to GMT, that Mercury Business Availability Center uses when aggregating data collected by this profile.

For example, if you want Mercury Business Availability Center to aggregate data collected by the profile based on Pacific Time, enter -8, since Pacific Time is GMT-8 hours. For a reference list of GMT time zones for locations throughout the world, see "GMT Time Zones" in *Reference Information*.

4 Optionally, click the **Downtime/Event Scheduling** link to access the Downtime/Event Schedule page in Platform Administration. You can define downtime or event schedules for when Mercury Business Availability Center is automatically instructed not to run the profiles.

You do this to exclude periods of time in which downtime or other events may skew the results of collecting data for reports and Dashboard status. You can assign multiple profiles to one downtime/event schedule. For details, see "Defining Downtime and Other Influencing Events" in *Platform Administration*.

5 Optionally, click **Add CIs** to attach a CI to this profile. You can create these relationships between profiles and any existing, logical CI in the CMDB. This relationship enables the monitor or profile to pass KPI status to the CI to which it is attached.

For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

6 Click **Next** to continue.

At this stage, you can also click **Finish** to create an empty profile.

The next stage of the wizard is to add transaction monitors to the profile you just created. Continue to "Adding Transaction Monitors" on page 9, in the next section.

Adding Transaction Monitors

Once you have added a profile, the next stage in creating the profile's content is to select, and configure properties for, the transaction monitors that you want your data collectors to run. The transaction monitors are the scripts that contain the transactions.

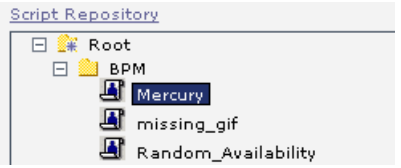
You record scripts using one of the Mercury Business Availability Center recording tools. For details on recording scripts for Business Process profiles, see "Developing Vuser Scripts" in *Using Mercury Virtual User Generator*. Before adding scripts to transaction monitors, you must upload the script to the Script Repository. For details, see "Script Repository" in *Platform Administration*.

When you add a transaction monitor to an existing profile by highlighting a profile in the monitor tree and clicking the **New Transaction Monitor** button, you open the Add Transaction Monitor page of the wizard and add the monitor using the wizard and the procedure below.

The process for selecting a script differs for Mercury Managed Services customers. For details, see the procedure on page 12.

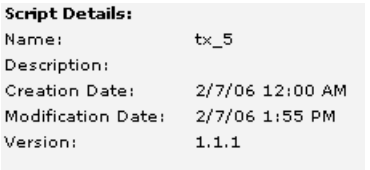
To add a transaction monitor to a profile:

1 Expand the top-level folder of the Script Repository, appearing in the center-left pane. This top level is called **Root** by default.



2 Expand each sub-folder until the script that you want to add to the transaction monitor is displayed. In the example, the script named Mercury contained in the BPM sub-folder has been selected.

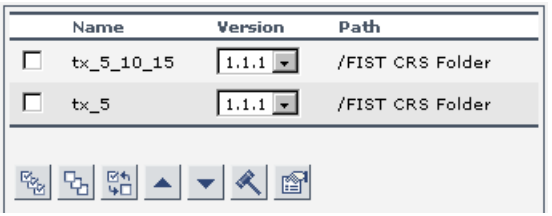
3 When a script is selected, its details are displayed below the Script Repository tree in the pane. You can see the script's name, description, creation date (date the script was first checked into the Script Repository), modification date (date the script was last checked into the Script Repository), and latest version number.



Note: You can also use the **Script Repository** link to access the Script Repository where you can create folders, add scripts, control script versions, and view script and version properties. For details, see "Script Repository" in *Platform Administration*.

---

4 Move the selected script to the right pane using the right-facing arrow. You can select multiple scripts using the CTRL key. The right pane lists all scripts selected for this monitor in the order that the profile will run the scripts.



5 In the right pane, specify the version number of the script that you want your profile to run. The latest version that was most recently checked into the Script Repository is the version selected by default.

6 Optionally, set the order that the profile runs the scripts using the arrow buttons.

a Select the check box next to the script whose position you want to change.

b Click one of the arrows to either move the script lower or higher in the list of scripts.

7 Optionally, set the transaction breakdown settings.

a Select the check box next to the script whose breakdown settings you want to modify.

b Click the Edit Breakdown Settings button. The Edit Breakdown Settings dialog box opens.

c Select **Enable breakdowns** to generate transaction breakdown data when running the selected monitor.

- If you have enabled breakdowns, select **Report additional error information** to include date, time, location, and error messages for failed transactions.
- If you have enabled breakdowns, select **Perform component breakdown** to save complete page component breakdown data for a sampling of transaction instances. By default, Mercury Business Availability Center saves page component breakdown data to the database once per every four transaction instances.

d Select **Enable Diagnostics breakdown** to view the performance status of transactions that are monitored by Diagnostics. This data is available in Diagnostics reports only if you have a valid Mercury Diagnostics license. For details, refer to *Mercury Diagnostics Installation and User's Guide*.

e Select **Enable Siebel breakdown** to see Siebel Application Response Measurement (SARM) data in Business Availability Center for Siebel.

For more details on these options, see "Enable/Disable Transaction Breakdown for the Transaction Monitor" on page 51.

f Click **OK** to save your breakdown settings and return to the wizard.

8 Optionally, add a description or attach CIs to the transaction monitors.

a Select the check box next to the script to which you want to add a description or attach an existing CI.

b Click the **Properties** button. The Script Properties dialog box opens.

- To add a description for the transaction monitor, enter text in the **Description** field.
- To attach an existing CI, click **Add CIs** to open the Select Related CIs dialog box. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

c Click **OK** to save your changes and close the Script Properties dialog box.

9 Click **Next** to continue.

The next stage of the wizard is to set transaction thresholds for the transactions in the scripts just added to the profile you created. Continue to "Setting Transaction Thresholds" on page 14, in the next section.

To add a transaction monitor to a profile for Mercury Managed Services customers:

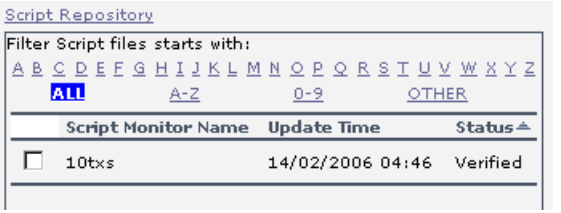
1 Select a script in the center-left pane listing the existing scripts in the Mercury Managed Services Script Repository. The list of scripts includes the script name, the last update time, and the verification status of the script.

Note: If there are no scripts in the Mercury Managed Services Script Repository, a message appears with a link to access the repository.

---

2 Optionally, click the **Script Repository** link to access the Mercury Managed Services Script Repository to view details of available scripts or verify unverified scripts. Only those scripts that have passed verification status can be added to a transaction monitor. For details, see "Mercury Managed Services Script Repository" in *Platform Administration*.

3 To filter your selection, click one of the links above the list to display only those scripts beginning with that letter, number, or symbol (**Other**). To revert to the complete list, click **ALL**.



4 Move the selected script to the right pane using the right-facing arrow. You can select multiple scripts using the CTRL key. The right pane lists all scripts selected for this monitor in the order that the profile will run the scripts.

5 To continue, follow steps 6 through 9 in the procedure for adding a transaction monitor to a profile on page 12.

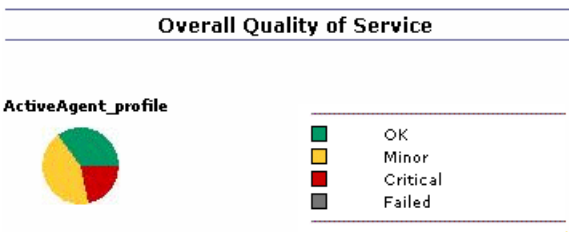
Setting Transaction Thresholds

Transaction thresholds are performance boundaries that organize transaction response time data in a meaningful way, enhancing validation of service level agreements. There are three color-coded transaction threshold ranges: OK, Minor, and Critical. The color codes are used in Dashboard and in the reports that display transaction performance data. The color-coding enables quick pinpointing of problem areas that need further analysis.

Range	Color Code
OK	Green
Minor	Yellow
Critical	Red

A fourth transaction threshold range enables classifying transactions as outliers. Outliers are transactions whose response time exceeds a defined time range. You can specify whether outlier transactions are treated as failed transactions or ignored completely in reports.

In the following example of an Overall Quality of Service chart, 35 percent of all transactions had response times in the OK range (colored green), 42 percent of response times were in the Minor range (colored yellow), and 23 percent were in the Critical range (colored red). When viewing the chart, these percentages are available in a tooltip that is displayed when you place your cursor over each section. The tooltip also specifies the number of outlier transactions.



Mercury Business Availability Center automatically sets default transaction threshold values for each transaction in the profile. If required, you can modify the default threshold values. The default transaction thresholds are as follows:

Range	Default Threshold
OK	8 seconds
Poor	12 seconds
Outlier	45 seconds

When setting transaction thresholds, you should take into account factors such as application performance under ideal conditions, competitors' performance, generally accepted performance standards, service level agreements, and end-user feedback.

Further, you should consider the alert trigger criteria you specify in your alert schemes. For example, if you set up an alert scheme to trigger a high priority alert whenever the response time of a transaction is greater than 15 seconds, you may want to set the Poor range for that transaction to 15 seconds or more.

In the Transaction Threshold Settings area, you can:

- configure how Mercury Business Availability Center treats outlier values (only while setting transaction thresholds for all of a profile's transaction monitors—the option is not available at the transaction monitor level)
- modify default threshold values for specific transactions
- update threshold values for more multiple transactions (useful when updating values for multiple transactions that have the same values)

To configure Transaction Threshold settings:

1 To instruct Mercury Business Availability Center to ignore outlier transactions (and not include the data in Dashboard or in reports), select **Ignore outlier data in Dashboard and reports**.

This is a profile-wide setting, so it is available only for all the transactions within the profile.

2 Select the check box next to the transactions whose thresholds you want to modify.

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

3 Click the **Edit Transaction Threshold** button. The Edit Transaction Thresholds dialog box opens.

4 Modify the values as required:

- OK – If the transaction response time is less than this value, it's status is OK.
- Critical – If the transaction response time is greater than this value, it's status is Critical.
- Outlier – If the transaction response time is greater than this value, the run of the transaction is considered outlier. If you selected to ignore outlier values in step 1, any transaction that takes longer than this value to complete is ignored in Dashboard and in reports. If you did not select to ignore outlier values and if the transaction response time is greater than this value, it's status is Failed.

If you selected multiple transactions in step 2, any changes you make modify the thresholds for all the transactions selected.

5 Click **OK** to save your changes and close the Edit Transaction Thresholds dialog box.

6 Review the table listing each transaction and its current threshold settings to ensure that they reflect the way the response times should be reported.

7 Click **Next** to continue.

The next stage of the wizard is to add WebTrace monitors to the profile. Continue to "Adding WebTrace Monitors" on page 17, in the next section.

Adding WebTrace Monitors

WebTrace monitors record the specific route taken from the data collector to the destination Web server or IP address, including the specific gateway servers at each hop.

The WebTrace reports provide information on network performance, which helps you analyze application performance issues. For example, by entering the addresses of the servers receiving the HTTP requests recorded in the profile's Business Process transaction monitors, you can later verify whether poor transaction response times are being caused by problems along the network. For details on the WebTrace report, see "WebTrace by Location Report" in *Using End User Management*.

You define the locations from which you want to run WebTrace, and specify one or more destination Web sites. Mercury Business Availability Center executes the WebTrace between the location of the defined data collector instance and the designated destinations.

To add a WebTrace monitor to the profile:

1. In the Add WebTrace Monitor page of the wizard, click the **Add WebTrace Monitor** button.
2. In the **Destination** field that opens in the table, enter a destination Web server to specify the Web server on which you want the trace to be performed. Do not include the string http:// or https:// when typing the server address.

Note: WebTrace monitors do not support destination servers that begin with a numeric digit. IP addresses are supported.

---

3. To define additional WebTrace monitors, repeat steps 1 and 2.
4. Click **Next** to continue.

The next stage of the wizard is to select the data collectors that run the transaction monitors and WebTrace monitors assigned to the profile. Continue to "Selecting Data Collectors" on page 18, in the next section.

Selecting Data Collectors

The table of available data collectors lists all data collector instances confirmed for this installation of Mercury Business Availability Center. You can assign any, or all, of the monitors added to the profile to any, or all, of the data collector instances listed. The table also lists the host name of the data collector instance and the version number of the data collector software.

By default, once a monitor is added and a data collector selected, all the monitors are scheduled to be run by all the data collectors. You can modify which data collectors run which monitors in the next step in the wizard. For details, see "Assign Data Collectors and Configure Settings" on page 19.

To select data collectors for running transaction and WebTrace monitors:

1 In the list of **Available Data Collectors**, select the data collectors to run the monitors you have added to this profile.

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

Note to Mercury Managed Services customers: You can use the **Package Information** link to view and edit the details of your current package and running data collectors. You can also use the **Customer Private Pops** link to view any data collectors running for only your company.

The list of data collectors includes the version number of the data collector software and indicates whether it is privately run for your company (Private Pop).

---

2 Click the right arrow to move the data collectors to the list of **Selected Data Collectors**.

To remove data collectors from the selected list, select the data collector and click the left arrow.

3 Click **Next** to continue.

The next stage of the wizard is to assign monitors to the selected data collectors and configure settings for the data collector instances. Continue to "Assign Data Collectors and Configure Settings" on page 19, in the next section.

Assign Data Collectors and Configure Settings

In the Assign Data Collectors page you can:

- view details for the data collectors selected in the Select Data Collectors page (for details, see page 19)
- modify the list of monitors each data collector runs (for details, see page 20)
- configure the data collectors' settings (for details, see "Configuring Data Collector Settings" on page 21)

Viewing Data Collector Details

The table in the Assign Data Collectors page lists the following parameters for each data collector instance:

- **Location.** Location of the data collector instance as defined on the data collector machine.
- **Host.** Host alias of the data collector instance as defined on the data collector machine.
- **Group.** The group name assigned to the host location on the Business Process Monitor or in Monitor Administration.
- **Version.** Version of the data collector software installed on the data collector machine.
- **Schedule.** The schedule configured for the profile to run on the selected data collector (only relevant for monitors running on a Business Process Monitor).
- **Assigned Monitors.** A listing of all the selected profile's monitors currently scheduled to run on the data collector host location. By default, only the first monitor and last monitor appear on screen. Clicking the link of the monitors' names brings you to the Assigned Monitors dialog box where you can modify the monitors to run on this data collector.

Note to Mercury Managed Services customers: The table also indicates whether the data collector is run privately for your company (a Private Pop).

Assigning Monitors to Run on Data Collector Instances

Once you have added transaction and WebTrace monitors to a profile and selected the data collectors, by default, every monitor is assigned to run on every data collector. You can modify this list to assign specific monitors to run on data collector instances.

To modify the list of monitors running on a data collector instance:

1. Click the monitors link in the Assigned Monitors column of the table. The Assign Monitors for:<data collector name> dialog box opens.
2. In the list of **Selected Monitors**, select the monitors that should not run on this data collector instance. You can select multiple monitors by pressing CTRL and selecting the monitors.
3. Click the left arrow to move the monitor to the list of **Available Monitors** and remove it from the list of monitors the data collector runs.

   To add a monitor to a data collector's list of monitors to run, select the monitor from the list of **Available Monitors** and click the right arrow.
4. Click **OK** to save your changes and close the Assign Monitors for <data collector name> dialog box.
5. You can either:

   ➤ Click **Next** to continue in the wizard to the Summary page. For details, see "Confirming Profile Configurations" on page 27.

   ➤ Configure the settings for the data collector instances. For details, see "Configuring Data Collector Settings" on page 21, in the next section.

Configuring Data Collector Settings

In the Assign Data Collectors page of the wizard, you can configure the following settings:

- group name (for details, see below)
- schedule for Business Process profiles (for details, see page 22)
- advanced properties for running Business Process profiles (for details, see page 25)

Note: These settings are saved to the data collector only if you complete the steps in the wizard and click **Finish**. If you click **Cancel** during the wizard, any changes you make to group name, schedule, or advanced properties will not be saved.

Editing the Group Name

When assigning group names, keep in mind that you can later organize and break down reports on application performance according to the groups you choose. You should therefore assign group names to locations/hosts according to the criteria you are most interested in tracking.

For example, if you assign different transaction monitors checking different business processes to different locations, you can assign group names related to the business process being emulated from each location. Another example would be to organize based on meaningful groups used by your organization, such as Internet Service Providers (ISPs), network connection, browser type, and department.

To edit the group name of a data collector instance:

1. In the table, select a data collector instance.

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

2. Click **Edit Group**. The Data Collector Group dialog box opens.

3 Enter the name of the group as you want it to appear in reports. If you selected multiple data collector instances in step 1, the group name you enter is the group name for all selected data collector instances.

4 Click **OK** to save your changes and close the Data Collector Group dialog box.

Editing the Schedule for Business Process Profiles

Defining a scheduling scheme for Business Process profiles is optional, as Mercury Business Availability Center automatically assigns a default scheduling scheme to each data collector instance. You can modify these settings to suit the individual needs of your organization.

The current schedule for the data collector instance is listed in the table. If no changes were made, the default schedule for the data collector to run all its transaction monitors is every 15 minutes, all week, all day, with a GMT offset of -1.

You can define multiple schedules for a profile running on a specific data collector instance. This enables you to run the profile using different schedules at different times. For example, you can have the profile run every 15 minutes during the working week and every hour during weekends.

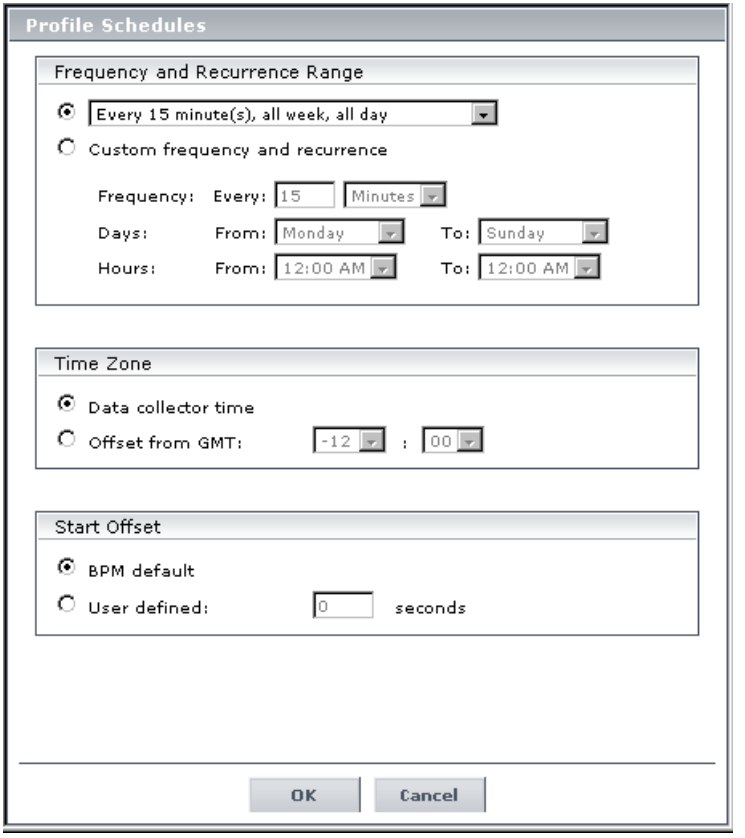
To define a scheduling scheme:

1 In the table, select a data collector instance.

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

2 Click **Edit Schedule**. The Profile Schedules dialog box opens and displays the current schedule settings.

3 To create a schedule, click **New Schedule**. To edit an existing schedule, click the **Edit** button next to the schedule. The Profile Schedule dialog box opens containing the same editable fields.



4 Set the schedule properties:

- Frequency for running the profile
- Days of the week on which to run the profile
- Hours in the day during which to run the profile

Tip: It is recommended that you use the default scheduling scheme: **Every 15 minutes, all week, all day**

---

5 Select the time zone properties:

- ➤ Choose **Data collector time** to have the data collector instance base its scheduling on the data collector machine's time clock. Note that, depending on the data collector location, local time may vary among machines.
- ➤ Choose **Offset from GMT** to have the data collector instance base its scheduling on the time zone you set. Specify a time zone in relation to GMT (for a reference list of GMT time zones for locations throughout the world, see "GMT Time Zones" in *Reference Information*).

  For example, if you want the data collector instance to run profiles based on Pacific Time, you would type **-8**, since Pacific Time is GMT-8 hours.

  Choosing **Offset from GMT** enables you to synchronize transaction run times among hosts.

6 Set a **Start Offset** option to delay the scheduled running of the profile. This enables the optimal distribution of script runs over time and minimizes the parallel running of many scripts. For details, see "Profile Start Offset" in *Business Process Monitor Administration*.

- ➤ Choose **BPM default** to use the start offset automatically assigned in the Business Process Monitor for each profile that has this setting.
- ➤ Choose **User defined** and set the amount of seconds the Business Process Monitor should offset the running of this profile.
  - If you define the start offset value as 0, then no offset is applied for the profile and the profile run will start at the time specified in the profile schedule.
  - If you define the start offset as -1, or do not enter a value, then the Business Process Monitor that runs the profile allocates a start offset, as described above.

- If you enter a positive value, the profile will be run that many seconds later than the schedule configured for the profile. For example, if the profile is scheduled to run every hour, beginning at noon and you enter 5 seconds as the user-defined start offset, the profile will begin running at 12:00 and 5 seconds, and continuing running every hour, at the hour plus 5 seconds.

7 Click **OK**. The schedule is added/updated in the Profile Schedules dialog box.

8 Repeat steps 2-7 to assign multiple schedules to this profile.

Note: When setting multiple schedules on a profile, keep in mind that if the schedules overlap at any time, the profile will be run according to both schedules. The exception is if the profile is still running when a second schedule is set to start; in which case, the iteration of that profile will not run and the data collector skips that scheduled iteration.

---

9 Click **OK** to save all your schedules and close the Profile Schedules dialog box.

Configuring Advanced Properties for Running Business Process Profiles

You set the run mode, step, and time out properties for the Business Process profile in the Advanced Properties dialog box. These properties instruct the Business Process Monitor on how to run the scripts in the profile.

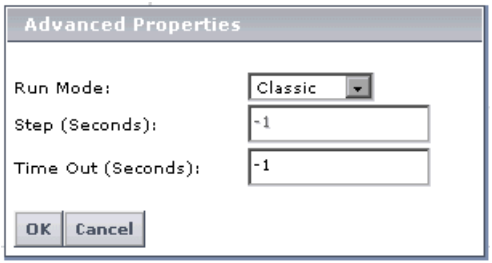
For details on the specific run mode options and setting the step value, see "Run Schedule for Profile Tasks" in *Business Process Monitor Administration*.

To configure advanced properties for Business Process profiles:

1 In the table, select a data collector instance.

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

2 Click **Advanced Properties**. The Advanced Properties dialog box opens.



3 Select a run mode from the available options.

4 If you select **Stepped** as the run mode option, set the **Step** value in seconds. (If **Stepped** is not selected as the run mode, this setting is disabled.)

5 Set the **Time Out** value in seconds.

This value determines the time limit after which the data collector (Business Process Monitor) running all the monitors added to this profile will timeout each of the scripts or WebTrace schemes if they are still running. This setting overrides the timeout value set on the data collector itself (default value on the Business Process Monitor is 15 minutes). If this value is set to -1 (default value), the timeout value on the Business Process Monitor is used.

6 Click **OK** to save the Advanced Properties settings and close the dialog box.

7 Click **Next** to continue.

The next stage of the wizard is to confirm the details of the profile and monitors you just created. Continue to "Confirming Profile Configurations" on page 27, in the next section.

Confirming Profile Configurations

In the Summary page of the wizard, you view the profile you just created and all the monitors that have been added to it.

For example, if you created a profile named Springfield_Processes, as in the example below, the Summary page displays the profile as the root object in a tree hierarchy with any monitors that have been added to the profile as the profile's child objects, including the individual transactions.

The object icons are the same as those displayed that in the monitor tree. This same hierarchy appears in the monitor tree once you finish the wizard.

To verify details and save the profile and/or monitors:

1. Read through the summary and verify that the details are correct.

   To make any changes to the profile or monitors, click **Back**.

2. Click **Finish** to save.

   Updating your new profile may take a few moments, depending on how many monitors you selected and the size of the scripts added as transaction monitors.

   The Finish page opens displaying the status of the profile and/or monitors you created and indicating if there were any errors during creation.

3. Click **OK** to return to Monitor Administration and view the created objects in the monitor tree.

2

Managing Business Process Profiles and Creating Client Monitor Profiles

The Business Process Monitor and Client Monitor collect data by running Business Process and Client Monitor profiles. You manage Business Process profiles and create Client Monitor profiles using the monitor tree in Monitor Administration.

About Managing Business Process and Client Monitor Profiles

Business Process profiles and transaction monitors are created using the Business Process Profile Wizard. For details, see "Creating Business Process Profiles" on page 1. Once created, these profiles and monitors are represented in the monitor tree of Monitor Administration. To make any changes to these profiles and monitors, you must use the monitor tree, Properties tab, and Contents tab.

Client Monitor profiles are created using the monitor tree, Contents tab, and Properties tab. You create and manage Client Monitor profiles in the same way you edit Business Process profiles.

You use Monitor Administration to:

- edit Business Process profiles and create Client Monitor profiles (for details, see "Creating Client Monitor Profiles and Editing Business Process Profiles" on page 31)
- add transaction monitors to Client Monitor profiles and edit Business Process profile transaction monitors (for details, see "Adding and Editing Transaction Monitors" on page 34)
- reassign monitors to run on host locations (for details, see "Host Assignment Settings" on page 48)
- configure settings for the profile and the transaction monitor (for details, see "Configuring Profile, Host, and Monitor Settings" on page 44)
- edit WebTrace destinations for Business Process profiles and add traceroute destinations for Client Monitor profiles (for details, see "Defining Traceroute Monitors and Editing WebTrace Monitors" on page 58)
- specify Single URL monitors (Mercury Managed Services customers only) (for details, see "Specifying Single URL Monitors for Business Process Profiles" on page 60)
- copy and paste configuration settings for profiles and monitors (for details, see "Replicating Profiles and Monitors" on page 67)

- start and stop the running of Business Process profiles (for details, see "Starting and Stopping Business Process and Client Monitor Profiles" on page 69)

You use the monitor tree to navigate through containers and elements in the tree structure and drill down to monitor and other configuration settings. For details on the different hierarchy elements, see "Using Monitor Administration" in *Working with Monitor Administration*.

You can customize your view of the monitor tree to list only those elements with which you are working. You can also assign categories to your profiles and monitors to further refine your views. For details, see "Setting Views and Defining Categories" in *Working with Monitor Administration*.

In addition, Monitor Administration enables you to change configurations across multiple profiles and transaction monitors using **Global Replace**. For details, see "Using Global Replace" in *Working with Monitor Administration*.

Creating Client Monitor Profiles and Editing Business Process Profiles

Monitor Administration uses containers to organize configuration data for profiles. A Client Monitor profile can be added directly to the enterprise node or into a container. For details on working with containers, see "Using Monitor Administration" in *Working with Monitor Administration*. For details on understanding the process of creating profiles, configuring settings, and adding monitors, see "About Managing Business Process and Client Monitor Profiles" on page 30.

To create Business Process profiles, use the Business Process Profile Wizard. For details, see "Creating Business Process Profiles" on page 1. To edit and manage existing Business Process profiles, use the fields described in the procedure for adding Client Monitor profiles. For details on managing Business Process profiles and how to access the profile for editing, see "Maintaining Business Process and Client Monitor Profiles" on page 64.

To create Client Monitor profiles and edit Business Process profiles:

1 Access Monitor Administration by selecting **Monitors** in the Admin menu. Select from the following options:

- In the monitor tree, right-click the enterprise node or container into which you want to add a new Client Monitor profile and choose **New Client Monitor Profile** in the container's menu.
- In the Contents tab, highlight the container into which you want to add the profile and click the **New Client Monitor Profile** button at the top of the page.

The Add Client Monitor Profile page opens.

Note: This first step covers the procedure for adding a Client Monitor profile only. If you are editing a Business Process profile and need details on accessing the profile, see "Accessing Object Properties for Editing" in *Working with Monitor Administration* and continue to step 2 for details on editing the profile's fields.

---

2 In the **Main Settings** area, enter or edit the following information:

- **Profile name.** A descriptive name that identifies the profile in the monitor tree, in the Dashboard, and in reports.
- **Profile description.** The profile description appears in reports as the tooltip for the profile name. For details on entering meaningful descriptions, see "Adding Descriptions for Reports" on page 55.

Note: If an existing profile's description is edited, the old description appears until the cache is refreshed (maximum 60 minutes).

➤ **Profile database name.** The database for storing profile information. This setting cannot be edited once it is set.

If you want to create a new profile database, click the **Manage Profile Databases** link which will take you to the page in Platform Administration where you can create a new profile database.

For details on creating a profile database, see "Database Management" in *Platform Administration*.

➤ **GMT offset.** The time zone, in relation to GMT, that Mercury Business Availability Center uses when aggregating data collected by this profile. For example, if you want Mercury Business Availability Center to aggregate data collected by the profile based on Pacific Time, enter -8, since Pacific Time is GMT-8 hours. For a reference list of GMT time zones for locations throughout the world, see "GMT Time Zones" in *Reference Information*.

Note: The **Script Order** (for Business Process profiles only) and **Transaction Threshold Settings** areas are editable only after a transaction monitor has been added to a profile. For details on defining these settings, see "Configuring Profile, Host, and Monitor Settings" on page 44.

---

3 Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this profile. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a profile to Monitor Administration and cannot be set while editing a profile.

---

4 Optionally, if there are any categories defined in the enterprise, you can assign a category to the profile under the **Category Settings** section.

For details on defining categories, see "Working with Categories" in *Working with Monitor Administration*.

5 Click **OK**. Your new Client Monitor profile is added to the monitor tree.

Adding and Editing Transaction Monitors

Once you have added a Client Monitor profile, one of the first steps in creating a profile's content is to select, and configure properties for, the transaction monitors that you want your data collectors to run. The transaction monitors are the scripts that contain the transactions.

You record scripts using one of the Mercury Business Availability Center recording tools. For details on creating Client Monitor scripts, see "Welcome to Using Client Monitor Recorder" in *Using Client Monitor Recorder*.

Before adding scripts to transaction monitors, you must upload the script to the Script Repository. For details, see "Using the Script Repository in Monitor Administration" on page 39 and "Script Repository" in *Platform Administration*.

Note: Business Process profile transaction monitors are added to a Business Process profile only by using the Business Process Profile Wizard. For details, see "Adding Transaction Monitors" on page 9. The fields described here in the procedure for adding a transaction monitor to a Client Monitor profile can be used to edit a Business Process transaction monitor.

For details on configuring the settings for transaction monitors, see "Configuring Profile, Host, and Monitor Settings" on page 44.

Adding Transaction Monitors to a Profile

You can add a Client Monitor transaction monitor only directly to a Client Monitor profile in the monitor tree and not to any other container in the tree.

Transaction monitors are added by selecting scripts from the Script Repository and configuring settings for how the profile should run the script within the transaction monitor. You can add multiple transaction monitors to a profile simultaneously. Each transaction monitor will have the same settings, which can be edited at a later time.

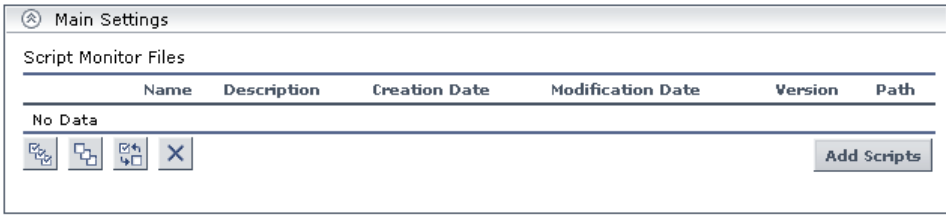
Client Monitor transaction monitors are assigned to run on containers or groups that can contain multiple Client Monitor hosts (for details on creating Client Monitor containers and groups, see "Managing Client Monitor Hosts" in *Platform Administration*). Business Profile transaction monitors are assigned to run on individual Business Process Monitor instances.

To add a Client Monitor transaction monitor:

1 Access Monitor Administration by selecting **Monitors** in the Admin menu. Select from the following options:

- In the monitor tree, right-click the Client Monitor profile to which you want to add a new transaction monitor and choose **New Transaction Monitor** in the profile's menu.
- In the Contents tab highlight the appropriate Client Monitor profile in the monitor tree, and click **New Transaction Monitor**.

2 In the **Main Settings** area, click **Add Scripts** to add a script from the Script Repository. For details, see "Using the Script Repository in Monitor Administration" on page 39.



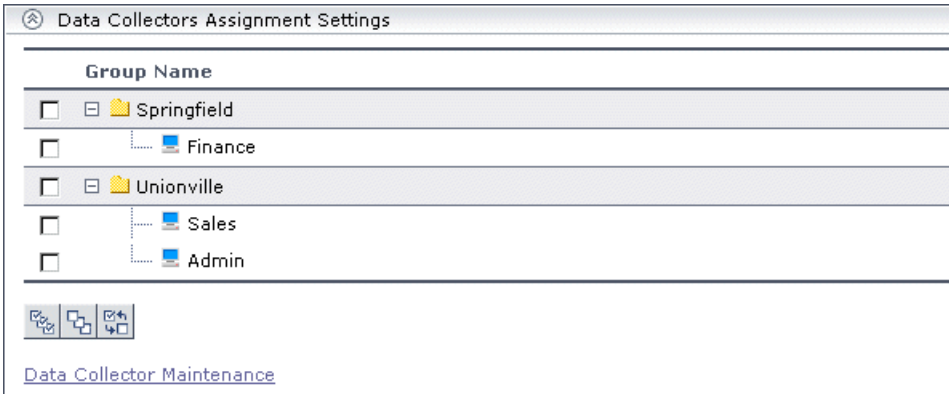
Note: Only scripts that have been added to the Script Repository can be added to the transaction monitor.

Note to Mercury Managed Services customers: All the scripts in the script repository are listed in the Main Settings area, along with their update time and status. To add one or multiple transaction monitors to a profile, select from these scripts. Click the link to access the repository. For details, see "Mercury Managed Services Script Repository" in *Platform Administration*.

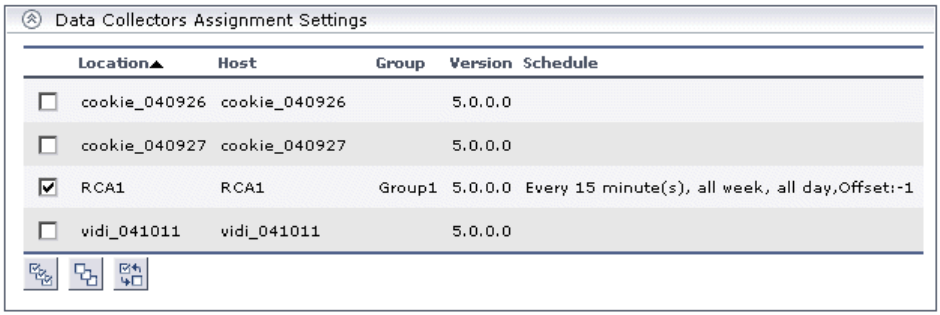
---

3 In the **Data Collector Assignment Settings** area, select the Client Monitor containers or groups, or the Business Process Monitor instances, on which to run this monitor. By default, all the Client Monitor containers and groups, or Business Process Monitor instances are listed. You can assign Client Monitor containers or groups, or Business Process Monitor instances at a later stage by editing the profile, but for the transaction monitor to run, at least one container, group, or instance must be assigned.

Data Collectors Assignment Settings area for Client Monitor containers and groups:



Data Collectors Assignment Settings area for Business Process Monitor instances:



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

All groups and containers that are included in a selected Client Monitor container are also automatically included in the selection.

If you want to create or manage Client Monitor containers and groups, click the **Data Collector Maintenance** link which will take you to the page in Platform Administration where you can create and manage Client Monitor containers and groups.

For details on creating and manage Client Monitor containers and groups, see "Managing Client Monitor Hosts" in *Platform Administration*.

You can also assign monitors to host locations using the Data Collectors tab (for details, see "Host Assignment Settings" on page 48) or from the Contents tab (for details, see "Assigning Data Collector Locations to Monitors" on page 68).

Note to Mercury Managed Services customers: The Data Collector Assignment Settings area lists all the locations in your package. Optionally, you can click the **Package Information** link and the **Customer Private Pops** link to view and modify package and location information. For details, see "Package Information" in *Platform Administration*.

---

4 In the **Transaction Breakdown Settings** area, select from the following options:

➤ Select **Enable breakdowns** to generate transaction breakdown data when running the selected monitor.

- If you have enabled breakdowns, you can select **Report additional error information** to include date, time, location, and error messages for failed transactions.
- If you have enabled breakdowns, you can select **Perform component breakdown** to save complete page component breakdown data for a sampling of transaction instances. By default, Mercury Business Availability Center saves page component breakdown data to the database once per every four transaction instances. This setting is available for Business Process transaction monitors only.

➤ Select **Enable Diagnostics breakdown** to see J2EE and .Net data. This data is available in Diagnostics reports only if you have a valid Mercury Diagnostics license. For details, refer to *Mercury Diagnostics Installation and User's Guide*. This setting is available for Business Process transaction monitors only.

➤ Select **Enable Siebel breakdown** to see Siebel Application Response Measurement (SARM) data in Business Availability Center for Siebel. This setting is available for Business Process transaction monitors only.

For more details on these options, see "Enable/Disable Transaction Breakdown for the Transaction Monitor" on page 51.

5 Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this transaction monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a transaction monitor to Monitor Administration and cannot be set while editing a transaction monitor.

---

6 Optionally, if there are any categories defined in this enterprise, you can assign a category to the transaction monitor under the **Category Settings** section.

For details on defining categories, see "Working with Categories" in *Working with Monitor Administration*.

7 Click **OK** to add the transaction monitor to your Client Monitor profile. The transaction monitor appears as a child object under the profile in the monitor tree.

For details on editing the profile and monitor properties, see "Configuring Profile, Host, and Monitor Settings" on page 44.

Note: The **Transaction Threshold Settings** and **Transaction Description Settings** are editable only after the transaction monitor has been added to the profile. Once the transaction monitor is added, edit the profile and the transaction monitor to configure these settings.

For details on how to set transaction thresholds, see "Transaction Threshold Settings" on page 53.

For details on what to include in the description, see "Adding Descriptions for Reports" on page 55.

Using the Script Repository in Monitor Administration

Note to Mercury Managed Services customers: The repository for Mercury Managed Services scripts functions differently from the repository described here. For details, see "Mercury Managed Services Script Repository" in *Platform Administration*.

The Script Repository is the central storage in which all your organization's Business Process Monitor scripts and Client Monitor scripts are stored and organized. In Monitor Administration, you can add to transaction monitors only those scripts that are in the Script Repository.

Adding Scripts from the Script Repository to Create a Transaction Monitor

When adding scripts to a transaction monitor, you must select a script from the Script Repository. You must locate and select the script containing those transactions you want this profile to run.

You can also use the **Script Repository** link at the top of the Add Transaction Monitors window to access the Script Repository where you can create folders, add scripts, control script versions, and view script and version properties. For details, see "Script Repository" in *Platform Administration*.

To add a script from the Script Repository to the transaction monitor:

1. While creating a transaction monitor, click **Add Scripts** in the Main Settings area. The Add Transaction Monitors page opens.
2. In the upper left Repository pane, select the folder containing the script to add to the transaction monitor.

   The upper right Scripts pane displays all of the scripts contained in the selected folder.
3. In the upper right Scripts pane, select the scripts to add to the transaction monitor. You can add multiple scripts to one transaction monitor.

   To make your selections, you can also use the buttons at the bottom of the area for **Select All**, **Clear All**, and **Invert Selection**.
4. In the Selected Scripts area at the bottom of the page, select the scripts you want to add to the transaction monitor.
5. Optionally, use the dropdown list of the version number to display and select older versions of the script. By default, the latest version number is displayed.
6. Click **OK**. The Add Transaction Monitors page closes and the script is added to the transaction monitor. You continue entering the fields for adding the transaction monitor as described in steps 3 through 7 in the procedure for adding a transaction monitor on page 36.

Adding Transaction Monitor Scripts to the Script Repository

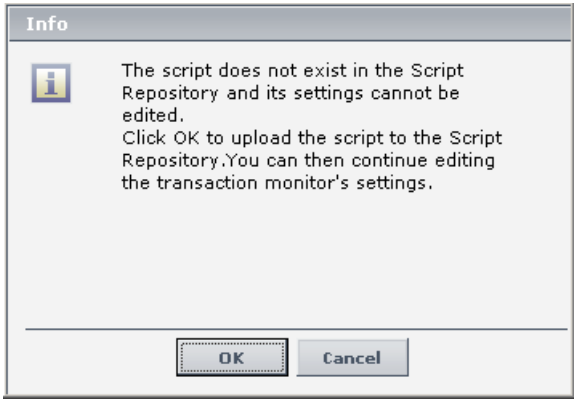
If a transaction monitor's script is not in the Script Repository, the transaction monitor's properties cannot be edited until that script is added to the repository. A note indicating as such appears in the Contents tab within the table listing the profile's transaction monitors.

You can add a transaction monitor's script to the Script Repository from within Monitor Administration. When you attempt to edit a transaction monitor whose script is not in the Script Repository, a message opens enabling you to add the script to the repository.

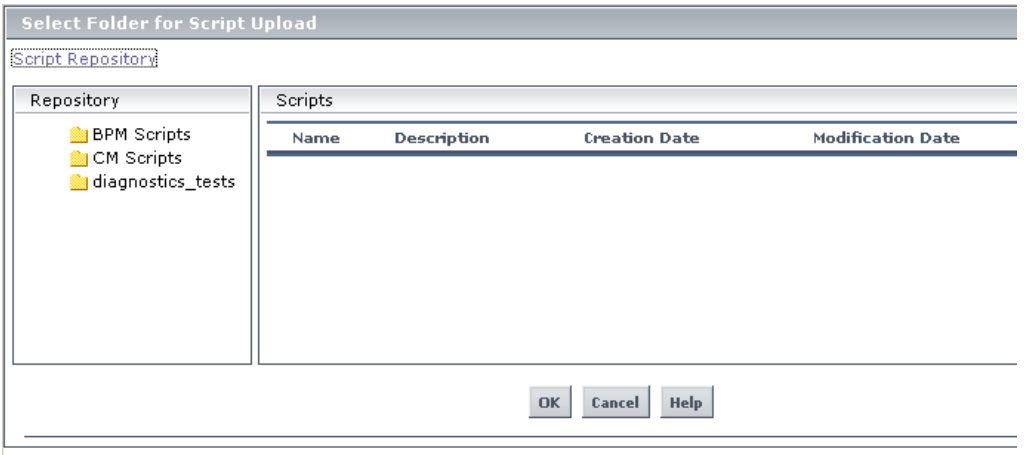
Note: When upgrading from a previous version of Mercury Business Availability Center that did not include a Script Repository, this is the same procedure to follow when the profiles and transaction monitors have been upgraded but the scripts are not in the Script Repository.

To add a transaction monitor's script to the Script Repository:

1 Edit the transaction monitor by clicking its **Edit** button in the Contents tab or by selecting **Edit** in the transaction monitor's menu (right-click the transaction monitor in the monitor tree). The following warning message opens.



2 Click **OK**. The Select Folder for Script Upload page opens.



3 In the Repository pane, select the folder into which you want to upload the transaction monitor's script. Click **OK**.

Optionally, you can click the **Script Repository** link at the top of the page to access the Script Repository and create a new folder into which to upload the script. For details on working in the Script Repository, see "Script Repository" in *Platform Administration*.

Updating Versions of a Transaction Monitor Script

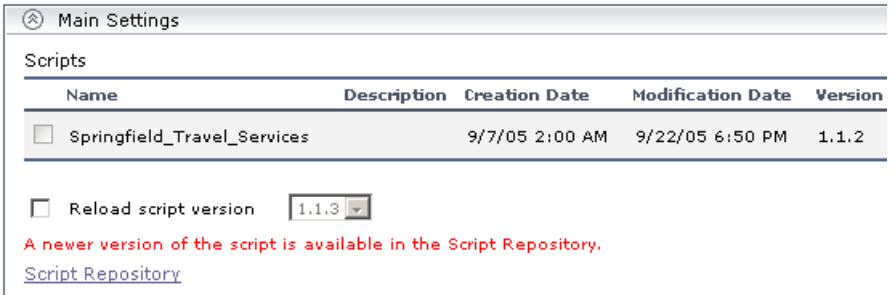
If an updated version of a transaction monitor's script exists in the Script Repository, a notification appears in the Contents tab within the table listing the profile's transaction monitors.

You can update the version of a transaction monitor script directly from the Edit Transaction Monitor Properties page in Monitor Administration.

To update the version of a transaction monitor script:

1 Access the transaction monitor's Edit page. For details, see "Accessing Object Properties for Editing" in *Working with Monitor Administration*.

In the Main Settings area, a message appears in red indicating that a newer version of the script is available in the Script Repository.



2 Select **Reload script version** to load the version of the script displayed in the script version box (by default, the latest available version). Optionally, you can select a different version of the script to reload for the transaction monitor.

3 Click **OK** at the bottom of the edit properties page.

Zipping Scripts

To add a transaction monitor to a Business Process profile in Monitor Administration, the files comprising the transaction must be zipped.

You can zip a transaction's files by:

- Using the Virtual User Generator. For details, see *Using Mercury Virtual User Generator* accessed from the table of contents in the Documentation Library.
- Zipping the files in your file manager as described in the following procedure.

To zip transactions:

1. In your file manager, browse to the transaction's directory.
2. Select all the files in the directory (CTRL A) and create a zip file including all the files. You must use the name of the .usr file as the name of the zipped file. For example, if the .usr file is called check_accounts.usr, the zip file must be named check_accounts.zip.

   Ensure that the **Save full path info** option is not selected so that there are no paths in the path column of the zip archive.

Note: Do not select the directory itself to **Add to Zip** as this will include the directory name in the path column. You cannot add a zipped file that includes a directory to a profile in the console.

Configuring Profile, Host, and Monitor Settings

Once transaction monitors are added to profiles, there are several configuration settings that must be defined according to the needs of your organization. These are defined using the Data Collectors tab or within the properties page for the profile or the individual monitor.

When adding Client Monitor profiles and monitors, you must follow the procedures detailed below. When adding Business Process profiles, these configurations are done within the Business Process Profile Wizard. For details, see "Creating Business Process Profiles" on page 1. To change any of the settings configured within the Business Process Profile Wizard, use the procedures described in the sections referenced below.

- Once you have created transaction monitors, you can select which monitors to run on which data collector's host locations using the Data Collectors tab.
- Also in the Data Collectors tab, you define data collector configurations for Business Process profiles, including group names, schedules, and advanced properties at the host location level.

- You determine threshold settings per monitor or, alternatively, for all the monitors running within a profile.
- You determine transaction breakdown settings and add descriptions to reports at the monitor level.

Location and Profile Settings

- Host Assignment Settings – For details, see page 48.
- Data Collector Configurations – For details, see page 50.

Profile or Transaction Monitor Settings

- Transaction Threshold Settings – For details, see page 53.

Note: While you can configure transaction thresholds at either the profile level or the transaction level, you can select or clear the ignore outlier value option only while editing the profile because this is a profile-wide setting.

Transaction Monitor Settings

- Enable/Disable Transaction Breakdown for the Transaction Monitor – For details, see page 51.
- Adding Descriptions for Reports – For details, see page 55.

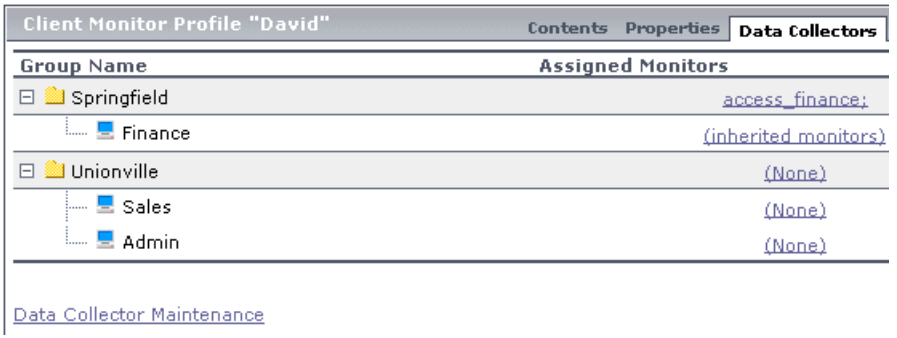
Using the Data Collectors Tab

The Data Collectors tab appears as an option when a Business Process or Client Monitor profile is highlighted in the monitor tree. You use the Data Collectors tab to assign monitors to host locations.

Note: When using the Business Process Profile Wizard to create profiles or add transaction monitors, the process of assigning monitors to host locations is one of the steps in the wizard. For details, see "Assign Data Collectors and Configure Settings" on page 19. You can modify the assignments by using the Data Collectors tab and the procedures described below.

You can assign any, or all, of the monitors added to the profile to any, or all, of the host locations configured for the platform. This gives you a complete picture of all the monitors running within the profile and which Client Monitor containers or groups, or which Business Process Monitor instances, are running which monitors.

Client Monitor profile Data Collectors tab:



The table in the Data Collectors tab for Client Monitor profiles lists the following parameters for each Client Monitor container or group:

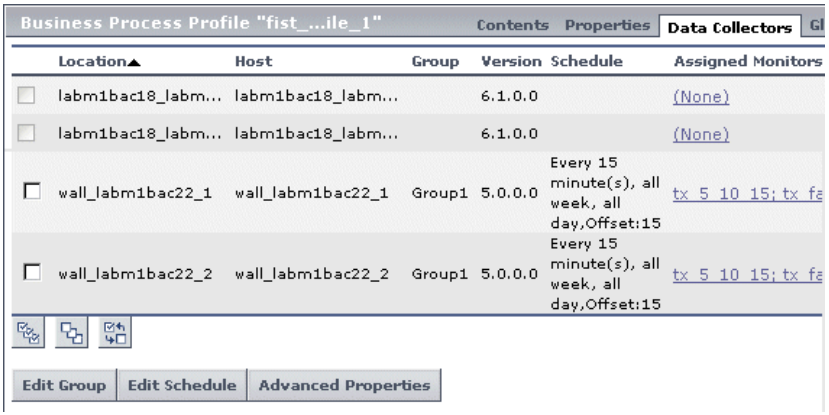
- **Group Name.** The Client Monitor container or group name, as defined in Platform Administration.

- **Assigned Monitors.** A listing of all the selected profile's monitors currently scheduled to run on the Client Monitor hosts included in the container or group. If none of the profile's monitors are scheduled to run on the Client Monitor hosts included in the container or group, **(None)** appears as a link. Clicking this link brings you to the Assigned Monitors dialog box where you can assign monitors to run on the host.

  If you want to create or manage Client Monitor containers and groups, click the **Data Collector Maintenance** link which will take you to the page in Platform Administration where you can create and manage Client Monitor containers and groups.

  For details on creating and manage Client Monitor containers and groups, see "Managing Client Monitor Hosts" in *Platform Administration*.

Business Process profile Data Collectors tab:



The table in the Data Collectors tab for Business Process profiles lists the following parameters for each host location:

- **Location.** Location of the Business Process Monitor instance as defined on the data collector machine.
- **Host.** Host alias of the Business Process Monitor instance as defined on the Business Process Monitor machine.
- **Group.** The group name assigned to the host location on the Business Process Monitor or in Monitor Administration.

- **Version.** Version of the Business Process Monitor software installed on the Business Process Monitor machine.
- **Schedule.** The schedule configured for the profile to run on the selected Business Process Monitor.
- **Assigned Monitors.** A listing of all the selected profile's monitors currently scheduled to run on the Business Process Monitor instance's host location. By default, only the first monitor appears on screen. To view all the monitors, expand the list using the plus sign button next to the first monitor that appears. If none of the profile's monitors are scheduled to run on the Business Process Monitor instance, **(None)** appears as a link. Clicking this link brings you to the Assigned Monitors dialog box where you can assign monitors to run on the host.

The Data Collectors tab enables you to manage:

- "Host Assignment Settings" on page 48
- "Data Collector Configurations" on page 50

Host Assignment Settings

Within the Data Collectors tab, you can assign multiple monitors to run on selected data collector host locations. The monitor types that can be assigned to a location and that are listed in the Assigned Monitors column in the Data Collectors tab include:

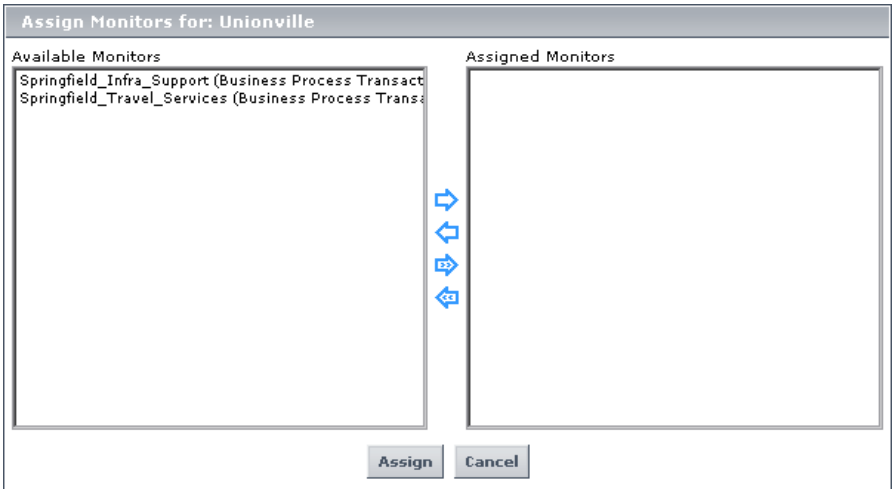
- transaction monitors (both Business Process and Client Monitor profiles)
- WebTrace monitors (Business Process profiles)
- traceroute (Client Monitor profiles)
- Single URL monitors (Business Process profiles for Mercury Managed Services customers only)

The monitors that appear in the **Assigned Monitors** column act as a link to a dialog box in which you can assign multiple monitors to run on, or remove monitors from running on, the selected host location and according to the host location's currently configured schedule.

To assign monitors to run on specific Business Process Monitor host locations or Client Monitor groups:

1. In the monitor tree, highlight the profile for which you want to edit the list of monitors running on specified host locations or groups.
2. Click the **Data Collectors** tab.
3. Navigate to the data collector host location or group for which you want to change the assigned monitors and in the **Assigned Monitors** column of that host location or group, click the link of the list of assigned monitors. If no monitors are running on this host, the link is the word **None**.

   The Assign Monitors dialog box opens.



4. Select the monitors that you want to assign to run on the selected data collector location or group from the **Available Monitors** list, and use the upper arrow to move your selection(s) to the **Assigned Monitors** list. You can select multiple monitors using the CTRL key or click the **Add All** arrow to select all the monitors.
5. Click **Assign** to confirm your selections and close the Assign Monitors dialog box.

To remove a specified monitor from the selection:

1. In the Assign Monitors dialog box, select the monitor you want to remove from the **Assigned Monitors** list, and use the lower arrow to remove the recipient. After removing, the recipient appears in the **Available Monitors** list. You can select multiple recipients using the CTRL key or click the **Remove All** arrow to select all the monitors.
2. Click **Assign** to confirm and close the Assign Monitors dialog box.

Data Collector Configurations

In the Hosts tab, you can edit the following settings that are configured while working in the Business Process Profile Wizard:

- group name (for details, see "Editing the Group Name" on page 21)
- schedule for the Business Process Monitor data collector (for details, see "Editing the Schedule for Business Process Profiles" on page 22)
- advanced properties for running Business Process profiles (for details, see "Configuring Advanced Properties for Running Business Process Profiles" on page 25)

Configuring Profile and Monitor Settings Using the Properties Page

The following configurations and settings are defined for Business Process profiles while adding transaction monitors in the Business Process Profile Wizard (for details, see "Adding Transaction Monitors" on page 9 and "Setting Transaction Thresholds" on page 14). They are configured for Client Monitor profiles or edited for Business Process profiles using the properties page in Monitor Administration:

- Enable/Disable Transaction Breakdown for the Transaction Monitor (for details, see below)
- Transaction Threshold Settings (for details, see page 53)
- Adding Descriptions for Reports (for details, see page 55)

Enable/Disable Transaction Breakdown for the Transaction Monitor

You specify whether you want Mercury Business Availability Center to generate transaction breakdown data when running the selected transaction monitor. You use transaction breakdown data to analyze relative server/network distribution time (for details, see "Understanding the Transaction Breakdown Reports" in *Using End User Management*).

You select the transaction breakdown settings while adding or editing a transaction monitor. For details, see step 4 in "Adding and Editing Transaction Monitors" on page 34.

➤ Select **Enable breakdowns** to enable transaction breakdown for the selected script. Note that Mercury Business Availability Center performs transaction breakdown by default.

➤ Clear **Enable breakdowns** to disable transaction breakdown. Disabling this option decreases the amount of data that is sent from the Business Process Monitor(s) to the profile database.

Note: Transaction breakdown supports only Web-based scripts. If you are running non-Web-based scripts, you must disable transaction breakdown.

Enable/Disable Reporting of Additional Error Information

If **Enable breakdowns** is enabled, you can select **Report additional error information** to specify that you want Mercury Business Availability Center to report transaction breakdown error details (date, time, location, and error message) in the Breakdown Summary report. If this option is disabled, Mercury Business Availability Center reports only average error times. Note that disabling this option decreases the amount of data that is sent from the Business Process Monitor(s) running the transaction breakdown to the Core Server and profile database. For details on the Breakdown Summary report, see "Understanding the Transaction Breakdown Reports" in *Using End User Management*.

Enable/Disable Page Component Breakdown (Business Process Profiles Only)

If **Enable breakdowns** is enabled, you can select **Perform component breakdown** to specify that you want Mercury Business Availability Center to save complete page component breakdown data for a sampling of transaction instances. For page component breakdown to appear in reports, the script containing the transactions had to have been recorded using one of the following protocols: SAP Web, Siebel Web, QTWeb, HTTP, SOAP, PS8, PS8WebJS, WinSockWeb, Oracle NCA, OracleWebJS.

For details on how page component breakdown data appears in reports, see "Page Component Breakdown Tool" in *Using End User Management*.

By default, Mercury Business Availability Center saves page component breakdown data to the database once per every four transaction instances. The setting for how often to save page component breakdown data can be modified from the PCBD section of the **topaz_data_server.cfg** file on the Business Process Monitor machine. For details, see "Parameters in topaz_data_server.cfg" in *Business Process Monitor Administration*.

Note to Mercury Managed Services customers: The default for saving page component breakdown data to the database differs for Mercury Managed Services. By default, page component breakdown data is saved when the transaction's threshold status changes to or from the Poor (red) status. For details on configuring transaction thresholds, see "Transaction Threshold Settings" on page 53.

Collecting page component breakdown data enables drilling down in the transaction breakdown reports, in the End User Management application. Drilling down to view the page component breakdown data for the transaction instances for which data is collected helps to pinpoint response time issues that occurred due to problems with a specific component of the page (for example, a large or missing image on the page).

Enable/Disable Diagnostics Breakdown (Business Process Profiles Only)

Mercury Business Availability Center integrates with Mercury Diagnostics to enable you to gain end-to-end visibility and comprehensive diagnostics for J2EE, .NET-connected, Siebel, SAP, Oracle, and other complex environments. To enable this integration, specify the Diagnostics Server details and configure the relevant components in Mercury Business Availability Center. For details, refer to *Mercury Diagnostics Installation and User's Guide*.

Transaction Threshold Settings

Transaction thresholds are performance boundaries that organize transaction response time data in a meaningful way, enhancing validation of service level agreements. For full details on how thresholds affect reports and data in Dashboard, see "Setting Transaction Thresholds" on page 14.

For Business Process profiles, transaction thresholds are set while adding transactions in the Business Process Profile Wizard. For Client Monitor profiles and to edit Business Process profiles, use the Transaction Threshold Settings area in the Properties tab.

In the Transaction Threshold Settings area, you can:

- configure how Mercury Business Availability Center treats outlier values (only while setting transaction thresholds for a profile—the option is not available at the transaction monitor level)
- using the lower table, modify default threshold values for specific transactions
- using the upper table, update threshold values for more than one transaction (useful when updating values for multiple transactions that have the same values)

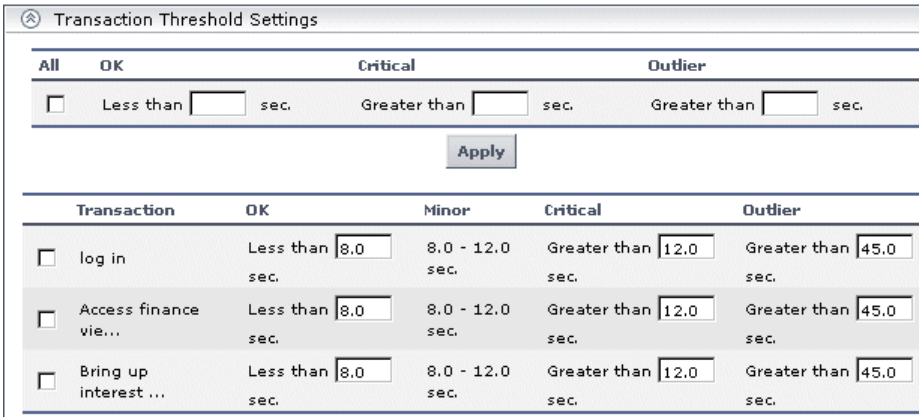
To modify transaction thresholds for specific transactions at either the profile or monitor level:

1 Access the page for editing either the profile or the transaction monitor (for details, see "Accessing Object Properties for Editing" in *Working with Monitor Administration*).

Note: This setting can be configured only after a monitor has been added to a profile and only when editing (and not adding) either the profile or the monitor.

---

2 Expand the Transaction Threshold Settings area.



3 To instruct Mercury Business Availability Center to ignore outlier transactions (and not include the data in reports), select **Ignore outlier data in reports**.

Note that this is a profile-wide setting, so it is available only when configuring profile properties (not transaction monitor properties).

4 Click the check box beside each transaction whose settings you want to modify.

If you are modifying thresholds for a profile, you can select the upper table and set the same transaction thresholds for all the transaction monitors in the profile.

5 In the OK and Critical columns in the lower table, modify the values (in seconds) as required. The OK range is from zero up to, but not including, the number you enter. The Critical range is between, but not including, the number you enter and infinity.

You can enter values that are less than a second. For example, you can set an OK range of 0.005 seconds (5 milliseconds).

6 In the Outlier column in the lower table, modify the outlier value as required.

Remember, a transaction whose response time exceeds its outlier value is treated as a failed transaction, unless you select the **Ignore outlier data in reports** option, in which case the data is excluded from reports.

You can view the number of outlier transactions that occurred during a specific time interval in the Error Summary report. For details, see "Error Summary Report" in *Using End User Management*.

7 Click **OK** to save the settings for the checked transactions.

To modify transaction thresholds for multiple transactions:

1 In the lower table, select the check box beside the transactions whose values you want to update.

To select all the transactions, select the **All** check box in the upper table.

2 Enter the required value(s) in the OK, Critical, and Outlier columns in the upper table.

3 Click **Apply** to apply the changes to the selected transactions in the lower table.

4 Click **OK** to save the settings for the selected transactions.

Adding Descriptions for Reports

You can configure Mercury Business Availability Center and Service Level Management reports to include a description of each profile and transaction. Profile and transaction descriptions appear as tooltips when you hold the cursor over the name in the report, or over the name of the profile in the list of profiles. For details, see "Example of Report Description" on page 57.

You can enter a maximum of 1000 characters. Keep in mind, however, that this description appears in a tooltip. If a user's computer monitor is set to a low resolution, not all of a very long description displays on the screen. The width of the tooltip is determined by the browser.

For details on adding a description to a profile, see step 2 under "Creating Client Monitor Profiles and Editing Business Process Profiles" on page 31.

To add transaction tooltip descriptions to a transaction monitor:

1. Access the page for editing the transaction monitor (for details, see "Accessing Object Properties for Editing" in *Working with Monitor Administration*).

   This setting can be configured only after a monitor has been added to a profile and only when editing (and not adding) the transaction monitor.

2. Expand the Transaction Description Settings area.

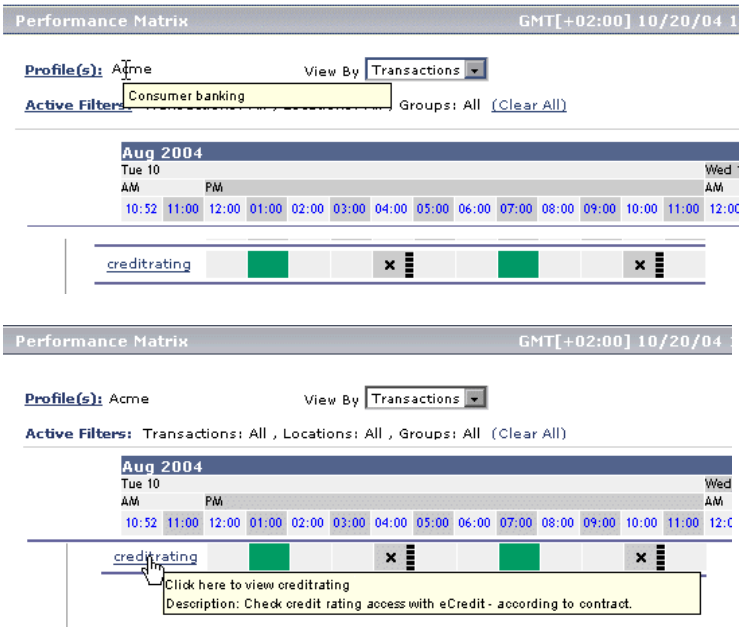
3. For each transaction listed for the transaction monitor, enter a description in the **Description** box.

4. Click **OK** to save your changes to the transaction monitor.

Example of Report Description

The profile **Acme** has the words Consumer banking added to the profile description box, and the transaction **creditrating** has the words Check credit rating access with eCredit - according to contract. added to the transaction description box.

These descriptions appear in the profile and transaction tooltips:



Defining Traceroute Monitors and Editing WebTrace Monitors

The traceroute and WebTrace monitors record the specific route taken from the data collector to the destination Web server or IP address, including the specific gateway servers at each hop.

The WebTrace monitor is added to Business Process profiles in the Business Process Profile Wizard while creating the profile. For details, see "Adding WebTrace Monitors" on page 17. To add a WebTrace monitor to an existing profile or to edit the monitor, use the descriptions below for adding a traceroute monitor to a Client Monitor profile.

You add a WebTrace monitor only to a Business Process profile and a traceroute monitor only to a Client Monitor profile and not to any other container in the monitor tree.

Note: Mercury Business Availability Center does not send traceroute definitions to Client Monitor until you add a script to the Client Monitor profile that includes the traceroute monitor.

To define a traceroute monitor to a Client Monitor profile or add a WebTrace monitor to an existing Business Process profile:

1 Access Monitor Administration by selecting **Monitors** in the Admin menu. Select from the following options:

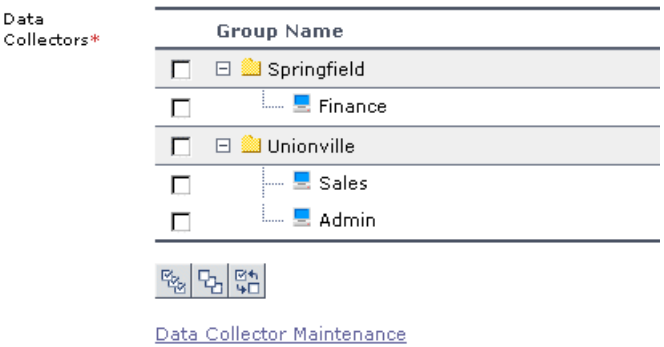
- In the monitor tree, right-click the Client Monitor or Business Process profile to which you want to add a new monitor and choose **New WebTrace** or **New Traceroute** in the profile's menu.
- In the Contents tab with the appropriate profile highlighted in the monitor tree, click **New WebTrace** or **New Traceroute**.

2 Type a destination Web server in the **Destination** box to specify the Web server on which you want the trace to be performed. Do not include the string http:// or https:// when typing the server address.

Note: WebTrace and Traceroute monitors do not support destination servers that begin with a numeric digit. IP addresses are supported.

---

3 In the **Data Collector** area, select the Client Monitor containers or groups, or the Business Process Monitor instances, on which to run this monitor. By default, all the Client Monitor containers and groups, or Business Process Monitor instances are listed. (For Mercury Managed Services customers, locations in your package are listed.) You must select at least one container, group, or instance to run the monitor.



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

If you want to create or manage Client Monitor containers and groups, click the **Data Collector Maintenance** link which will take you to the page in Platform Administration where you can create and manage Client Monitor containers and groups.

For details on creating and manage Client Monitor containers and groups, see "Managing Client Monitor Hosts" in *Platform Administration*.

For details on configuring the data collector assignment settings for the profile, see "Host Assignment Settings" on page 48.

Note to Mercury Managed Services customers: Optionally, you can click the **Package Information** link and the **Customer Private Pops** link to view and modify package and location information. For details, see "Package Information" in *Platform Administration*.

---

4 Optionally, if there are any categories defined in this enterprise, you can assign a category to the monitor under the **Category Settings** section.

For details on defining categories, see "Working with Categories" in *Working with Monitor Administration*.

5 Click **OK**. The WebTrace or traceroute monitor is added to the profile.

Specifying Single URL Monitors for Business Process Profiles

Note: This section applies to Mercury Managed Services customers only.

You define a URL to emulate navigation to the specified URL. You then track the response time and availability results in reports.

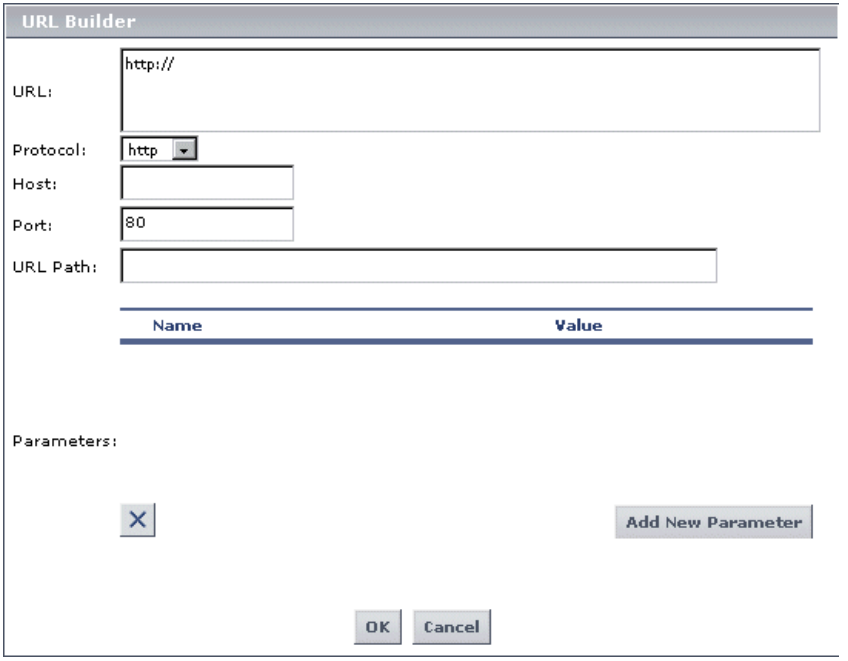
To define a single URL monitor:

1 Access Monitor Administration by selecting **Monitors** in the Admin menu. Select from the following options:

- In the monitor tree, right-click the Business Process profile to which you want to add a new single URL monitor and choose **New Single URL Monitor** in the profile's menu.
- In the Contents tab with the appropriate Business Process profile highlighted in the monitor tree, click **New Single URL Monitor**.

2 Type the URL that you want Mercury Business Availability Center to access in the **URL to monitor** box. In the **URL to monitor** box, include the protocol, host, and optionally include the port, URL path, and parameters.

Alternatively, click **URL Builder** to open the dialog box in which you define each of these elements of the URL in separate boxes. You can optionally add parameters to the URL by clicking the **Add New Parameters** button.



3 Enter a name for the single URL monitor in the **Transaction Name** box. This name identifies this monitor in the monitor tree, in the Dashboard, and in reports.

4 If the URL you specify requires authentication, in the Authentication area, select **Use secure logon**, and specify the required **Login name** and **Login password**.

5 Type a description for the URL in the **Transaction description** box. This description appears in a tooltip when you hold the cursor over the transaction name in reports, as well as in the Description column in the Performance Update report. For details, see “Adding Descriptions for Reports” on page 55.

6 In the **Data Collector Assignment Settings** area, select the data collector instances on which to run this monitor. By default, all the locations of the data collector type in your customer package are listed. You must select at least one data collector instance to run the monitor.

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

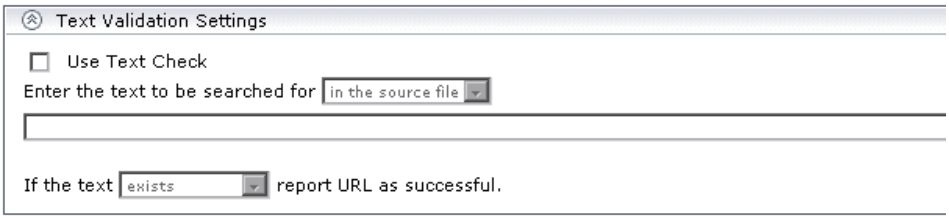
For details on configuring the data collector assignment settings for the profile, see "Host Assignment Settings" on page 48.

Note: Optionally, you can click the **Package Information** link and the **Customer Private Pops** link to view and modify package and location information. For details, see "Package Information" in *Platform Administration*.

---

7 Text checks are a way of verifying that the URL reaches the correct page. To perform a text check on the page loaded by the URL, in the Text Validation Settings area:

➤ Select **Use Text Check**.



➤ Specify whether Mercury Business Availability Center should search for the text in the HTML source file or on the screen (the text that appears in the browser window). Note that, if you select **in the source file**, Mercury Business Availability Center looks for text strings as they appear in the Web page's source code. Ensure that text strings do not include hard returns or special characters. For example: <

➤ Type the required text string.

➤ Specify whether the text should exist or not exist for Mercury Business Availability Center to consider the URL successful.

8 In the Run-Time Settings section, select the modem emulation setting that best reflects the type of connection used by your customer base. In this way, the data that Mercury Business Availability Center collects more closely reflects the actual user experience of your customers.

9 In the Transaction Threshold Settings section, specify the OK and Poor transaction threshold ranges and an outlier value. For details about transaction thresholds, see "Transaction Threshold Settings" on page 53.

10 In the Transaction Breakdown Settings area, select from the following options:

➤ Select **Enable breakdowns** to generate transaction breakdown data when running the monitor.

- If you have enabled breakdowns, you can select **Report additional error information** to include date, time, location, and error messages for failed transactions.
- If you have enabled breakdowns, you can select **Perform component breakdown** to save complete page component breakdown data for a sampling of transaction instances. By default, Mercury Business Availability Center saves page component breakdown data to the database once per every four transaction instances.

➤ Select **Enable Diagnostics breakdown** to see J2EE and .Net data. This data is available in Diagnostics reports only if you have a valid Mercury Diagnostics license. For details, refer to *Mercury Diagnostics Installation and User's Guide*.

For details on these options, see "Enable/Disable Transaction Breakdown for the Transaction Monitor" on page 51.

11 Optionally, if there are any categories defined in this enterprise, you can assign a category to the monitor under the **Category Settings** section.

For details on defining categories, see "Working with Categories" in *Working with Monitor Administration*.

12 Click **OK** to save the settings. The Single URL Monitor is added to the profile in the monitor tree.

You can add as many URLs as your Mercury Business Availability Center package allows. Mercury Business Availability Center displays usage status information at the top of the URLs table.

Maintaining Business Process and Client Monitor Profiles

Over time, you may find it necessary to make changes to profiles that you create, due to organizational changes, changes to your network environment, and so forth. You edit existing Business Process and Client Monitor profiles in Monitor Administration.

You also may find it necessary to synchronize the information stored in the profile database with your monitor tree.

Note that you do not have to stop a profile run to edit the profile. However, when you make changes to profiles, the data that Mercury Business Availability Center collects reflects the changes that you make. Such changes may be significant when you are viewing performance data reports. Keep in mind that, if you choose to view a report for a time period during which changes were made to the profile, the significance of the data may be affected.

Changes in Your Organization

The following table describes typical changes that might occur in your organization, requiring you to modify profiles:

Type of Change	Description
Changes to your network	Changes to your network may require you to select different host machines on which to run scripts. Alternatively, if your network grows, you may want to add hosts to a Business Process profile.
Changes to your customer base	Changes to your customer base may require you to select different locations, which better reflect the geographical dispersion of your customers.

Type of Change	Description
Changes within your organization	Changes within your organization, such as opening or closing of branch offices, or restructuring of departments, may require you to select different data collectors and/or different Group settings for them.
Changes to your monitored application	Changes to your monitored application may require you to redefine or rerecord existing scripts to suit the changes to the application. Alternatively, if new features are added to the application, you may want to define or record new scripts that include these new URLs or business processes, and add them to the profile.
Changes to application performance monitoring priorities	Changes to application performance monitoring priorities—due to changes in application usage, competition, hardware or software improvements, and so forth—may require you to modify your profiles. For example, you may decide that a particular transaction in your profile no longer reflects a typical or commonly used business process in your application. In such a case, you may want to remove the transaction from the profile and replace it with a more relevant one.

Editing Profile or Monitor Properties

Any of the changes mentioned above may necessitate making changes to the objects defined in your monitor tree.

These can also include those properties that are native to Monitor Administration, including categories. For details, see "Setting Views and Defining Categories" in *Working with Monitor Administration*.

To edit a profile or monitor:

1. Access the object's Edit page. For details, see "Accessing Object Properties for Editing" in *Working with Monitor Administration*.
2. Edit the properties of the object as required.

Note: After changing a profile name, it may be necessary for users viewing the trend reports for that profile to log in to Mercury Business Availability Center again.

---

3 Click **OK** to save your new settings or **Cancel** to disregard any changes.

Working with Business Process Profiles and Transaction Monitors

Once your profiles and monitors are added to the monitor tree, you can perform various functions in Monitor Administration, including:

- Managing Alerts and Recipients (for details, see next section)
- Creating and Assigning Downtime/Event Schedules to Profiles (for details, see page 67)
- Replicating Profiles and Monitors (for details, see page 67)
- Assigning Data Collector Locations to Monitors (for details, see page 68)
- Starting and Stopping Business Process and Client Monitor Profiles (for details, see page 69)

Managing Alerts and Recipients

Once you have set up your profiles and monitors, you can create alerts schemes for those profiles to inform users when predefined performance limits are breached.

You can define alert schemes for your profiles by choosing **Alerts Management** from the Business Process profile menu (right-click a profile in the monitor tree) or in the Contents page under the list of Business Process profiles. The Alerts Management page opens listing all the alerts configured for the selected profile. To a create a new alert scheme for the profile, click **New Alert**.

For details on configuring alert schemes, see "Creating Alert Schemes" and for details on defining recipients to receive alerts, see "Configuring and Selecting Recipients" in *Platform Administration*.

Creating and Assigning Downtime/Event Schedules to Profiles

You may want to exclude periods of time in which downtime or other events may skew the results of collecting data for reports and in Dashboard status. You can define downtime or event schedules for when Mercury Business Availability Center is automatically instructed not to run the profiles. You may want to base a downtime schedule on a recurring maintenance event or a holiday.

You can assign multiple profiles to one downtime/event schedule. In Monitor Administration, you access the Downtime/Event Scheduling page while editing or adding a profile. In the Main Settings area of the profile properties page, click the **Downtime/Event Scheduling** link.

For details on creating and managing downtime/event schedules, see "Defining Downtime and Other Influencing Events" in *Platform Administration*.

Replicating Profiles and Monitors

You can use Monitor Administration to replicate configuration settings for profiles and monitors.

To copy and paste:

1. In the monitor tree, right-click the profile or monitor whose configurations you want to replicate. The item's menu opens.
2. Select **Copy**. The message in the info area indicates whether the copy has been successful.

3 Right-click the item into which you want to paste the configuration settings and select **Paste** from the action menu.

- ➤ You can paste a profile directly into the enterprise node or into a container.
- ➤ You can paste a monitor's configurations only into an existing profile.

The profile or monitor appears in the monitor tree with duplicated configuration settings.

4 To edit the name or any other settings, right-click the object in the monitor tree and select **Edit**.

Assigning Data Collector Locations to Monitors

You can assign monitors that have been added to a profile to run on selected data collector locations. You can do this per data collector location, using the Data Collectors tab (for details, see "Host Assignment Settings" on page 48) or per monitor as described here.

To assign data collector locations per monitor:

1 In Monitor Administration, click the **Contents** tab.

2 Within the contents tab, navigate to the monitor that you want to assign to run on one or multiple data collector locations.

3 Under the **Assigned Locations** column, click the link of the list of locations currently running the monitor.

The Assign Host dialog box opens.

4 Select the data collector host locations on which you want to run the selected monitor. For Client Monitor Profile transaction monitors, select the check boxes next to the Client Monitor containers or groups on which you want to run the selected monitor. For Business Process Profile transaction monitors, select the Business Process Monitor instances from the **Available Host Locations** list, and use the upper arrow to move your selection(s) to the **Assigned Host Locations** list. You can select multiple locations using the CTRL key.

5 Click **Assign** to confirm your selections and close the Assign Host Locations dialog box.

Starting and Stopping Business Process and Client Monitor Profiles

Monitor Administration enables you to begin running the profile and end the profile on the selected host machine or group.

Once you have created a profile, added to it a transaction monitor, and configured the schedule settings, Monitor Administration begins running the profile by default. To stop the profile run, right-click the profile and choose **Stop Profile** or highlight the profile and click the **Stop Profile** button in the Contents tab. To begin running the profile again, choose **Start Profile**.

3

Configuring the Real User Monitor

After you install a Mercury Real User Monitor engine and probe, you must configure Real User Monitor in Monitor Administration to begin the monitoring process.

About Real User Monitor

After having installed a Mercury Real User Monitor engine and probe (for details, see *Real User Monitor Administration*) you must configure Real User Monitor in Monitor Administration to be able to monitor applications and end-users.

The settings you configure in Monitor Administration are used by the Mercury Real User Monitor engine to collect and process real-time data from the Real User Monitor probes. By comparing this data to pre-defined thresholds, Mercury Business Availability Center is able to pinpoint performance related issues as experienced by end-users. You use Real User Monitor reports to help identify the cause of delays and determine the business impact of performance issues experienced by end-users. For details on Real User Monitor reports, see "Real User Monitor Reports" in *Using End User Management*.

You use Monitor Administration to:

1 Add a Real User Monitor engine. This includes configuring:

- ➤ the engine – see page 74
- ➤ general settings – see page 77
- ➤ probes – see page 85
- ➤ global HTTP error events – see page 86
- ➤ server names – see page 88
- ➤ host aliases – see page 90

2 Define applications to be monitored. This includes configuring:

- ➤ applications – see page 91
- ➤ application events – see page 107
- ➤ page containers – see page 99
- ➤ pages – see page 99
- ➤ page events – see page 107
- ➤ transaction containers – see page 103
- ➤ transactions – see page 103

3 Create end-user groups to be monitored. This includes configuring:

- ➤ end-user group containers – see page 114
- ➤ end-user groups – see page 114

You use the monitor tree to navigate through containers and elements in the tree structure and drill down to monitor and other configuration settings. For details on the different hierarchy elements, see "Using Monitor Administration" in *Working with Monitor Administration*.

While there are several ways to perform actions and edit object properties, the method described in this document is that of highlighting an object in the monitor tree and right-clicking it to access a menu of options valid for that object. For details on the different ways to perform actions and edit object properties, see "Navigating and Performing Actions in the Contents Tab and the Monitor Tree" in *Working with Monitor Administration*.

You can customize your view of the enterprise tree to list only those elements with which you are working. You can also assign categories to your profiles and monitors to further refine your views. For details, see "Setting Views and Defining Categories" in *Working with Monitor Administration*.

In addition, Monitor Administration enables you to change configurations across multiple profiles and monitors using **Global Replace**. For details, see "Using Global Replace" in *Working with Monitor Administration*.

Note:

- ➤ Real User Monitor does not support I18N. This means that all data input for configuration and processing must be made using English language characters only.
- ➤ The ability of a user to configure Real User Monitor engines, general settings, applications, pages, transactions, events, and end-user groups is dependent on the access permissions granted that user. For details on granting permissions, see "Configuring User Permissions" in *Platform Administration*.

Adding a Real User Monitor Engine

To configure an engine you installed for real-user monitoring, you must add it to the monitor tree in Monitor Administration. Once added, you can view or edit the properties of the engine, or delete the engine from the monitor tree.

To add a Real User Monitor engine to the monitor tree:

1. Right-click **Enterprise** and select **New Real User Monitor Engine**.
2. On the New Real User Monitor Engine page, under **Main Settings**, enter the following:
   - the name of the Real User Monitor engine machine (note that this field is limited to 100 characters)
   - a description of the machine, which you can view in Monitor Administration only (note that this field is limited to 260 characters)
   - the Real User Monitor engine machine's IP address
   - whether you want the Real User Monitor engine to report data for defined applications only, or for all applications. A probe gathers data for all the applications that pass through it, but you can limit the amount of data reported by the probe by defining specific applications for the probe to report. For details on defining applications, see "Configuring Applications" on page 91.
3. On the New Real User Monitor Engine page, under **Probe Settings**, enter the following:
   - the name of a probe machine (note that the probe name must be unique within the Real User Monitor engine you are adding and must not exceed 100 characters)
   - a description of the probe machine, which you can view in Monitor Administration only (note that this field is limited to 260 characters)
   - the probe machine's IP address
   - a user name for accessing the probe machine
   - a password for accessing the probe machine

Note: The user name and password for accessing the probe must be the same as those configured during the probe installation. For details on installing the probe machine, see "Installing the Real User Monitor Probe" in *Real User Monitor Administration*.

Note: You can disable the probe from monitoring temporarily, while keeping its configuration. For example, you may want to disable a probe from monitoring if you are expecting heavy network traffic which is of no particular interest to you, during a certain period of time.

To disable the probe from monitoring, clear the **Enable** check box.

---

4 If SSL is configured on the Real User Monitor engine machine, you must define the **Real User Monitor engine URL** setting, located on the Real User Monitor Engine definition page, under **Advanced Settings**.

To define the URL, enter the https protocol, together with the host name of the machine on which the Real User Monitor engine resides (an IP address cannot be used), and the port number (the default port is 443).

Example: **https://myenginemachinename:443**

5 On the New Real User Monitor Engine page, under **Category Settings**, you can assign a category to the Real User Monitor engine for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.

6 Click **OK** at the bottom of the page. The Real User Monitor engine you defined is added to the monitor tree.

To view the properties of the engine:

To view configured settings for an engine, click the engine name in the monitor tree and click the **Properties** tab.

Note: For information on the Contents tab, see "Navigating and Performing Actions in the Contents Tab and the Monitor Tree" in *Working with Monitor Administration*.

To edit the properties of the engine:

To edit the properties of an existing Real User Monitor engine, right-click the engine in the monitor tree and select **Edit**. On the Edit Real User Monitor Engine page, edit the settings as required. Note that you cannot edit the engine name.

Note: The Probe Settings pane that is displayed when adding a Real User Monitor engine to the monitor tree is not available when editing the properties of the engine. For details on editing probe settings, see "Configuring a Probe" on page 85.

To delete the engine from the monitor tree:

To delete a Real User Monitor engine from the monitor tree, right-click the engine and select **Delete**.

Configuring Real User Monitor Engine Settings

To begin monitoring real-user traffic using Real User Monitor, you must add and configure the probes that will collect the real-user data. In addition, you can define server names and host aliases.

You can also configure general monitoring settings for all pages, applications, transactions, servers, and end-users being monitored by the engine, as well as events and HTTP errors used to report errors and events.

This section describes:

- Configuring a Probe – see page 85
- Defining HTTP Global Error Events – see page 86
- Defining a Server Name – see page 88
- Defining a Host Alias – see page 90

Note: When you click the **Engine Settings** object, the Engine Settings Contents tab is displayed. For information on the Contents tab, see "Navigating and Performing Actions in the Contents Tab and the Monitor Tree" in *Working with Monitor Administration*.

Configuring General Settings

To view the default page, transaction, server availability, end-user latency, data reporting, broken link referral, and session reset settings, click the **General Settings** object in the monitor tree. The default settings are displayed in the Properties tab.

To modify the default settings, click the **Edit** button at the bottom of the Properties tab, or right-click the **General Settings** object and select **Edit**. The Edit Real User Monitor General Settings page opens, displaying the following sections and editable fields:

- Page Settings – see page 78
- Transaction Settings – see page 79
- Server and End User Group Settings – see page 80
- Data Reporting Settings – see page 81
- Broken Link Referral Settings – see page 83
- Session Reset Settings – see page 84

Page Settings

In the Page Settings section, you can configure the default threshold settings that are displayed when you configure a new Page in Real User Monitor. Note that the page time and server time you enter here are those displayed by default when you configure a new application in Real User Monitor.

Page Setting	Explanation
Page Time (seconds)	Configure, in seconds, the page download time threshold. If a page is downloaded within this amount of time, its page time is displayed in green in the Real User Monitor reports. If the page is not downloaded within this amount of time, its page time is displayed in red in the Real User Monitor reports.
Server Time (seconds)	Configure, in seconds, the server time threshold for the page. If the server time for a page falls within this threshold, the page's server time is displayed in green in the Real User Monitor reports. If the server time for a page does not falls within this threshold, the page's server time is displayed in red in the Real User Monitor reports. Note that the server time threshold must be lower than the page download time threshold.
Availability (%)	Configure, in percent, the page availability threshold. If the availability of a page falls within this threshold, the page's availability is displayed in green in the Real User Monitor reports. If the availability of a page does not fall within this threshold, the page's availability is displayed in red in the Real User Monitor reports.
Timeout (seconds)	Configure, in seconds, the amount of time after which Real User Monitor considers the downloading of a page's components to have timed out.

Transaction Settings

In the Transaction Settings section, you can configure the default threshold settings that are displayed when you configure a new Transaction in Real User Monitor.

Transaction Setting	Explanation
Total Time (seconds)	Configure, in seconds, the total transaction time (download time + think time) threshold. If the total time of a transaction falls within this threshold, the transaction's total time is displayed in green in the Real User Monitor reports. If the total time of a transaction does not fall within this threshold, the transaction's total time is displayed in red in the Real User Monitor reports.
Net Time (seconds)	Configure, in seconds, the net transaction time (which you define when you configure a transaction—see "Configuring Transactions" on page 103 for details) threshold. If the net time of a transaction falls within this threshold, the transaction's net time is displayed in green in the Real User Monitor reports. If the net time of a transaction does not fall within this threshold, the transaction's net time is displayed in red in the Real User Monitor reports.
Server Time (seconds)	Configure, in seconds, the server time threshold for the transaction. If the server time for a transaction falls within this threshold, the transaction's server time is displayed in green in the Real User Monitor reports. If the server time for a transaction does not fall within this threshold, the transaction's server time is displayed in red in the Real User Monitor reports. Note that this threshold must be lower than the total time and net time thresholds.

Transaction Setting	Explanation
Availability (%)	Configure, in percent, the transaction availability threshold. If the availability of a transaction falls within this threshold, the transaction's availability is displayed in green in the Real User Monitor reports. If the availability of a transaction does not fall within this threshold, the transaction's availability is displayed in red in the Real User Monitor reports.
Timeout (seconds)	Configure, in seconds, the amount of time after which Real User Monitor considers the downloading of a page within a transaction to have timed out.

Server and End User Group Settings

In the Server and End-User Group Settings section, you can configure the server availability threshold for all servers, as well as the default latency threshold setting that is displayed when you define a new end-user group.

Setting	Explanation
Server Availability (%)	Configure, in percent, the server availability threshold. If the availability of a server falls within this threshold, the server's availability is displayed in green in the Real User Monitor reports. If the availability of a server does not fall within this threshold, the server's availability is displayed in red in the Real User Monitor reports.
Latency (milliseconds)	Configure, in milliseconds, the average network latency threshold for each end-user within an end-user group subnet. If the latency of an end-user falls within this threshold, the end-user's latency is displayed in green in the Real User Monitor reports. If the average network latency of an end-user does not fall within this threshold, the end-user's latency is displayed in red in the Real User Monitor reports.

Data Reporting Settings

In the Data Reporting Settings section, you can configure the collection parameters for the following global statistics:

Global Statistics Setting	Explanation
Snapshot on Event	Configure the maximum number of previous, session pages that you want the Real User Monitor to report when a page with an error or event is encountered (including the page with the error or event itself). To instruct Real User Monitor not to collect this information, clear the Snapshot on Event check box.
Most Popular Pages	Configure the maximum number of most popular pages—that is, the pages that received the highest number of end-user requests (hits)—you want Real User Monitor to collect per hour. To instruct Real User Monitor not to collect this information, clear the Most Popular Pages check box. **Note:** A maximum number of 100 most popular pages can be collected.
Most Active End Users	Configure the maximum number of most active end-users you want Real User Monitor to collect per hour. You can define whether activity is measured by the number of page requests, or the amount of bandwidth used. To instruct Real User Monitor not to collect this information, clear the Most Active End Users check box. **Note:** A maximum number of 100 most active end-users can be collected.

Global Statistics Setting	Explanation
Slowest End Users	Configure the maximum number of slowest end-users—that is, the end-users whose average network latency was highest—you want Real User Monitor to collect during each five-minute period. You can define the minimum number of hits required for an end-user's data to be collected. To instruct Real User Monitor not to collect slowest end-user data, clear the Slowest End Users check box. **Note:** A maximum of 50 slowest end-users can be collected. The minimum number of hits required cannot exceed 10,000.
Slowest Pages	Configure the maximum number of slowest pages—that is, the pages that took the greatest amount of time to download—you want Real User Monitor to collect during each five-minute period. You can define the minimum number of hits required for a page's data to be collected. To instruct Real User Monitor not to collect slowest pages data, clear the Slowest Pages check box. **Note:** A maximum of 50 slowest pages can be collected. The minimum number of hits required cannot exceed 10,000.
Pages with Most Errors	Configure the maximum number of pages with most errors—that is, the pages on which the greatest number of HTTP and application errors occurred—you want Real User Monitor to collect during each five-minute period. You can define the minimum number of hits required for a page's data to be collected. To instruct Real User Monitor not to collect pages with most errors data, clear the Pages with Most Errors check box. **Note:** A maximum of 20 slowest pages can be collected.

Broken Link Referral Settings

In the Broken Link Referral Settings section, you can configure the number of broken links that Real User Monitor collects in a given time period and define the hosts from which Real User Monitor collects broken link data.

Broken Link Referral Setting	Explanation
Broken Links	Configure the maximum number of broken links you want Real User Monitor to collect during each five-minute period. To instruct Real User Monitor not to collect broken link data, clear the Broken Links check box. **Note:** A maximum number of 50 broken links can be collected.
Referring Host Name(s)	Define the host names from which to report broken link data. If a user clicks a link on a page from one of these hosts and the link is broken, the broken link data is collected by Real User Monitor. If a user clicks a link on a page from a host that is not defined in this section, the data is ignored by Real User Monitor.

Note: By default, no broken link referral settings are defined. Unless you define hosts in this section, no broken link data will be collected and no data will be displayed in the Broken Links table in the Global Statistics report.

To define a Referring Host:

To define a referring host, click the New Referring Host Name(s) button and enter, in the text box displayed, the host machine from which you want to monitor broken links. Note that you need only enter the host part of the URL – for example, mercury.co.jp.

To delete a Referring Host:

To delete a referring host that you added, select the check box to the left of the host and click the Delete button.

Session Reset Settings

In the Session Reset Settings section you can configure the parameters that will cause a session to be reported to Real User Monitor and a new session to be started.

For example, in a call center, such as directory enquiries for a telephone company, a default session for an operator may be from the log-in at the beginning of a shift to the log-out at the end of a shift. However, you may wish to report a separate session for each inquiry handled by the operator so you can set the Session Reset URL to the URL of the page that begins each new inquiry. Whenever that page is accessed, the previous session will be closed and reported and a new session will be opened.

The following are the session reset parameters that you can configure:

Session Reset Settings	Explanation
By Timeout	Configure the maximum time (in minutes) that a session can be open before it is reported to Real User Monitor and a new session is started.
Session Reset URL	Define the URLs which, when accessed, will cause the current session to be reported to Real User Monitor and a new session to be started.

To define a Session Reset URL:

To define a Session Reset URL, click on the **New Session Reset URL** button and, using the URL Builder (for details, see Using the URL Builder on page 119), define the URL that you want to include in the Session Reset URL list. Click **OK**. The URL appears in the Session Reset URL list.

To delete a Session Reset URL:

To delete a Session Reset URL that you added, select the check box to the left of the URL and click the **Delete** button.

Note: A session will be reported to Real User Monitor and a new session started if either of the session reset settings is encountered, or if the session ends normally.

Configuring a Probe

To begin the real-user monitoring process, you must configure at least one probe. The initial probe is configured when adding a new Real User Monitor engine to the monitor tree (for details, see "Adding a Real User Monitor Engine" on page 74), but additional probes can be added later. Once you have configured a probe, you can view the probe settings, edit the probe settings, or delete the probe from the monitor tree.

To configure a probe:

1. Right-click the **Probes** object in the monitor tree and select **New Probe**. The Real User Monitor New Probe page opens.
2. On the Real User Monitor New Probe page, under **Main Settings**, enter the following:
   - the name of a probe machine (note that the name must be unique and must not exceed 100 characters)
   - a description of the probe machine, which you can view in Monitor Administration only (note that this field is limited to 260 characters)
   - the probe machine's IP address
   - a user name for accessing the probe machine
   - a password for accessing the probe machine

Note: To disable the probe from monitoring, clear the **Enable** check box.

---

3 On the Real User Monitor New Probe page, under **Category Settings**, you can assign a category to the Real User Monitor probe for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.

4 Click **OK** at the bottom of the page. The Real User Monitor probe you defined is added to the monitor tree, under the Probes object.

To view probe settings:

In the monitor tree, click the probe whose settings you want to view. The configured settings are displayed in the Properties tab.

To edit settings for a probe:

In the monitor tree, right-click the probe whose settings you want to reconfigure and select **Edit**. On the Edit Real User Monitor Probe page, edit the probe's settings as required.

To delete a probe:

Right-click the probe in the monitor tree and select **Delete**.

Defining HTTP Global Error Events

You can define HTTP errors to be recorded by the Real User Monitor for reporting in Real User Monitor reports. For information on Real User Monitor reports, see "Real User Monitor Reports" in *Using End User Management*.

Note: When you click the **Global HTTP Error Events** object, the HTTP Error Events Contents tab is displayed. For information on the Contents tab, see "Navigating and Performing Actions in the Contents Tab and the Monitor Tree" in *Working with Monitor Administration*.

To define an HTTP global error event:

1 Right-click the **Global HTTP Error Events** object in the monitor tree and select **New Global HTTP Error Event**. The New HTTP Error Event page opens.

2 On the New HTTP Error Event page, under **Main Settings**, enter the following:

- the name of the HTTP error event. For example, you can create an HTTP global error event called Database errors and include the applicable HTTP error codes for this.
- whether to create a snapshot for the event, if it occurs in an application for which snapshots are recorded (for details on defining applications, see "Configuring Applications" on page 91). By default, the **Create Snapshot for Event** check box is enabled. Clear the check box to disable snapshot creation.
- the HTTP error codes you want to include under the HTTP error event. To add more than one HTTP error code to the HTTP error event, click the **New Error Code** button for each additional HTTP error code you want to add. The HTTP error code must be a value between 400-599.

To delete an HTTP error code that you added, select the check box to the left of the error code and click the **Delete** button.

Note: To disable monitoring for the HTTP error event, clear the **Enable** check box.

Note: By default, the most common HTTP error codes are predefined under four global HTTP error events—Bad user request, Request not found, Request refused, and Server error. For details, see "HTTP Error Codes" in *Using End User Management*.

An HTTP error code cannot be included in more than one HTTP error event within the same Real User Monitor engine.

---

3 On the New HTTP Error Event page, under **Category Settings**, you can assign a category to the HTTP Error Event for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.

4 Click **OK** at the bottom of the page. The HTTP error event you defined is added to the monitor tree, under the Global HTTP Error Events object.

To view HTTP global error event settings:

In the monitor tree, click the HTTP error event whose settings you want to view. The configured settings are displayed in the Properties tab.

To edit settings for an HTTP global error event:

In the monitor tree, right-click the HTTP error event whose settings you want to reconfigure and select **Edit**. On the Edit HTTP Error Event page, edit the error event's settings as required.

To delete an HTTP global error event:

Right-click the HTTP error event in the monitor tree and select **Delete**.

Defining a Server Name

You can define a server name for each IP address that is being monitored, which will appear in the Real User Monitor reports, thereby making them more meaningful. Once a server name has been defined, you can view the server name settings, edit the server name, or delete the server name from the monitor tree.

Note: When you click the **Server Names** object, the Server Names Contents tab is displayed. For information on the Contents tab, see "Navigating and Performing Actions in the Contents Tab and the Monitor Tree" in *Working with Monitor Administration*.

To define a server name:

1 Right-click the **Server Names** object in the monitor tree and select **New Server Name**. The New Server Name page opens.

2 On the New Server Name page, under **Main Settings**, enter the following:

- the server name you want to assign the server (note that the server name must be unique and must not exceed 100 characters)
- a description of the server which you can view in Monitor Administration only (note that the description must not exceed 260 characters)
- the IP address of the server you are defining

3 On the New Server Name page, under **Category Settings**, you can assign a category to the Server Name for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.

4 Click the **OK** button at the bottom of the page. The server name you defined is added to the monitor tree, underneath the Server Names object.

To view server name settings:

In the monitor tree, click the server name whose settings you want to view. The configured settings (IP address and description) are displayed in the Properties tab.

To edit settings for a server name:

Right-click the server name in the monitor tree and select **Edit**. On the Edit Server Name page, edit the server name settings as required.

To delete a server name:

Right-click the server name in the monitor tree and select **Delete**.

Defining a Host Alias

For analysis purposes, it is often helpful to group several hosts and monitor these hosts together, as a unit. This enables you to monitor pages that are located on multiple servers as the same page and view them as such in the Real User Monitor reports. For example, if your organization has different Web sites in a number of countries, each showing similar information such as company profile, events, products, and so forth, you could create a host alias for all of the required pages so that they would appear as one unit in the Real User Monitor reports. The host unit is known as a host alias, which you can define on the New Host Alias page. Once a host alias has been defined, you can view the host alias settings, edit the host alias, or delete the host alias from the monitor tree.

Note: When you click the **Host Aliases** object, the Host Aliases Contents tab is displayed. For information on the Contents tab, see "Navigating and Performing Actions in the Contents Tab and the Monitor Tree" in *Working with Monitor Administration*.

To define a host alias:

1. Right-click the **Host Aliases** object in the monitor tree and select **New Host Alias**. The New Host Alias page opens.
2. On the New Host Alias page, under **Main Settings**, enter the name you want to assign to the host alias (note that the name you enter must be unique within the Real User Monitor engine and must not exceed 100 characters.)
3. On the New Host Alias page, under **Hosts**, click the **New Hosts** button and enter the host part of the URL that you want to include in the host alias you are defining (for example, **mercury.co.jp**.) Repeat this step for each host you want to include in the host alias unit. Note that each host you enter must be unique.

To delete a host from the host alias unit, select the check box to the left of the host and click the **Delete** button.

4 On the New Host Alias page, under **Category Settings**, you can assign a category to the host alias for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.

5 Click the **OK** button at the bottom of the page. The host alias you defined is added to the monitor tree, underneath the Host Aliases object.

To view host alias settings:

In the monitor tree, click the host alias whose settings you want to view. The host alias settings are displayed in the Properties tab.

To edit settings for a host alias:

Right-click the host alias in the monitor tree and select **Edit**. On the Edit Host Alias page, edit the host alias' settings as required.

To delete a host alias:

Right-click the host alias in the monitor tree and select **Delete**.

Configuring Applications

Real User Monitor organizes the data it collects according to applications, which you define. For each application you define, you stipulate the application servers and URLs that you want to associate with the application.

Once you configure an application, you can configure the pages, transactions and events for which you want to collect specific data. For details on configuring pages, see page 99. For details on configuring transactions, see page 103. For details on configuring events, see page 107.

Once an application has been configured, you can view the application, edit the application, delete the application from the monitor tree, or copy and paste the application to a different Real User Monitor engine in the monitor tree.

Note: When you click the **Applications** object, or the name of the application in the monitor tree, the Applications, or specific application's Contents tab is displayed. For information on the Contents tab, see "Navigating and Performing Actions in the Contents Tab and the Monitor Tree" in *Working with Monitor Administration*.

To configure an application:

1. Right-click the **Applications** object in the monitor tree and select **New Application**. The New Application page opens.
2. On the New Application page, under **Main Settings**, enter the following:
   - the name you want to assign the application. Note that the name you enter must be unique and must not exceed 100 characters.
   - the probe(s) to be used in monitoring the application. Use the Ctrl key to select multiple probes, or choose **All** to select all the probes within the Real User Monitor engine.
   - clear the **Enable Application Clickstream** check box if you do not want snapshots of the pages and related events included in the application to be recorded. This means that snapshots of the pages and events will not be available for viewing in the Session Analyzer report (for details on viewing snapshots in the Session Analyzer report, see "Session Analyzer Report" in *Using End User Management*).
   - the page time threshold to be used as default for all pages being monitored as part of the application.
   - the server time threshold to be used as default for all pages being monitored as part of the application.

Note: To disable monitoring for the application, clear the **Enable** check box.

---

3 On the New Application page, under **Application Location Settings**, you define the IP ranges of the application servers, or the URLs in which the application resides.

➤ To stipulate the application servers and ports to be associated with the application you are defining, click the **New** button to enter the IP address, or IP range, of application servers you want to associate with the application you are defining and the port, or port range that the application server is using. Repeat this procedure for each application server you want to add.

A single IP address, or port number should be entered as is and ranges should be separated by a dash (-). For example, a range of IP addresses is entered as **110.132.10.96-110.132.10.99**.

Note: Do not associate an application server with more than one application otherwise it will not be associated with any of the applications you define.

To delete an application server from the list, select the check box to the left of the IP address and click the **Delete** button.

➤ To stipulate the URLs to be associated with the application you are defining, click the **New Application URL** button and, using the URL Builder (for details, see Using the URL Builder on page 119), define a URL that you want to associate with the application you are defining. Click **OK**. The URL appears in the list of Application URLs. Repeat this procedure for each URL you want to add to the list.

Note: Do not include a URL in more than one application otherwise it will not be associated with any of the applications you define.

To delete a URL from the list, select the check box to the left of the site and click the **Delete** button.

4 On the New Application page, under **User Name Detection**, you stipulate where to search for a user name in the application you are defining so that the data for the sessions associated with the application will contain the names of the session users (or their IP addresses, if you select this option). To configure user name detection, enter the following:

- from the **Search in** box, select the string in which you want Real User Monitor to locate the user name: **All Parameters, HTTP header**, **Content**, **IP address** or **Parameter** (for a single parameter). If you select HTTP header, or Content, enter the specific HTML tag, or header parameter within which the user name can be located.
- the strings between which the user name can be located. Note that if you selected **IP address**, these text boxes are irrelevant and are greyed out.
- for more advanced string specification methods, click the **Advanced** button. In the **Scan for (Regular Expression)** box, enter the regular expression that represents the string within which you want Real User Monitor to locate the user name. In the **Retrieve** box, enter the phrase representing the object(s) to be matched. For example, enter <h[^>]*>[W,w]elcome, (.*?)</h[^>]> in the **Scan for** box and user_($1) in the Retrieve box if you want Real User Monitor to retrieve user_bob from the following HTML tag:

  <h1>Welcome, bob</h1>

  Click **OK** to save your settings and close the Advanced String Location dialog box.

Note: You can test your expression by entering text in the **Test your expression here** box and clicking the **Test** button. A message is displayed as to whether or not a match was made, and if so, the retrieved value is also displayed.

➤ the pages within which you want Real User Monitor to search for the user name. You can instruct Real User Monitor to scan all pages associated with the application, or you can define specific login pages for Real User Monitor to scan. To define a login page, click the **New Login Page URL** button and, using the URL Builder (for details, see Using the URL Builder on page 119), define the URL that you want to include in the Login Pages list. Click **OK**. The page appears in the Login Page URL list.

To delete a page from this list, select the check box to the left of the page and click the **Delete** button.

Note: For more efficient performance, it is recommended to configure specific login pages to be searched rather than configuring Real User Monitor to search all pages.

➤ select **Use name translation file** if you want Real User Monitor to translate the user name it locates.

A name translation file called **Login_Users.csv** must be created in the **<Real User Monitor engine root directory>\conf\resolver** directory on the Real User Monitor engine machine. A sample of the Login_Users.csv file that can be copied is located in the **<Real User Monitor engine root directory>\conf\resolver\samples** directory.

To add a user to the **<Real User Monitor engine root directory>\conf\resolver\Login_Users.csv** file, edit the file, and enter the user's login name in the first column and the user's real name in the second column.

Note: It is recommended that you select this option if you choose **IP address** in the **Search in** box. Otherwise, the user name will be reported only as an IP address.

---

5 On the New Application page, under **Session Identification**, you configure where to search for the session ID of the application you are defining. To configure session identification, enter the following:

- ➤ from the **In application type** box, select the application type that is the same as, or similar to, the type of application you are defining. The parameter in which Real User Monitor will search for the session ID is automatically displayed.
- ➤ if the application you are defining does not match one of the default types listed in the **In application type** box, select User defined application to stipulate your own session identification parameters.

  In the **Search for session id in** box, enter the name of the parameter in which the session ID is located. This parameter will be searched for in Header fields, Parameters and Content tags.

  In **Between** and **and**, you can enter strings within the parameter between which the session ID is located, if applicable.

  For more advanced string specification methods, click the **Advanced criteria** button. Using the Advanced Finding and Retrieving dialog box (for details, see step 4), define the regular expression you wish to use for locating the session ID.
- ➤ to instruct Real User Monitor to search additional parameters if the session ID is not found in the initial parameter defined, click the **New** button and enter the required parameter settings.

6 On the New Application page, under **Page Names Configuration**, you can specify an XML file to be used by the application to assign meaningful names to pages that have not been configured in monitor administration. You can select an existing file that is available for the application from the dropdown list, or select **user defined** from the dropdown list and enter a new file name in the adjacent field. Note that the full file name including the extension (.xml) must be entered. The files are located on the Real User Monitor engine machine in the **<MercuryRUM>\conf\resolver\meaningful_pages** directory.

For details on assigning meaningful names to pages and configuring an XML file, see "Configuring Meaningful Page Names" in *Real User Monitor Administration*.

7 On the New Application page, under **Snapshot Collection Settings**, enter the following:

➤ check the **Snapshot on Event** box to enable snapshots to be made of pages on which events that have been configured for snapshots occur. Clear the check box to disable snapshots of event pages in the application.

➤ if the **Snapshot on Event** check box is enabled, enter the number of pages back for which snapshots should be made when an event occurs, including the event page itself.

➤ in the **Snapshot on Transaction Detection** section, configure a transaction snapshot collection schedule. Transaction snapshots can be viewed when displaying session details in the Session Analyzer report (for details, see "Session Analyzer Report" in *Using End User Management*), and are used to include the monitored real-user transactions in a VuGen script generated from the Business Process distribution Report (for details, see "Business Process Distribution Report" in *Using Application Performance Lifecycle*).

Select whether you want to collect transaction snapshots immediately, during a single interval or at various points throughout the monitoring process.

- **Run now.** If you select this option, specify the number of hours and minutes for which you want Real User Monitor to collect transaction snapshots.
- **Run every.** If you select this option, specify the day(s) of the week, as well as the time and duration, for which you want to schedule Real User Monitor transaction snapshot collection.

When transaction snapshot collection is configured, a significant amount of data is generated. Ensure that the duration for which transaction snapshots are collected is not excessive so that Real User Monitor is not overloaded.

8 On the New Application page, under **Advanced Settings**, enter the following:

- HTTP POST and/or GET parameters (such as password parameters) that you want to exclude from Real User Monitor for security reasons. These parameters will not appear on Real User Monitor reports, or anywhere else in Mercury Business Availability Center. Use semicolons to separate the parameters you enter in this box.
- HTTP POST and/or GET parameters (such as session ID, or time stamp) that Real User Monitor should ignore when assessing the pages that received the highest number of hits and are to be listed in the Global Statistics report's Most Popular Pages table. Use semicolons to separate the parameters you enter in this box.

9 On the New Application page, under **Category Settings**, you can assign a category to the application for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.

10 Click the **OK** button at the bottom of the page. The application you defined is added to the monitor tree, underneath the Applications object.

Note: If an application or session passes through more than one server, for example in the case of load balancing or server delegation, only the first server listed in the session will be reported.

If an application or session includes resources from more than one server, for example images in a page coming from a separate image server, these resources will not be correlated for statistical purposes as they do not contain the session identifier.

To view application settings:

In the monitor tree, click the application whose settings you want to view. The application settings are displayed in the Properties tab.

To edit settings for an application:

Right-click the application in the monitor tree and select **Edit**. On the Edit Application page, edit the application's settings as required.

To delete an application:

Right-click the application in the monitor tree and select **Delete**.

To copy and paste an application:

Right-click the application in the monitor tree and select **Copy**. To paste the application, right-click the object to which you want to copy the application and select **Paste**. A copy of the application appears in the monitor tree.

Note: An application can be copied from one Real User Monitor engine to another, but cannot be copied within the same Real User Monitor engine.

Configuring Pages

To collect data for specific pages that are a part of the application you want to monitor, you must first define these pages and configure monitoring settings for them. You can choose to create containers within which to categorize the pages you define, or you can define pages directly under the Pages object. To manage pages more efficiently, it is recommended to group pages in an application and create a container for each group. There should not be more than 200 pages in any one container.

Once you configure a container, or page, you can configure the events for which you want to collect specific data. For details on configuring events, see page 107.

Once a container, or page, has been configured, you can view the page, or container settings, edit the page or container settings, delete the page or container from the monitor tree, or copy and paste the page or container in the monitor tree.

Note: When you click the **Pages** object, or the name of the page container in the monitor tree, the Pages, or page container Contents tab is displayed. For information on the Contents tab, see "Navigating and Performing Actions in the Contents Tab and the Monitor Tree" in *Working with Monitor Administration*.

To create a page container:

1. Right-click the **Pages** object, or an existing page container in the monitor tree and select **New Container**. The New Container page opens.
2. On the New Container page, under **Main Settings**, enter the name you want to assign the page container. Note that the name you enter must be unique and must not exceed 100 characters.
3. On the New Container page, under **Category Settings**, you can assign a category to the container for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.
4. On the New Container page, under **Advanced Settings**, enter a description of the group, which you can view in Monitor Administration only. Note that the description is limited to 260 characters.
5. Click the **OK** button at the bottom of the page. The page container you configured is added to the monitor tree, underneath the Pages object, or the page container within which you added it.

To configure a page to monitor:

1. In the monitor tree, right-click the **Pages** object, or the page container within which you want to define a page, and select **New Page**. The New Page page opens.
2. On the New Page page, under **Main Settings**, enter the following:
   - the name you want to assign the page. Note that the name you enter must be unique and must not exceed 100 characters. The page name can include the following special characters: ; : / ? = * & { } % @ + - $

- a description of the page, which you can view in Monitor Administration only. Note that the description you enter must not exceed 260 characters.
- the monitoring condition for the page your are defining. From the **Monitoring conditions** box, select one of the following options:
  - **Always.** Instructs Real User Monitor to collect data for all requests of the page. This data appears in the Global Statistics and Page Summary reports.
  - **Never.** Instructs Real User Monitor not to collect data for the page. Data for this page will not appear in the Global Statistics, or Page Summary reports.
  - **Only as part of a transaction.** Instructs Real User Monitor to collect data for the page only if the page is included in a transaction. If the page is part of a transaction, data for it will appear in the Transaction Summary report. Data for the page will not appear in the Page Summary report.

➤ the URL of the page you want to monitor. To specify the URL, click the **URL Builder** button and, using the URL Builder (for details, see Using the URL Builder on page 119), configure a URL that you want to associate with the page you are defining. Click **OK** to save the URL settings you entered and return to the New Page page.

Note: To disable monitoring for the page, clear the **Enable** check box.

---

3 On the New Page page, under **Threshold Settings**, you can change the default page time, server time, availability, and timeout settings for the page you are defining. For information on these settings, see "Page Settings" on page 78.

4 On the New Page page, under **Configuration Item Attachment Settings**, you can attach a CI to this page. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a page to Monitor Administration and cannot be set while editing a page.

---

5 On the New Page page, under **Category Settings**, you can assign a category to the page for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.

6 Click the **OK** button at the bottom of the page. The page you configured is added to the monitor tree, underneath the Pages object, or the page container within which you added it.

Note: A maximum of 2000 pages can be configured for each engine.

To view settings for a page or page container:

In the monitor tree, click the page, or page container whose settings you want to view. The configured settings are displayed in the Properties tab.

To edit settings for a page or page container:

Right-click the page, or page container in the monitor tree and select **Edit**. On the Edit Real User Monitor Page, or Edit Page Container page, edit the page, or page conainer settings as required.

Note: If you change the name of a page, the Real User Monitor reports display data for the page under both the original and the new page names.

To delete a page or page container:

Right-click the page, or page container in the monitor tree and select **Delete**. Note that you cannot delete a page if it is part of a transaction.

To copy and paste a page or page container:

Right-click the page, or page container in the monitor tree and select **Copy**. To paste the page, or page container, right-click the object to which you want to copy the page, or page container and select **Paste**. If you are copying a page, a copy of the page with the name **<page name>.1** appears in the monitor tree. If you are copying a page container, a copy of the page container appears in the monitor tree (with each of the pages in the **<page name>.1** format).

Configuring Transactions

To collect specific data for specific transactions that are a part of the application you want to monitor, you must first define these transactions and configure monitoring settings for them. You can choose to create containers within which to categorize the transactions you define, or you can define transactions directly under the Transactions object.

Note: If an application does not include a session ID, it is possible that two or more simultaneous transactions originating from a single end-user may be reported by Real User Monitor as a single transaction.

Once a container, or transaction, has been configured, you can view the transaction or container settings, edit the transaction or container settings, delete the transaction or container from the monitor tree, or copy and paste the transaction or container in the monitor tree.

Note: When you click the **Transactions** object, or the name of the transaction container in the monitor tree, the Transactions Contents tab is displayed. For information on the Contents tab, see "Navigating and Performing Actions in the Contents Tab and the Monitor Tree" in *Working with Monitor Administration*.

To create a transaction container:

1. Right-click the **Transactions** object, or an existing transaction container in the monitor tree and select **New Container**. The New Container page opens.
2. On the New Container page, under **Main Settings**, enter the name you want to assign the transaction container. Note that the name you enter must be unique and must not exceed 100 characters.
3. On the New Container page, under **Category Settings**, you can assign a category to the container for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.
4. On the New Container page, under **Advanced Settings**, enter a description of the container, which you can view in Monitor Administration only. Note that the description is limited to 260 characters.
5. Click the **OK** button at the bottom of the page. The transaction container you configured is added to the monitor tree, underneath the Transactions object, or the transactions container within which you added it.

To configure a transaction to monitor:

1 In the monitor tree, right-click the **Transactions** object, or the transaction group within which you want to define a transaction and select **New Transaction**. The New Transaction page opens.

2 On the New Transaction page, under **Main Settings** enter the following:

- the name you want to assign the transaction. Note that the transaction name must be unique and must not exceed 100 characters.
- a description of the transaction, which you can view in Monitor Administration only. Note that the description is limited to 260 characters.

Note: To disable monitoring for the transaction, clear the **Enable** check box.

---

3 On the New Transaction page, under **Included Pages Settings**, select the individual pages and/or page containers that you want to include in the transaction you are defining, by clicking the check box to the left of the page, or page container in the Pages tree above. The selected pages (the individual pages and the pages within the page containers you selected) appear in the Pages Added list.

Note: You can select only pages that are part of the application for which you are creating a transaction.

To determine the order of pages within the transaction, use the **Up** and **Down** buttons. To delete a page, clear the check box to the left of the page in the Pages tree above.

4 On the New Transaction page, under **Threshold Settings** section, you can change the default total time, net time, server time, availability, and timeout settings. For information on these settings, see "Transaction Settings" on page 79.

5 On the New Transaction page, under **Advanced Settings**, you can set the following:

- **Report transaction if user reaches page.** Instructs Real User Monitor to report data for a transaction only if the transaction run includes the page you select. By configuring this setting, you filter transactions that are aborted before the user reaches the page(s) you really want to monitor. Note that, by default, this setting is set at the first page you added to the transaction.
- **Measure first/last page instance.** Instructs Real User Monitor to report data for either the first, or last instance of a page refresh. By default, data for the last page instance is reported.

6 On the New Transaction page, under **Configuration Item Attachment Settings**, you can attach a CI to this transaction. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a transaction to Monitor Administration and cannot be set while editing a transaction.

---

7 On the New Transaction page, under **Category Settings**, you can assign a category to the transaction for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.

8 Click the **OK** button at the bottom of the page. The transaction you configured is added to the monitor tree, underneath the Transactions object, or the transaction container within which you added it.

To view settings for a transaction or transaction container:

In the monitor tree, click the transaction, or transaction container whose configuration settings you want to view. The configured transaction settings are displayed in the Properties tab.

To edit settings for a transaction or transaction container:

Right-click the transaction, or transaction container in the monitor tree and select **Edit**. On the Edit Transaction, or Edit Transaction Container page, edit the transaction, or transaction container settings as required.

To delete a transaction or transaction container:

Right-click the transaction, or transaction container in the monitor tree and select **Delete**.

To copy and paste a transaction or transaction group:

Right-click the transaction, or transaction container in the monitor tree and select **Copy**. To paste the transaction, or transaction container, right-click the object to which you want to copy the transaction, or transaction container and select **Paste**. If you are copying a transaction, a copy of the transaction with the name **<transaction name>.1** appears in the monitor tree. If you are copying a transaction container, a copy of the transaction container appears in the monitor tree (with each of the transactions in the **<transaction name>.1** format).

Note: A transaction, or transaction container can only be copied within the same engine.

Configuring Events

To collect specific data for specific events that occur on pages that are a part of the application you want to monitor, you must first define these events and configure monitoring settings for them.

You can define events for an entire application, or for specific pages and page containers that are part of the application you want to monitor, depending on the type of event. If you are defining an event for a page container, the event will be applied to all pages contained within that page container. If you are defining an event for an application, the event will be applied to all pages contained within that application.

You can define an event to be reported in Real User Monitor Event reports as an error event, or as an informational event. By default, events are defined as informational events. For information on Real User Monitor reports, see "Real User Monitor Reports" in Using End User Management.

You can define the following types of events:

Text Pattern Events

Text pattern events can be defined for applications, or for pages and page containers that are part of an application you wish to monitor.

A text pattern event is triggered when a page includes, or fails to include, a defined string of characters.

To configure a Text Pattern event to monitor:

1. In the monitor tree, right-click the **Pages** object, the pages container, or the **Application** object within which you want to define a Text Pattern event and select **New Text Pattern Event**. The New Text Pattern Event page opens.
2. On the New Text Pattern Event page, under **Main Settings** do the following:
   - ➤ enter the name you want to assign the event (note that the event name must be unique and must not exceed 100 characters)
   - ➤ check the **Report as error** box if you want the event to be reported as an error event instead of an informational event
   - ➤ check the **Create Snapshot for Event** box to create a snapshot of the page on which the event occurs. The application in which the page is included must be configured for snapshot collection (for details on defining applications, see "Configuring Applications" on page 91).
   - ➤ in the **Search in** box select where on the page to search for the string of characters. You can choose from:
     - **Header.** Instructs Real User Monitor to look for the pattern in the page header. You can further define a specific field within the header in which to search.
     - **Get/post parameters.** Instructs Real User Monitor to look for the pattern in the get/post parameters. All the get/post parameters will be searched.

- **Content.** Instructs Real User Monitor to look for the pattern in the page content. You can further define a specific html tag within the content in which to search.

➤ under **Trigger an event for pages**, select whether you want the event to be triggered if the page includes the string of characters (**containing**), or if the page does not include the string of characters (**not containing**). In the **string** box, enter the specific string of characters to be searched for.

You can also specify a value to be retrieved from the page, which will be displayed in the Real User Monitor Event reports. To enable this option, check the box to the left of the option and then specify the expressions on the page between which the value is located. This option is valid only if a value is found on the page where specified. The option works in conjunction with the main **Trigger an event for pages** option so that both conditions must be met for the event to be triggered.

For example, an HTML Web page that contains the window title **Mercury Business Availability Center** includes the following line:

<title>Mercury Business Availability Center</title>

If you wish to trigger an event for this page and extract the text **Mercury Business Availability Center** for inclusion in the Real User Monitor Event reports, you configure the event to be triggered for pages **containing** the string **title** and containing any value between the expressions **<title>** and **</title>**.

For more advanced string specification methods, click the **Advanced criteria** button. Using the Advanced Finding and Retrieving dialog box, (for details, see step 4 in the procedure for configuring an application on page 92), define the regular expression you wish to use for locating the required string.

Note: To disable monitoring for the event, clear the **Enable** check box.

---

3 On the New Text Pattern Event page, under **Category Settings**, you can assign a category to the text pattern event for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.

4 Click the **OK** button at the bottom of the page. The text pattern event you configured is added to the monitor tree, underneath the Page object, page container, or Transactions object within which you added it.

Page Size Events

Page size events can be defined for pages and page containers that are part of an application you wish to monitor.

A page size event is triggered when a page size is either greater than or less than a defined number of kilobytes.

To configure a Page Size event to monitor:

1 In the monitor tree, right-click the **Pages** object, or the pages container within which you want to define a Page Size event and select **New Page Size Event**. The New Page Size Event page opens.

2 On the New Page Size Event page, under **Main Settings** enter the following:

- the name you want to assign the event. Note that the event name must be unique and must not exceed 100 characters.
- check the **Report as error** box if you want the event to be reported as an error event instead of an informational event.
- in the **Trigger event when page size** box, select either greater than (>), or less than (<) and then enter the page size in kilobytes in the adjacent box.

Note: To disable monitoring for the event, clear the **Enable** check box.

---

3 On the New Page Size Event page, under **Category Settings**, you can assign a category to the page size event for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.

4 Click the **OK** button at the bottom of the page. The page size event you configured is added to the monitor tree, underneath the Page object, or page container within which you added it.

Session Failed Pages Events

Session failed pages events can be defined for applications you wish to monitor.

A session failed pages event is triggered when a session in an application includes a defined number of unavailable pages.

To configure a Session Failed Pages event to monitor:

1. In the monitor tree, right-click the **Application** object within which you want to define a Session Failed Pages event and select **New Session Failed Pages Event**. The New Session Unavailable Pages Event page opens.
2. On the New Session Unavailable Pages Event page, under **Main Settings** enter the following:
   - the name you want to assign the event. Note that the event name must be unique and must not exceed 100 characters.
   - check the **Report as error** box if you want the event to be reported as an error event instead of an informational event.
   - the number of unavailable pages which, when reached, will trigger the event.

Note: To disable monitoring for the event, clear the **Enable** check box.

---

3. On the New Session Unavailable Pages Event page, under **Category Settings**, you can assign a category to the session failed pages event for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.
4. Click the **OK** button at the bottom of the page. The session failed pages event you configured is added to the monitor tree, underneath the Transaction object within which you added it.

Session Pages Events

Session pages events can be defined for applications you wish to monitor.

A session pages event is triggered when a session in an application includes a defined number of pages.

To configure a Session Pages event to monitor:

1. In the monitor tree, right-click the **Application** object within which you want to define a Session Pages event and select **New Session Pages Event**. The New Session Pages Event page opens.
2. On the New Session Pages Event page, under **Main Settings** enter the following:
   - the name you want to assign the event. Note that the event name must be unique and must not exceed 100 characters.
   - check the **Report as error** box if you want the event to be reported as an error event instead of an informational event.
   - the number of pages which, when reached, will trigger the event.

Note: To disable monitoring for the event, clear the **Enable** check box.

---

3. On the New Session Pages Event page, under **Category Settings**, you can assign a category to the session pages event for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.
4. Click the **OK** button at the bottom of the page. The session pages event you configured is added to the monitor tree, underneath the Transaction object within which you added it.

Error Page Events

Error page events can be defined for applications you wish to monitor.

An error page event is triggered when a specified page in an application encounters an error.

To configure an Error Page event to monitor:

1. In the monitor tree, right-click the **Application** object within which you want to define an Error Page event and select **New Error Page Event**. The New Error Page Event page opens.
2. On the New Error Page Event page, under **Main Settings** enter the following:
   - the name you want to assign the event. Note that the event name must be unique and must not exceed 100 characters.
   - check the **Report as error** box if you want the event to be reported as an error event instead of an informational event.
   - the URL of the page which, if an error is encountered, will trigger the event. To specify the URL of the page, click the **URL Builder** button and, using the URL Builder (for details, see Using the URL Builder on page 119), define the URL of the page.

Note: To disable monitoring for the event, clear the **Enable** check box.

---

3. On the New Error Page Event page, under **Category Settings**, you can assign a category to the error page event for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.
4. Click the **OK** button at the bottom of the page. The error page event you configured is added to the monitor tree, underneath the Transaction object within which you added it.

Once an event has been configured, you can view the event settings, edit the event settings, delete the event from the monitor tree, or copy and paste the event in the monitor tree.

To view settings for an event:

In the monitor tree, click the event whose configuration settings you want to view. The configured event settings are displayed in the Properties tab.

To edit settings for an event:

Right-click the event in the monitor tree and select **Edit**. On the Edit Event page, edit the event settings as required.

To delete an event:

Right-click the event in the monitor tree and select **Delete**.

To copy and paste an event:

Right-click the event in the monitor tree and select **Copy**. To paste the event, right-click the object to which you want to copy the event and select **Paste**. A copy of the event with the name **<event name>.1** appears in the monitor tree.

Configuring End-User Groups

You can use Real User Monitor to collect data for each end-user accessing the server(s) being monitored. To collect specific data for specific groups of end-users, you must first define these groups of end-users and configure monitoring settings for them. You can choose to create containers within which to categorize the end-user groups you define, or you can define end-user groups directly under the End User Groups object.

Once a container, or end-user group has been configured, you can view the end-user group or container settings, edit the end-user group or container settings, delete the end-user group or container from the monitor tree, or copy and paste the end-user group or container in the monitor tree.

Note: When you click the **End User Groups** object in the monitor tree, the Contents tab is displayed. For information on the Contents tab, see "Navigating and Performing Actions in the Contents Tab and the Monitor Tree" in *Working with Monitor Administration*.

To create an end-user group container:

1. Right-click the **End User Groups** object, or an existing end-user group container in the monitor tree and select **New Container**. The New Container page opens.
2. On the New Container page, under **Main Settings**, enter the name you want to assign the end-user group container. Note that the name you enter must be unique and must not exceed 100 characters.
3. On the New Container page, under **Category Settings**, you can assign a category to the container for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.
4. On the New Container page, under **Advanced Settings**, enter a description of the container, which you can view in Monitor Administration only. Note that the description is limited to 260 characters.
5. Click the **OK** button at the bottom of the page. The end-user group container you configured is added to the monitor tree, underneath the End User Groups object, or the end-user group container within which you added it.

To configure an end-user group to monitor:

1. Right-click the **End User Groups** object in the monitor tree and select **New End User Group**. The New End User Group page opens.
2. On the New End User Group page, under **Main Settings**, enter the following:
   - the name you want to assign the end-user group. Note that the name you enter must be unique and must not exceed 100 characters.
   - a description of the end-user group, which you can view in Monitor Administration only. Note that the description is limited to 260 characters.
   - from the **Monitoring conditions** box, select one of the following options:
     - **Always.** Instructs Real User Monitor to collect data for all traffic generated by end-users within the end-user group. This data appears in the Real User Monitor reports.
     - **Never.** Instructs Real User Monitor not to collect data for the end-users within the end-user group. Data for the end-user group will not appear in the Real User Monitor reports.
   - the starting IP address of the IP range (subnet) of the end-user group.
   - the ending IP address of the IP range (subnet) of the end-user group.
   - the IP resolution. Select one of the following methods by which the subnet is displayed in the Real User Monitor reports:
     - **As entered.** The defined IP range is displayed in the Real User Monitor reports according to the way in which you enter it in this dialog box.
     - **Class A.** The IP addresses in the range you defined are displayed in the Real User Monitor reports according to the Class A network IP addressing method.
     - **Class B.** The IP addresses in the range you defined are displayed in the Real User Monitor reports according to the Class B network IP addressing method.
     - **Class C.** The IP addresses in the range you defined are displayed in the Real User Monitor reports according to the Class C network IP addressing method.

- **According to RFC.** The IP addresses in the range you defined are displayed in the Real User Monitor reports according to RFC class divisions (0.0.0.0 to 127.255.255.255 = Class A; 128.0.0.0 to 191.255.255.255 = Class B; 192.0.0.0 to 255.255.255.255 = Class C).
- **Defined CIDR mask.** The IP addresses in the range you defined are displayed in the Real User Monitor reports according to the mask (CIDR notations, 0 to 32) you define in the text box provided to the right of the selector.

➤ the end-user latency threshold. Enter the average network latency threshold in milliseconds, for each end-user in the end-user group.

➤ choose whether to select the **Perform end-user name resolution** check box. If you select this check box, Real User Monitor uses internal methods (such as the DNS, the NIS, or other internal files) to resolve the host name of each IP address within the subnet you are defining.

➤ choose whether to select the **Specify a geographical location** check box. If you select this check box, choose the country, state, and city in which the IP range you are defining is located.

Note: To disable monitoring for the end-user group, clear the **Enable** check box.

---

3 On the New End User Group page, under **Category Settings**, you can assign a category to the end-user group for use when filtering the monitor tree. For information on category settings, see "Working with Categories" in *Working with Monitor Administration*.

4 Click the **OK** button at the bottom of the page. The end-user group you configured is added to the monitor tree, underneath the End User Groups object, or the end-user group container within which you added it.

To view settings for an end-user group or end-user group container:

In the monitor tree, click the end-user group, or end-user group container, whose settings you want to view. The configured settings are displayed in the Properties tab.

To edit settings for an end-user group or end-user group container:

Right-click the end-user group, or end-user group container in the monitor tree and select **Edit**. On the Edit End User Groups, or Edit Container page, edit the end-user group or end-user group container settings as required.

To delete an end-user group or end-user group container:

Right-click the end-user group or end-user group container in the monitor tree and select **Delete**.

To copy and paste an end-user group or end-user group container:

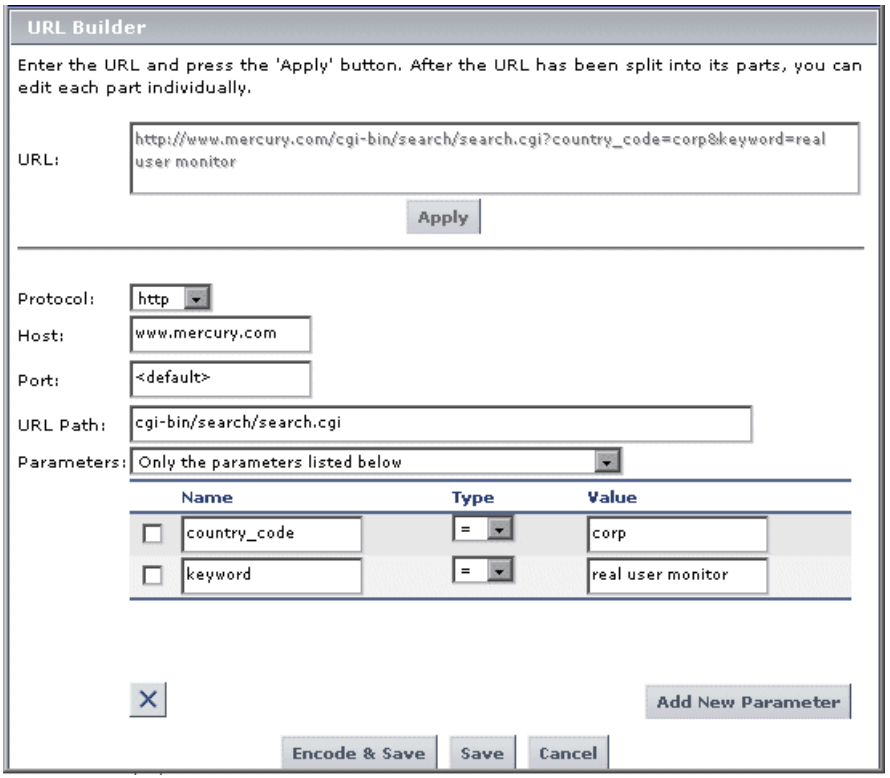
Right-click the name of the end-user group or end-user group container in the monitor tree and select **Copy**. To paste the end-user group or end-user group container, right-click the End User Groups object or end-user group container to which you want to copy the end-user group or end-user group container and select **Paste**. A copy of the end-user group or end-user group container appears in the monitor tree.

Note: An end-user group, or end-user group container, can be copied from one Real User Monitor engine to another, but cannot be copied within the same Real User Monitor engine.

Using the URL Builder

You use the URL Builder to define URLs when configuring session reset settings, applications, pages, and error page events.

The URL Builder dialog box consists of two areas. The upper area contains a field for the full URL and the lower area contains a field for each of the five composite parts of the URL.



To specify a URL, you enter the URL in the **URL** box in the upper area of the URL Builder dialog box. You can enter a URL by typing it in the **URL** box directly, or by copying a URL from an external source and pasting it in the **URL** box. Once you have entered the URL, click the **Apply** button and the URL is automatically broken down into its five composite parts in the lower area of the URL Builder dialog box.

Once you click the **Apply** button and the URL is broken down into its parts, you cannot edit the URL directly in the **URL** box in the upper area of the URL Builder dialog box, but do so by editing the individual parts in the lower area of the URL Builder dialog box. Any change to the individual parts is automatically updated and displayed in the full URL in the **URL** box in the upper area of the URL Builder dialog box.

Note: The URL cannot exceed 1000 characters and cannot include the # sign followed by an asterisk (#*).

The following are the five composite parts of the URL, which you are able to edit:

- URL Protocol – see page 121
- URL Host – see page 122
- URL Port – see page 122
- URL Path – see page 122
- URL Parameters – see page 123

For example, the following table shows the composite parts of the URL **http://www.mercury.com/cgi-bin/search/search.cgi?country_code=corp&keyword=real%20user%20monitor**

URL Part	Value
Protocol	http
Host	www.mercury.com
Port	80 (default)
URL Path	cgi-bin/search/search.cgi
Parameters	country_code=corp&keyword=real%20user%20 monitor

You can use wildcard expressions when defining URLs (for details, see “Wildcard Expressions” on page 121).

Wildcard Expressions

The asterisk (*) is the only valid wildcard character that can be used when defining a URL. The asterisk can be used in the URL host, the URL port, the URL path, and the URL parameters. The asterisk wildcard character represents any combination of characters and is applicable to where it is placed. For example:

- **mercury*** is equivalent to any string of characters that begins with **mercury**
- ***mercury** is equivalent to any string of characters that ends with **mercury**
- ***mercury*** is equivalent to any string of characters that has **mercury** in it somewhere
- **mer*cury** is equivalent to any string of characters that begins with **mer** and ends with **cury**

By default, an asterisk is considered to be a wildcard. If you want to use an asterisk as a literal in a string and not as a wildcard, precede it with a backslash (\). For example, the string **my*str*** will be matched with **my*str123**, but will not be matched with **my123str123**.

Note: The asterisk wildcard character cannot be used in the URL port when defining an application URL.

URL Protocol

The URL protocol is the protocol used to fetch the URL. You select the protocol from the list available for this field and can choose either the HTTP or HTTPS protocol. HTTP is the standard protocol for regular communications and HTTPS is the protocol used when the URL is accessed using Secure Sockets Layer (SSL.)

URL Host

The URL host is the name of the machine on which the file, or resource, that you wish to access via the URL resides. For example, if the URL you entered is **http://www.mercury.com/cgi-bin/search/search.cgi?country_code=corp&keyword=real%20user%20monitor**, the host is **www.mercury.com**.

The asterisk wildcard character can be used. For example, if you enter **www.mer*** as the URL host, any host that begins with **www.mer** can be correlated with the configured URL.

URL Port

The URL port is the port number used to connect to the URL host machine. If no port is specified, a default port number will be used. The default port when using the HTTP protocol is 80 and when using the HTTPS protocol, the default port is 443.

The asterisk wildcard character can be used. For example, if you enter **44*** as the URL port, any port that begins with 44 can be correlated with the configured URL.

Note: The asterisk wildcard character cannot be used in the URL port when defining an application URL.

URL Path

The URL path is the path to the file, or resource, that you wish to access via the URL. For example, if the URL you entered is **http://www.mercury.com/cgi-bin/search/search.cgi?country_code=corp&keyword=real%20user%20monitor**, the path is **cgi-bin/search/search.cgi**.

The asterisk wildcard character can be used. For example, if you enter **cgi*search.cgi** as the URL path, any path that begins with **cgi** and ends with **search.cgi** can be correlated with the configured URL.

URL Parameters

URL parameters form a query string that is used by the URL to narrow its search by filtering for specific values in specific parameters. Each parameter in the string includes the parameter name and the value being searched for. For example, if the URL you entered is **http://www.mercury.com/cgi-bin/search/search.cgi?country_code=corp&keyword=real%20user%20monitor**, the parameter string is **country_code=corp&keyword=real%20user%20monitor**. Within this parameter string, the following are the parameter names and values being sought:

Parameter Name	Requested Value
country_code	corp
keyword	real user monitor

Parameters are separated from the rest of the URL by a question mark (?).

Configured URLs must use the ampersand character (&) as the parameter delimiter.

The asterisk wildcard character can be used in the value part of a parameter, but cannot be used in the parameter name. For example, if you enter **country_code=corp*** as the URL parameter, any value that begins with **corp** in the parameter called **country_code** can be correlated with the configured URL. If the URL parameter string contains only an asterisk wildcard character and nothing else, this indicates that the URL must contain at least one parameter, but it does not matter what the parameter name, or the value, is.

To edit the parameters:

1 From the **Parameters** box, select one of the following options:

- **None.** This option does not define any parameters.
- **None or more.** This option specifies that either no parameters, or any combination of parameters are valid.
- **Only the parameters listed below.** This option allows you to specify specific parameters and values that must be matched.
- **Those parameters listed below as well as other parameters.** This option allows you to specify specific parameters and values that must be matched, but also will accept any other additional parameters and values.
- **At least one parameter.** This option indicates that the URL must contain at least one parameter, but it does not matter what the parameter name, or the value, is.

2 If you select **Only the parameters listed below**, or **Those parameters listed below as well as other parameters**, click the **Add New Parameter** button.

- In the **Name** box, enter the name of the parameter.
- In the Type box, select **All** to include all values of the parameter, or = to include only a specific parameter value.
- If you chose to include only a specific parameter value, enter that value in the **Value** box.
- Click the **Add New Parameter** button for each additional parameter you wish to add.

To delete a parameter, select the check box to the left of the parameter and click the **Delete** button.

When you have finished defining the URL, click **Encode & Save** to convert the URL into UTF-8 format and save it in your configuration, or click **Save** to enter the URL into your configuration without any encoding. By saving a URL without UTF-8 encoding, you can define a URL that is externally encoded by a different encoding scheme.

Exit from the URL Builder.

Note: URL matching is affected by the encoding of recorded and configured URLs. For recorded and configured URLs to match, they must have the same encoding.

Correlating Collected Data with Configured Pages

This section discusses various principles of correlation that Real User Monitor uses, in addition to correlating the wildcard expressions that can be used in the URL builder (see "Wildcard Expressions" on page 121 for details), to correlate the data collected by the probe(s) with the specific URLs that you configured for each application.

In addition, this section describes the algorithm that Real User Monitor uses to determine which URL definition a recorded URL will be correlated with, if several URL definitions match the recorded URL.

Principles of Correlation

In addition to correlating wildcard expressions (for details, see "Wildcard Expressions" on page 121), Real User Monitor uses other guiding principles, or rules in correlating recorded URLs with the URLs you configured. You can reconfigure some of the default correlation rules according to which Real User Monitor operates in the Real User Monitor Engine. For details on configuring the Real User Monitor Engine, see "URL Correlation Parameters" in *Real User Monitor Administration*.

Correlating Session ID Parameters

By default, Real User Monitor takes the session ID parameters of the recorded URL into consideration when correlating the recorded URL with a configured URL. It looks to match the recorded URL to a configured URL containing the identical session ID parameter values. In addition, Real User Monitor treats URLs with non-identical session ID parameter values as separate entities when calculating global statistics such as Most Popular Pages.

You can instruct Real User Monitor to ignore session ID parameters when correlating a recorded URL with a configured URL by configuring the **MercuryRUM\conf\configurationmanager\ Application_Server_Types_configuration.xml** file on the Real User Monitor engine machine (for details, see "Correlating Session ID Parameters" in *Real User Monitor Administration*). For example, if you set the application server as **BroadVision** Real User Monitor ignores the **BV_SessionID** and **BV_EngineID** parameters in the following URL:

```
http://www.mercury.com/~anand/Ticket_Confirm.jsp?BV_SessionID=@@@@1
812057630.1043567934@@@@&BV_EngineID=cccdadchgidfmlmcefecehidfhf
dffk.0&value=0000144976
```

The URL is translated as follows:

```
http://www.mercury.com/~anand/Ticket_Confirm.jsp?BV_SessionID=*&BV_Engi
neID=*&value=0000144976
```

As a result, the recorded URL can be correlated with a configured URL that contains different BV_SessionID and BV_EngineID parameters.

The different BV_SessionID and BV_EngineID parameter values are also ignored when Real User Monitor calculates global statistics such as Most Popular Pages. In the above example, all BroadVision sessions are recorded as **http://www.mercury.com/~anand/Ticket_Confirm.jsp? BV_SessionID=*&BV_EngineID=*&value=0000144976** for global statistic purposes.

Note: Vugen and Business Process Monitor transactions that do not contain a session ID in either a header cookie or the URL, cannot be correlated as individual sessions. Vugen and Business Process Monitors should be configured to include a session ID in a header cookie, or the URL, in transactions.

If the interval between Business Process Monitor samples is greater than the session time-out configured for the Real User Monitor engine in Monitor Administration, the open session will be closed and a new session started for the next sample, even if a session ID is not included in the sample.

Correlating URL Suffixes

By default, Real User Monitor considers a URL such as **http://www.mercury.com/index.html** to be different from the URL **http://www.mercury.com/**. To instruct Real User Monitor to consider two such URLs as being identical, you can set the **adaptIndexurl** parameter in the Real User Monitor engine (for details, see "Setting URL Correlation Parameters Via the JMX Console" in *Real User Monitor Administration*).

Correlation and Case-Sensitivity

By default, Real User Monitor URL correlation is case-insensitive—that is, a recorded URL such as **http://www.mercury.com/rumEnginePage.html** will be correlated with the configured URL **http://www.mercury.com/rumenginepage.html**. However, you can instruct Real User Monitor to use case-sensitive URL correlation (for all but the host and protocol parts of a URL) by setting the **adaptCaseSensitive** parameter in the Real User Monitor engine (for details, see "Setting URL Correlation Parameters Via the JMX Console" in *Real User Monitor Administration*).

Correlating Parameters Without Values

Real User Monitor will correlate a URL even if it contains a parameter key without a value. For example, a recorded URL such as **http://www.mercury.com/cgi-bin/search/search.cgi?country_code** will still be correlated even though no value has been specified for the country_code parameter.

Note: You cannot configure Real User Monitor to operate differently in this respect.

Correlating URLs Containing Bookmarks

Real User Monitor ignores bookmarks when performing URL correlation. For example, the recorded URL **http://www.mercury.com:80/?A=2#bookmark3** will be correlated with the configured URL **http://www.mercury.com:80/?A=2**.

Correlating URLs Without URL Paths

Real User Monitor considers URLs that do not contain URL paths to be identical to URLs that contain a slash following the host part of the URL. For example, the recorded URL **http://www.mercury.com** will be correlated with the configured URL **http://www.mercury.com/**.

Note: You cannot configure Real User Monitor to operate differently in this respect.

Correlating URLs Ending with a Directory

Real User Monitor does not consider URLs that contain a double slash representing a directory to be identical to URLs that contain a single slash following the host part of the URL. For example, the recorded URL **http://www.mercury.com//** will not be correlated with the configured URL **http://www.mercury.com/**.

Note: You cannot configure Real User Monitor to operate differently in this respect.

Correlating Ports

Real User Monitor assigns a default port to a recorded URL in which a port number is not specified. For example, a recorded URL such as **http://www.mercury.com** will be correlated with the configured URL **http://www.mercury.com:80**.

Correlating URLs Containing Basic Authentication

By default, Real User Monitor ignores basic authentication when performing URL correlation. For example, the recorded URL **http://bob:my_password@www.mercury.com** will be correlated with the configured URL **http://www.mercury.com**. However, you can instruct Real User Monitor to consider basic authentication when performing URL correlation by setting the **basicAuthentication** parameter in the Real User Monitor engine (for details, see "Setting URL Correlation Parameters Via the JMX Console" in *Real User Monitor Administration*).

Correlating Parameters

By default, Real User Monitor query parameter correlation is not order-sensitive. For example, the recorded URL **http://www.mercury.com:80/?a=2&b=2&c=3** can be correlated with the configured URL **http://www.mercury.com:80/?b=2&c=3&a=2** or the configured URL **http://www.mercury.com:80/?b=2&a=2&c=3**.

Note: You cannot configure Real User Monitor to operate differently in this respect.

Correlation Algorithm for Multiple URL Matches of Business Critical Pages

Whereas in previous versions of Real User Monitor a recorded URL could be correlated with several configured pages—if the URL matched several page definitions—in the current version of Real User Monitor a URL can be correlated with only one configured page.

If a recorded URL matches several URL definitions, Real User Monitor determines which configured page to correlate with the recorded URL based on the placement of the asterisk (*) wildcard character in the configured URL. URLs comprise up to five parts, separated by delimiters (for details of the different parts, see "Using the URL Builder" on page 119). Real User Monitor will first try to match the recorded URL to a defined URL with an asterisk in the last part of the defined URL. If no match can be made, Real User Monitor will then try to match the recorded URL to a defined URL with an asterisk in the one but last part of the defined URL. In this manner it will keep trying to find a match up to an asterisk, moving backwards from part to part in the defined URL.

For example, if you configured two URLs—**http://www.mercury.com/cgi-bin/search/search.cgi?*** and **http://www.mercury.com/cgi***—and the URL **http://www.mercury.com/cgi-bin/search/search.cgi?country_code=corp&keyword=real+user+monitor** is recorded, the recorded URL will be correlated with **http://www.mercury.com/cgi-bin/search/search.cgi?*** because the asterisk is located in the last part (query parameters), rather than in a preceding part of the URL.

If two configured URLs both contain asterisks in the same part of the URL, the Real User Monitor matches the recorded URL to the configured URL with which it shares the greatest number of consecutive joint characters from the beginning of the URL. For example, if you configured two URLS—**http://www.mercury.com/cgi*** and **http://www.mercury.com/cgi-bin***—and the URL **http://www.mercury.com/cgi-bin/search/search.cgi?country_code=corp&keyword=real+user+monitor** is recorded, the recorded URL will be correlated with **http://www.mercury.com/cgi-bin***.

Backward Compatibility

In Mercury Business Availability Center 6.2, Real User Monitor no longer supports the following:

- the old probe machine. Real User Monitor in Mercury Business Availability Center 6.0 works with the new Real User Monitor probe.

- matching of business critical pages on a page level only. Business critical pages are matched only if they are defined under the same, reported application in Monitor Administration.
- order-sensitive correlation of GET/POST parameters of defined pages.
- the possibility of defining a page in monitor administration for a secondary component such as a GIF. Pages can be defined only for main components.
- the ability to ignore a sub-component by defining a business critical page on this component with monitoring conditions set to **never**. This means that there is no possibility of ignoring a missing component.
- specifying POST parameters to be sent by the probe. All POST parameters are sent by the probe and appear as part of the URL. This must be taken into consideration when defining pages in monitor administration.
- the automatic removal of known, session identification parameters and values. The values of such parameters are removed, but the actual parameter key is not and is still reported in the URL.
- the automatic discovery of application servers to be checked for the removal of the application server session ID parameter key and value of a recorded URL. The current version of Real User Monitor checks only application servers that have been enabled in the **<Real User Monitor HOME>\conf\resolver\AppServer.xml** file. If enabled, the session ID parameter value is removed, but the parameter key is still included.
- single IP address, or host resolution.
- the configuring of pages with generic patterns. Pages can now be configured with text patterns instead.
- reporting of slowest components. The Real User Monitor engine now reports slowest pages instead.
- predefined thresholds for the reporting of slowest pages and end-users. Slowest pages and end-users are now displayed without the need to meet a predefined threshold.
- the display of the page name for most popular pages. The defined URL of the page is now displayed.

Index

E

G

H

M

O

P

R

S

T

U

W

Z