OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

Using End User Management

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

Using End User Management

Version 6.2

Document Release Date: June 20, 2006

MERCURY™

Mercury Business Availability Center, Version 6.2
Using End User Management

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

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

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

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

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

© 2005-2006 Mercury Interactive Corporation, All rights reserved

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

AMLIB_EUM6.2/01

Table of Contents

Welcome to Using End User Management ..... **v**
How This Guide Is Organized v
Who Should Read This Guide vi
Getting More Information vii

Chapter 1: Introduction to End User Management Reports **1**
Overview of End User Management Reports 1
End User Management Reports 3

Chapter 2: Status Snapshot **5**
Overview of Status Snapshot 5
Working With Status Snapshot 7

Chapter 3: Summary Reports **9**
About Summary Reports 9
Multi-Profile Summary Report 10
Single Profile Summary Report 14
Performance Matrix Report 18
Triage Report 23

Chapter 4: Business Process Reports **31**
About Business Process Reports 32
Triage Raw Data Report 34
Availability over Time Report 38
Response Time over Time Report 40
Transaction Analysis Report 42
Error Summary Report 43
Location Analysis Reports 51
Understanding the Transaction Breakdown Reports 52
Breakdown over Time Report 57
Breakdown Summary Report 59
Min./Max. Response Time Report 65
Desktop Performance Report 67
Response Time by Percentile Report 69

Chapter 5: Real User Monitor Reports....71
Overview of Real User Monitor Reports....72
Working with Real User Monitor Reports....75
Global Statistics Report....86
Page Summary Report....94
Transaction Summary Report....113
End User Summary Report....129
Server Summary Report....133
Session Analyzer Report....139
Event Count Over Time Report....150
Event Summary Report....152
Business Process Distribution Report....155
Network Latency Report....160
HTTP Error Codes....162

Chapter 6: Alert Reports....165
About Alert Reports....166
Alert Log....167
Alert Count over Time Report....169

Chapter 7: Network Reports and Tools....171
About Network Reports and Tools....172
WebTrace by Location Report....173
Network Analysis Report....177
Page Component Breakdown Tool....178
Instant Diagnostics....184

Chapter 8: User Reports....187

Index....189

Welcome to Using End User Management

This guide describes how to work with the End User Management application in Mercury Business Availability Center.

How This Guide Is Organized

The guide contains the following chapters:

Chapter 1 Introduction to End User Management Reports

Introduces the End User Management application.

Chapter 2 Status Snapshot

Describes how to use End User Management Status Snapshot, to determine the five worst-performing business processes in the system for the last day.

Chapter 3 Summary Reports

Describes reports that provide an overall picture of the performance of your monitored environment, based on data collected by the Business Process Monitor and Client Monitor data collectors.

Chapter 4 Business Process Reports

Describes reports that provide an in-depth view of the health of your monitored environment, based on data collected by the Business Process Monitor and Client Monitor data collectors.

Chapter 5 Real User Monitor Reports

Describes reports that detail the real user activity reported by the Real User Monitor data collector.

Chapter 6 Alert Reports

Describes reports that provide information about all Mercury Business Availability Center alerts that have been logged to the database.

Chapter 7 Network Reports and Tools

Describes reports that provide data on the quality of network performance, including data collected by the WebTrace monitor.

Chapter 8 User Reports

Provides a pointer to the complete documentation for user reports, which are common to the Service Level Management, End User Management, and System Availability Management applications.

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 end users

Readers of this guide should be knowledgeable about navigating and using enterprise applications, and be familiar with Mercury Business Availability Center and enterprise monitoring and management concepts.

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

Introduction to End User Management Reports

Mercury End User Management reports enable you to proactively monitor network and application performance and availability in real time, from the end-user perspective, so you can resolve issues before customers experience problems.

This chapter describes:	On page:
Overview of End User Management Reports	1
End User Management Reports	3

Overview of End User Management Reports

You use the End User Management application to view and analyze reports based on performance data collected by Mercury Business Availability Center data collectors and stored in the Mercury Business Availability Center database.

End User Management reports enable you to:

- detect end-user business process issues before customers are impacted
- track alerts for user performance and availability issues
- proactively identify end-user performance and availability trends that need IT attention
- assess business impact and prioritize resolution efforts, escalating user problems to the correct IT groups

- prioritize IT response based on customer/business impact
- manage the customer's Quality of Experience (QoE), and gain real-time visibility into the QoE of real users

You access End User Management reports from the End User Management application in the Applications menu.

For details on working with Mercury Business Availability Center reports, see "Working in Reports" in *Working with Applications*.

For details on configuring reports in Mercury Business Availability Center, see "End User Management Report Configuration" in *End User Management Data Collector Configuration*.

Report Access and Permissions

The availability of report data for a specific user is dependent on the profile access permissions granted that user. Furthermore, access to specific data within a profile can also be limited by the administrator using report filters. For details on granting permissions, see "Configuring User Permissions" in *Platform Administration*.

For details on setting report filters, see "Configuring Report Filters Globally" in *Platform Administration* and "Report Filters" in *Application Administration*.

Data Aggregation

Mercury Business Availability Center uses data aggregation to make data handling and management more efficient and to improve the speed and performance of report generation. For more information on data aggregation in Mercury Business Availability Center, see "Data Aggregation" in *Reference Information*.

End User Management Reports

The following reports are available:

Reports	Description	For Details, See...
End User Management Snapshot Status	Displays a summary of the five worst transactions and locations for Business Process Monitor and Client Monitor for the last day. For Real User Monitor, End User Management displays the five worst sessions (that is, the least available) and the slowest applications.	Chapter 2, "Status Snapshot"
Summary reports	Displays reports that provide an overall snapshot of the health of your monitored environment. Report data is based on Business Process Monitor and Client Monitor data.	Chapter 3, "Summary Reports"
Business Process reports	Displays reports that provide an in-depth look at the health of your monitored environment and help you diagnose and pinpoint the root cause of performance problems. Report data is based on Business Process Monitor and Client Monitor data.	Chapter 4, "Business Process Reports"
Real User Monitor reports	Displays reports that help you monitor the experience of real users who access your application. Report data is based on Real User Monitor data.	Chapter 5, "Real User Monitor Reports"

Reports	Description	For Details, See...
Alert reports	Displays reports that detail the types and frequency of alerts sent. Report data is based on alerts for Business Process and Client Monitor profiles.	Chapter 6, "Alert Reports"
Network and Tool reports	Displays reports that help you identify problems along the network. Report data is based on WebTrace/Traceroute monitor data.	Chapter 7, "Network Reports and Tools"
User Reports	Enables creating and viewing reports that are tailored to the specific monitoring requirements of your organization or business unit, and displaying those reports. Report data is based on Business Process Monitor, Client Monitor, WebTrace/Traceroute Monitor, Real User Monitor, SiteScope, and custom data. Enables searching for and viewing reports in the report repository.	Chapter 8, "User Reports"

2

Status Snapshot

This chapter describes the End User Management Status Snapshot.

This chapter describes:	On page:
Overview of Status Snapshot	5
Working With Status Snapshot	7

Overview of Status Snapshot

Status Snapshot displays a summary of the following data:

- for Business Process Monitor and Client Monitor, the five worst transactions and locations (that is, the least available) across all profiles, for the last day
- for Real User Monitor, the five least available applications (that is, the applications with the highest number of sessions ending in error) and the five slowest applications, for the last day

From the data in the graphs, you can drill down to the Transaction Analysis, Location Analysis, and Session Analyzer reports.

This section includes the following topics:

- "How End User Management Calculates Status Snapshot" on page 6
- "Editing Settings With the Infrastructure Settings Manager" on page 6

How End User Management Calculates Status Snapshot

For Business Process Monitor and Client Monitor, End User Management calculates the Status Snapshot by data aggregation, once an hour (by default). For Real User Monitor, End User Management calculates the Status Snapshot on raw data.

The calculated data resides in the cache and remains there until an hour has passed and a user has accessed Status Snapshot. When these two criteria are fulfilled, End User Management empties the cache and calculates the data again. If a user attempts to access the Status Snapshot when the cache is empty, a message is displayed until new data is processed.

You can verify the date and time that data was last calculated by looking at the Status Snapshot title:



Editing Settings With the Infrastructure Settings Manager

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

Administrators with an advanced knowledge of Mercury Business Availability Center can customize the End User Management setting that defines the time (in seconds) to hold cached calculated data for the Status Snapshot.

Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Applications**, select **End User Management**, and locate the **EUM Top View data timeout** entry in the **End User/System Availability Management – Timing** table. Update the value as required.

Note for Mercury Managed Services customers: To access the **End User/System Availability Management – Timing** table, select the Customer Settings tab.

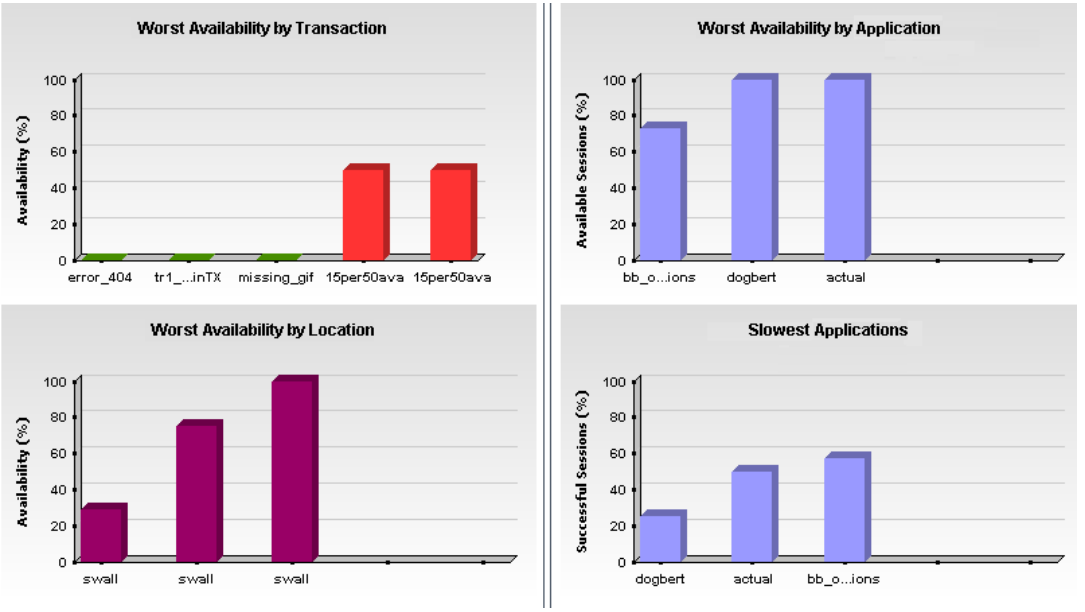
For details on editing infrastructure settings, see "Editing Infrastructure Settings" in *Platform Administration*.

Working With Status Snapshot

Status Snapshot shows data organized in graphs for Business Process Monitor, Client Monitor, and Real User Monitor.

To work with Status Snapshot:

1 Select **Applications** > **End User Management** > **Status Snapshot**.



2 Hold the pointer over a bar in a graph to view a tooltip showing:

- For Business Process Monitor and Client Monitor – average response time and average availability for each transaction or location
- For Real User Monitor – availability and performance for each application and for the slowest applications

3 Click a bar to drill down to the analysis report.

- For details on the Transaction Analysis report, see "Transaction Analysis Report" on page 42.
- For details on the Location Analysis report, see "Location Analysis Reports" on page 51.
- For details on the Session Analyzer report, see "Session Analyzer Report" on page 139.

4 Transactions and sessions are color coded according to the transaction performance thresholds. For details, see "Transaction Threshold Settings" in *End User Management Data Collector Configuration*.

3

Summary Reports

This chapter describes the Summary reports and explains how to assess the overall performance of your monitored environment.

This chapter describes:	On page:
About Summary Reports	9
Multi-Profile Summary Report	10
Single Profile Summary Report	14
Performance Matrix Report	18
Triage Report	23

About Summary Reports

Summary reports include data collected by Business Process Monitor, Client Monitor, and Real User Monitor data collectors, and provide response time and availability data from profile, transaction, and location perspectives. You access Business Process reports from the Business Process tab in the End User Management application.

For details on working with reports (setting reports to generate automatically, choosing the time range, selecting a profile, saving and sharing reports, and so forth), see "Working in Reports" in *Working with Applications*.

The following Summary reports are available:

Category	Description	For Details, See...
Multi-Profile Summary report	Provides an overall snapshot of application performance for multiple Business Process and Client Monitor profiles.	page 10
Single Profile Summary report	Provides a quick snapshot of application performance for a specific Business Process or Client Monitor profile.	page 14
Performance Matrix report	Displays a distribution of average transaction response times—organized by transaction, location, or group—over a specified period of time.	page 18
Triage report	Displays transaction data for Business Process Monitor profiles for the past day or for 24 hours, organized by location.	page 23

Multi-Profile Summary Report

The Multi-Profile Summary report provides an overall snapshot of application performance for multiple Business Process and Client Monitor profiles.

The first time Mercury Business Availability Center generates the Multi-Profile Summary report, it includes all profiles up to a maximum of 10. You can change the number of profiles that are included in the report by clicking the **Profile(s)** link and selecting the profiles in the Profiles window. For details on selecting profiles, see "Selecting Profiles" in *Working with Applications*.

To access the Multi-Profile Summary report:

Select **Applications** > **End User Management** > **Summary Reports**.

This section includes the following topics:

➤ "Working with the Multi-Profile Summary Report" on page 11

➤ "Profile Performance" on page 11

➤ "Location Performance" on page 12

➤ "Alert Summary" on page 13

➤ "Multi-Profile Summary Report Limitations" on page 14

Working with the Multi-Profile Summary Report

➤ To view a tooltip describing the exact number and percentage of transactions for a segment, point to that segment of the pie chart.

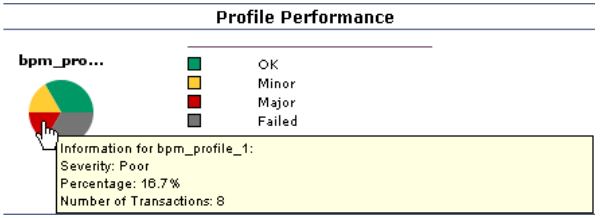
➤ When you point to a **Failed** segment, Mercury Business Availability Center also displays the number of outlier transactions. Outlier data appears in a report if **Ignore outlier data in reports** is cleared in the profile's settings for transaction thresholds (set in Monitor Administration—for details, see "Transaction Threshold Settings" in *End User Management Data Collector Configuration*).

➤ You can add a chart to a custom report. For details, see "Workflow for Creating Custom Reports" in *Working with Applications*. For the Profile Performance report, Custom Report Manager enables you to add a version of the report that displays the performance of all profiles, not just the three with the worst performance.

Profile Performance

This chart provides you with a quick snapshot of the worst-performing profiles from among the Business Process and Client Monitor profiles you select. The chart displays—for the defined time frame—the three profiles in which transactions most often fail or have response times in the Minor and Critical ranges. If there are fewer than three profiles, Mercury Business Availability Center displays a pie chart for each profile.

In the following example, the **bpm pro** profile has 33.3% of all transactions with response times within the OK (green) threshold range, 16.7% within the Minor (yellow) range, 16.7% within the Critical (red) range, and 33.3% within the Failed (gray) range.

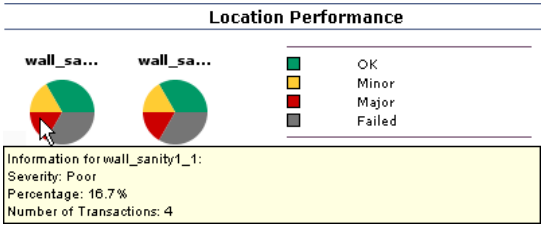


To generate the Transaction Analysis report for a profile, click a pie chart. For details on the Transaction Analysis report, see "Transaction Analysis Report" on page 42.

Location Performance

This chart provides you with a quick snapshot of the worst-performing locations for the selected Business Process and Client Monitor profiles, in terms of transaction response time. The chart displays—for the selected profiles and defined time frame—the three locations from which transactions most often fail or have response times in the Minor and Major range. If there are fewer than three locations in the selected profiles, Mercury Business Availability Center displays a pie chart for every location.

In the following example, the **wall_sa** profile has 33.3% of all transactions with response times within the OK (green) threshold range, 16.7% within the Minor (yellow) range, 16.7% within the Critical (red) range, and 33.3% within the Failed (gray) range.



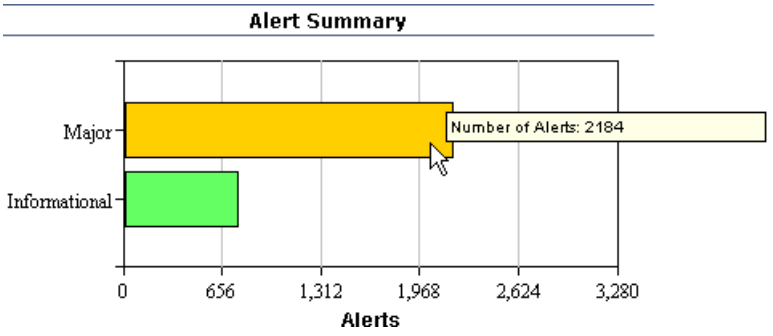
Alert Summary

This chart provides you with a quick snapshot of the total number of alert notices sent during the defined time period, for all selected profiles, grouped by their severity level:

- Unknown
- OK
- Warning
- Minor
- Major
- Critical

To view a tooltip describing the exact number of alerts, point to a bar.

In the following example, the total number of alert notices with major severity is 2104, and the total number of alert notices with informational severity is 760.



Multi-Profile Summary Report Limitations

- Mercury Business Availability Center does not display aggregated and raw data simultaneously in the Multi-Profile Summary report.
- Mercury Business Availability Center can display profiles concurrently only if they have the same outlier value settings. Outlier settings for each profile are listed in the report page, before report generation. Make sure to select a set of profiles that have the same settings for outlier values. For details on modifying outlier value settings for a profile, see "Transaction Threshold Settings" in *End User Management Data Collector Configuration*.
- Attempting to generate a Multi-Profile Summary report for a large number of profiles that are stored in multiple databases can significantly affect report generation time. If the time required to generate the report is greater than the browser timeout setting, the report will not be generated.

Single Profile Summary Report

The Single Profile Summary report provides a quick snapshot of application performance for a specific Business Process or Client Monitor profile. End User Management displays the last selected profile. To view the report for a different profile, click the **Profile(s)** link and select the required profile in the Profiles window. For details on selecting profiles, see "Selecting Profiles" in *Working with Applications*.

To access the Single Profile Summary report:

Select **Applications** > **End User Management** > **Summary Reports**.

This section includes the following topics:

- "Working with the Single Profile Summary Report" on page 15
- "Overall Quality of Service" on page 16
- "Alert Summary" on page 16
- "Performance of Transactions" on page 17
- "Performance of Locations" on page 17

Working with the Single Profile Summary Report

This section explains how to work with the single profile summary report.

To modify the report view:

Select **Transactions**, **Locations**, or **Groups** in the **View By** list, and click **Generate** to generate the transaction performance organized by transaction, location, or group.

To modify the report time frame:

Make changes to the report time frame (located above the **Single Profile Summary** area) and click **Generate** to generate the modified report.

To apply active filters:

Click the **Active Filters** link, and select or clear check boxes to view the report filtered by specific transactions, locations, or groups. Click **Generate** to generate the modified report.

To view a tooltip describing the exact number and percentage of transactions for each segment of the pie chart:

Point to a segment.

When you point to a **Failed** segment, Mercury Business Availability Center also displays the number of outlier transactions. The outlier data appears here if the **Ignore outlier data in reports** setting is disabled in the profile's transaction threshold settings (set in Monitor Administration—for details, see "Transaction Threshold Settings" in *End User Management Data Collector Configuration)*.

To generate a Transaction Analysis report for a transaction:

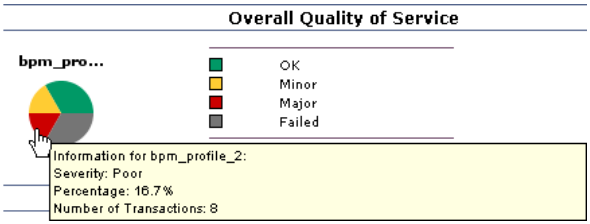
Click a chart. For details on the Transaction Analysis report, see "Transaction Analysis Report" on page 42.

To generate a Location Analysis report for a transaction:

Click a chart. For details on the Location Analysis report, see "Location Analysis Reports" on page 51.

Overall Quality of Service

This chart provides you with a quick snapshot of the quality of service of your monitored application, in terms of transaction response time. The pie chart displays—for the selected profile and time frame—the percentages of transactions that fall in the OK, Minor, Critical, and Major threshold ranges.



Alert Summary

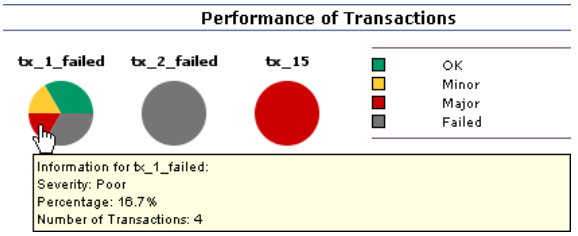
You view this chart to get a quick snapshot of the total number of alert notices, grouped by their severity level, sent during the defined time period for the selected Business Process profile (or for the selected Business Process profile when viewed in a custom report):

- Informational
- Warning
- Minor
- Major
- Critical

To view a tooltip describing the exact number of alerts, point to a bar.

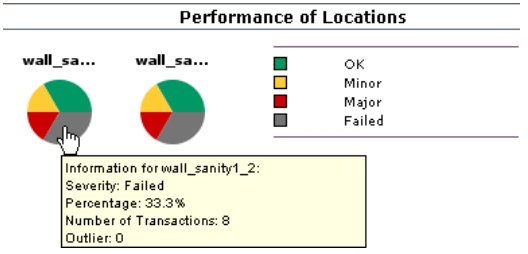
Performance of Transactions

This chart provides you with a quick snapshot of the worst-performing transactions in the profile. The chart displays—for the selected profile and time frame—the three transactions that most often failed or had response times in the Critical and Minor ranges. If there are fewer than three transactions in the profile, Mercury Business Availability Center displays a pie chart for each transaction.



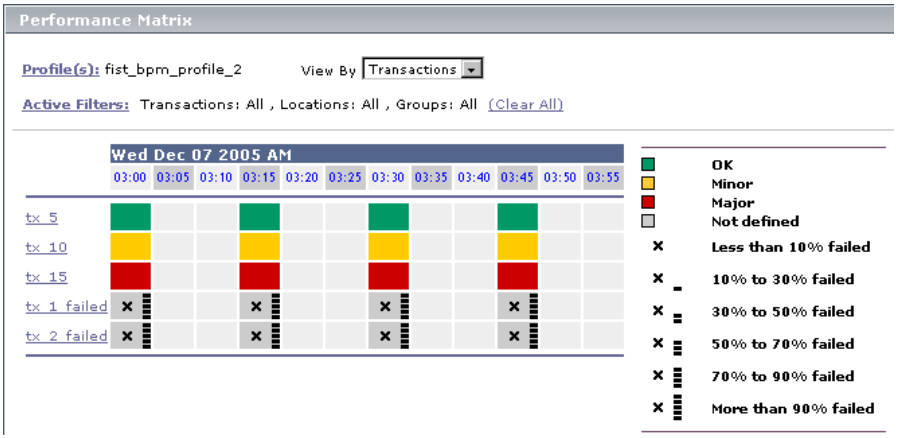
Performance of Locations

This chart provides you with a quick snapshot of the worst-performing locations in the profile. The chart displays—for the selected profile and time frame—the three locations from which transactions most often failed or had response times in the Critical and Minor range. If there are fewer than three locations in the profile, Mercury Business Availability Center displays a pie chart for each location.



Performance Matrix Report

The Performance Matrix report displays a distribution of average transaction response times—organized by transaction, location, or group—over a specified period of time.



The Performance Matrix report helps you pinpoint and characterize specific problem areas related to average transaction response time and transaction availability. By breaking down the table by transaction, location, or group across different time frames, you can identify exactly where and when average transaction response times are too slow and/or when there are too many failed transactions. For example, you may determine that response times of transactions running from a particular location are consistently in the poor range. This could indicate a problem with the network connections in that location.

In the transaction view, the report's color-coding corresponds to that of the transaction threshold settings—green for OK, yellow for Minor, and red for Critical. For details on setting transaction thresholds in Monitor Administration, see "Transaction Threshold Settings" in *End User Management Data Collector Configuration*.

To access the Performance Matrix report:

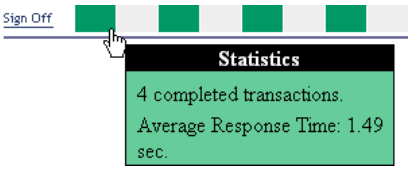
Select **Applications** > **End User Management** > **Summary Reports**.

This section includes the following topics:

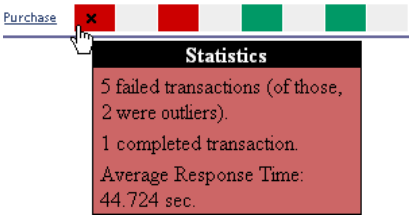
- "Working With the Performance Matrix Report" on page 19
- "Drilling Down to Smaller Time Frames" on page 21
- "Analyzing the Performance Matrix Report" on page 22

Working With the Performance Matrix Report

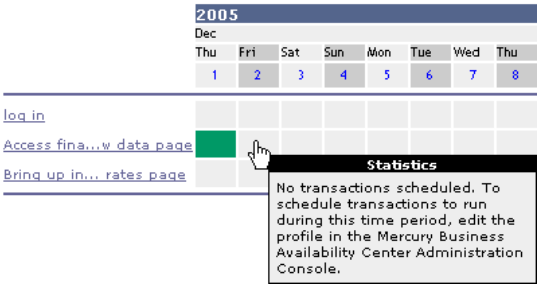
- Place the pointer over any colored cell in the table to view a tooltip containing details about the average response time of all completed transactions performed by hosts during the time period of the cell.



- Place the pointer over a cell with a black X to view a tooltip containing details on the number of failed transactions, the number of outlier transactions, and the average response time of completed transactions, for the time period of the cell.



➤ Place the pointer over a grey cell. A tooltip indicating that there are no transactions scheduled for this time frame is displayed.



➤ Modify the report view by selecting **Transactions**, **Locations**, or **Groups** in the **View By** list, and clicking **Generate** to generate the transaction performance organized by transaction, location, or group.

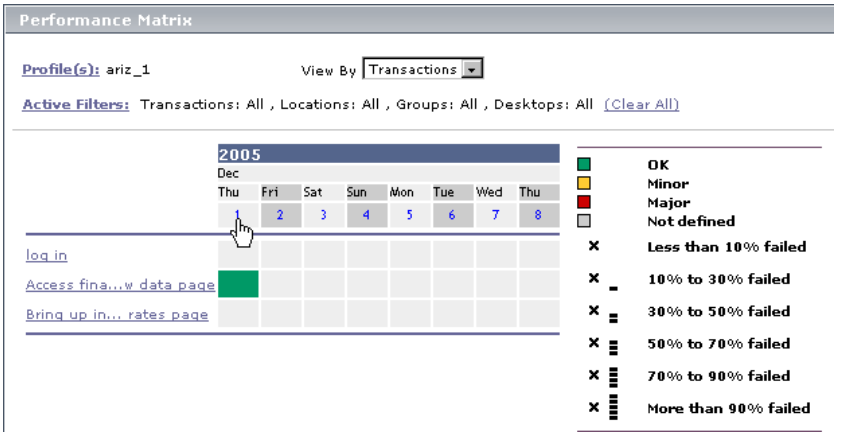
➤ Modify the report time frame (located above the **Performance Matrix** area) and click **Generate** to generate the modified report.

➤ Apply active filters by clicking the **Active Filters** link, and selecting or clearing check boxes to view the report filtered by specific transactions, locations, or groups.

➤ Click any link in a column header, row header, or cell to drill down to a greater level of detail.

Drilling Down to Smaller Time Frames

You can pinpoint and characterize specific problem areas related to average transaction response time and availability by drilling down in the report to display a smaller time frame. To drill down to a smaller time frame, click a range title.



Depending on the tracking period selected in the View box, clicking the range title displays the report with a smaller time range. For example, in a report with a day tracking period, clicking the range title displays the report with a two-hour tracking period:

Analyzing the Performance Matrix Report

The Performance Matrix report's color-coded cells enable you to analyze average transaction response times at a glance and get a quick snapshot of overall transaction health. For example, if most of the cells in the report are green, then average response times are generally OK. If most of the cells are red, then average response times are generally critical. Color coding is available only when the report is grouped by transactions.

Furthermore, when one or more transactions fail or exceed their outlier value within the tracking period represented by one cell in the table, a black **X** is displayed in the cell. Mercury Business Availability Center classifies transactions as outliers if they do not complete within a specified time range. You set outlier parameters in the transaction threshold settings in Monitor Administration. For details, see "Transaction Threshold Settings" in *End User Management Data Collector Configuration*.

In addition to the black X, 1 to 5 horizontal bars are used to signify transaction failure or outlier values as follows:

Icon	Description
	Less than 10% of the transactions failed or exceeded the outlier value.
	Between 10% to 30% of the transactions failed or exceeded the outlier value.
	Between 30% to 50% of the transactions failed or exceeded the outlier value.
	Between 50% to 70% of the transactions failed or exceeded the outlier value.
	Between 70% to 90% of the transactions failed or exceeded the outlier value.
	Over 90% of the transactions failed or exceeded the outlier value.

You use the black Xs and horizontal bars to analyze the frequency of failed and outlier transactions. For example, if many of the cells display black Xs, transactions are consistently failing or exceeding their outlier value over time. If black Xs appear only at certain times, but with 5 horizontal bars (over 90 percent failure rate), there may be a problem with server availability during specific time periods.

Triage Report

The Triage report displays transaction data organized by location, for Business Process Monitor profiles for the past day, or for any selected 24 hours. By default, the first 20 transactions are displayed. (This number is configurable. For details, see "Changing the Maximum Number of Transactions and Locations" on page 28.)

Data in the Triage report is organized by transactions and locations and includes a transaction breakdown graph and an error summary table. The report also includes information about the health of the transaction scripts running at the various locations (Script Health) and about the health of each collector sorted by location (Collector Health). Collector Health gives you an overall status when triaging end user problems, but can also be used when investigating current collector health.

You can access the Triage report from the Dashboard console or directly through the End User Management application. From this report, you can drill down to the Triage Raw Data report. (For details, see "Triage Raw Data Report" on page 34.)

You would use this report to verify the reasons for a problem in a certain profile.

This section includes the following topics:

- "Filtering Report Data" on page 24
- "Working With the Triage Report" on page 24
- "Changing the Maximum Number of Transactions and Locations" on page 28
- "Changing Last Ping Time and Last Data Time Parameters" on page 29

➤ "Incorporating a Triage Report into a Custom Report" on page 30

➤ "Notes" on page 30

Filtering Report Data

To filter report data, you can change the view, profile, or active filter:

➤ For details on choosing a view, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

➤ For details on choosing a profile, see "Selecting Profiles" in *Working with Applications*.

➤ For details on filtering queries, see "Filtering Data Using Active Filters" in *Working with Applications*.

You can print, format, and export the Triage report. For details, see "Sharing and Storing Reports" in *Working with Applications*.

Working With the Triage Report

This section explains how to access the Triage report, generate a report, work with the report, and modify the report.

To access the Triage report:

➤ **From Dashboard.** You can drill down to the Triage report from any configuration item (CI) of type Business Process Group or Business Process Step. Right-click the CI in the Console to display the context menu. Select **Go to Report** > **Triage report**.

The Triage report displays data for the profile, transaction, and location of the CI you chose here.

➤ **From the End User Management application.** Select **Applications** > **End User Management** > **Summary Reports** > **Triage**.

The Triage report displays data for the transactions and locations of the first profile on the list. (Click the **Profile** link to view the list of profiles.)

To work with the Triage report:

1 End User Management displays:

- The first 20 transactions and their first 20 locations. For details on changing this number, see "Changing the Maximum Number of Transactions and Locations" on page 28.
- An icon that shows whether transactions have finished successfully (**Script Health**).

  When a script in a profile is run, but for some reason does not finish successfully (that is, it does not end with a status of Finished properly or Finished (errors occurred)), samples for transactions that are part of the script but were not run are sent to Mercury Business Availability Center for inclusion in the Triage report.

  A yellow icon signifies that there are problems with the transaction. To view a tooltip showing at which location the script ran with errors, the host machine name, and the number of errors, place the pointer over the icon. The tooltip displays the errors sorted by location.

  A green icon signifies that there are no problems.
- An icon that shows the health of each collector sorted by location (**Collector Health**).

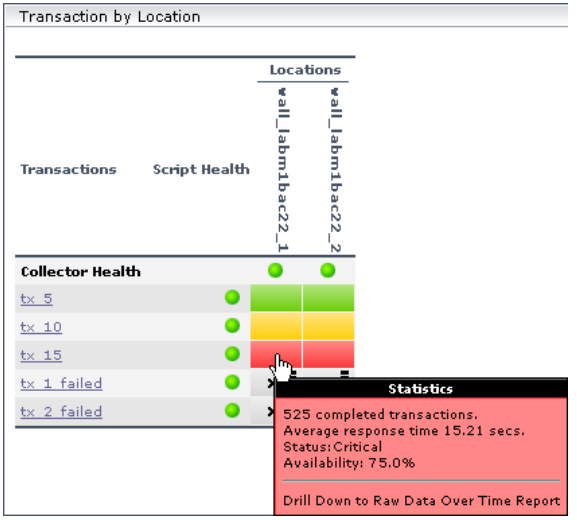
  A yellow icon signifies that a Business Process Monitor host has problems. To view a tooltip showing the host machine name, last ping time, and last data time of the problematic host machines, place the pointer over the icon.

  For details on changing the values, see "Changing Last Ping Time and Last Data Time Parameters" on page 29.

  A green icon signifies that there are no problems.
- Automatically generated transaction data. For details on setting reports to be automatically generated, see "Configuring Report Generation Settings" in *Platform Administration*.
- Transaction data for the first profile in the list, or for the profile, transaction, and location of the CI chosen in Dashboard, depending on how you accessed the Triage report.

2 To verify the threshold ranges for the transaction results, use the legend next to the table. Outlier ranges are also shown.

3 To view a tooltip showing statistics about completed transactions, average response time of each transaction, the status of the transaction at that location, and transaction availability, place the pointer over any colored cell in the table.



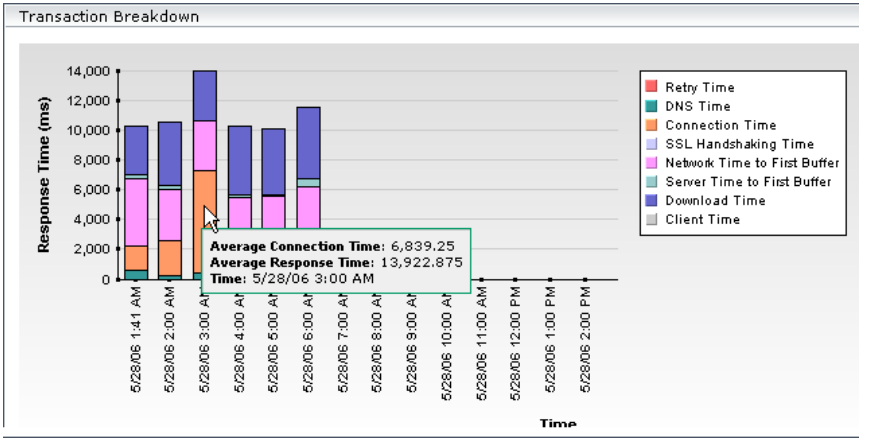
4 To drill down and view the raw data upon which the report is calculated, click a cell. The Triage Raw Data report shows data for the transaction and location whose results are shown in the cell you clicked.

To drill down and view the raw data for a transaction, click the transaction.

For details, see “Triage Raw Data Report” on page 34.

5 To view a tooltip containing details on the number of failed transactions as well as status and availability, place the pointer over a cell with a black X.

6 To view transaction breakdown data, scroll down to the Transaction Breakdown section. Each column in the Transaction Breakdown graph shows the average response time for all the transactions displayed in the Transaction by Location table, for that time.



Time granularity is as follows: on a time scale of 24 hours, points are displayed for each hour. On a time scale of less than two hours, points are displayed for every five minutes. For a discussion of transaction breakdown, see "Understanding the Transaction Breakdown Reports" on page 52.

7 To view data for each period, hold the cursor over a column.

8 To verify breakdown categories, use the legend next to the table.

9 To view a table of errors that occurred during a profile run, over a specified time period, scroll down to the Error Summary section. The Error Summary table includes the following information:

Error Category. Categories can be HTTP, General, Content, and Script. For details on these categories and on the way Business Process Monitor reports errors, see "Error Summary Report" on page 43.

Error Type. A description or code of the error that occurred during script execution.

Failed/Total Measurements. The number of transaction instances that failed due to the error, out of the total number of transaction instances that occurred during the specified time period.

Transactions/Total. The number of defined transactions that caused the error, out of the total number of transactions defined in the profile.

Locations/Total. The number of locations from which errors occurred, out of the total number of locations from which scripts ran.

➤ To view more errors, click the **Next page** or **Last page** buttons.

➤ To view previous errors in the list, click the **Previous page** or **First page** buttons.

To modify the report view:

1. Select a new time range or granularity. For details, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.
2. Choose a different profile from the profile list.
3. To view the report filtered by specific transactions or locations, apply active filters by clicking the **Active Filters** link, and selecting or clearing check boxes. For details, see "Filtering Data Using Active Filters" in *Working with Applications*.
4. To display the transactions and their locations, click **Generate**.

Changing the Maximum Number of Transactions and Locations

By default, End User Management displays 20 locations and 20 transactions. You can change this setting in the Infrastructure Settings Manager.

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

Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **End User/System Availability Management**, select **End User/System Availability Management.**

➤ Locate the **Max. number of transactions in Triage report filter** entry in the **End User/System Availability Management – Data** table. Update the value as required.

➤ Locate the **Max. number of locations in Triage report filter** entry in the **End User/System Availability Management – Data** table. Update the value as required.

Changing Last Ping Time and Last Data Time Parameters

When the Triage report is requested, Mercury Business Availability Center checks when the collector ping time and data time were last reported. By default, Mercury Business Availability Center compares these values to 60 minutes. If the last report time is higher than the default, a yellow icon is displayed in the Triage report. You can change this setting in the Infrastructure Settings Manager.

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

Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **End User/System Availability Management**, select **End User/System Availability Management**.

➤ Locate the **Max. time since last reported collector ping time** entry in the **End User/System Availability Management – Data** table. Update the value as required.

➤ Locate the **Max. time since last reported collector data time** entry in the **End User/System Availability Management – Data** table. Update the value as required.

Incorporating a Triage Report into a Custom Report

You can create a custom report from a Triage report. Create a report, choose the Triage Report component, and select the Triage report in the Add Component window. For details, see "Adding a Component to a Report" in *Application Administration*.

Notes

- The Triage report does not display deleted transactions, although End User Management does store transaction history.
- Once you have generated a Triage report with a specific profile and specific filters, End User Management displays the report with these parameters upon subsequent visits to the report, during the same Web session.

4

Business Process Reports

This chapter describes the Business Process reports and explains how to use them to understand the performance of your system.

This chapter describes:	On page:
About Business Process Reports	32
Triage Raw Data Report	34
Availability over Time Report	38
Response Time over Time Report	40
Transaction Analysis Report	42
Error Summary Report	43
Location Analysis Reports	51
Understanding the Transaction Breakdown Reports	52
Breakdown over Time Report	57
Breakdown Summary Report	59
Min./Max. Response Time Report	65
Desktop Performance Report	67
Response Time by Percentile Report	69

About Business Process Reports

Business Process reports provide you with an in-depth view of the health of your monitored environment. You access Business Process reports from the Business Process tab in the End User Management application.

For details on working with reports (choosing the time range, selecting the profile, saving and sharing reports, and so forth), see "Working in Reports" in *Working with Applications*.

The following reports are available:

Category	Description	For Details, See...
Availability over Time Report	Displays the percentage of successful transactions performed by all hosts in a profile—organized by transaction, location, or group—over time.	page 38
Response Time over Time Report	Displays the average response times (in seconds) of completed transactions—organized by transaction, location, or group—over time.	page 40
Transaction Analysis Report	Provides an in-depth picture of the performance of transactions.	page 42
Error Summary Report	Provides a detailed list—organized by error type—of errors that occurred during a profile run, over the specified time period.	page 43
Location Analysis Reports	Provides an in-depth picture of the performance of transactions, organized per defined location.	page 51

Category	Description	For Details, See...
Breakdown over Time Report	Helps you determine whether poor transaction response times are being caused by network or server problems, or by client delays, and enables you to pinpoint exactly when the problems are occurring.	page 57
Breakdown Summary Report	Enables you to assess whether poor transaction response times are being caused by network or server problems, or by client delays.	page 59
Min./Max. Response Time Report	Displays the minimum, average, and maximum response time (in seconds) of completed transactions—organized by transaction, location, or group.	page 65
Desktop Performance Report	Displays the availability, performance, and activity monitoring results for all Client Monitor Agents running on machines registered with Mercury Business Availability Center.	page 67
Response Time by Percentile Report	Displays, for the defined time range, the specific response time value that all measured response time values are equal to or below, for the 10th to 100th percentile, in 10% increments.	page 69

Triage Raw Data Report

The Triage Raw Data report displays performance and availability raw data for a Business Process Monitor transaction. You access the Triage Raw Data report by drilling down from the Triage report or through the End User Management application.

This section includes the following topics:

- "Filtering Report Data" on page 34
- "Working With the Triage Raw Data Report" on page 34
- "Incorporating a Triage Raw Data Report in a Custom Report" on page 37

Filtering Report Data

To filter report data, you can change the view, profile, or active filter:

- For details on choosing a view, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.
- For details on choosing a profile, see "Selecting Profiles" in *Working with Applications*.
- For details on filtering queries, see "Filtering Data Using Active Filters" in *Working with Applications*.

You can print, format, and export the Triage Raw Data report. For details, see "Sharing and Storing Reports" in *Working with Applications*.

Working With the Triage Raw Data Report

This section explains how to access the Triage Raw Data report, generate a report, work with the report, and modify the report.

To access the Triage Raw Data report:

- Select **Applications** > **End User Management** > **Business Process** > **Triage Raw Data**.

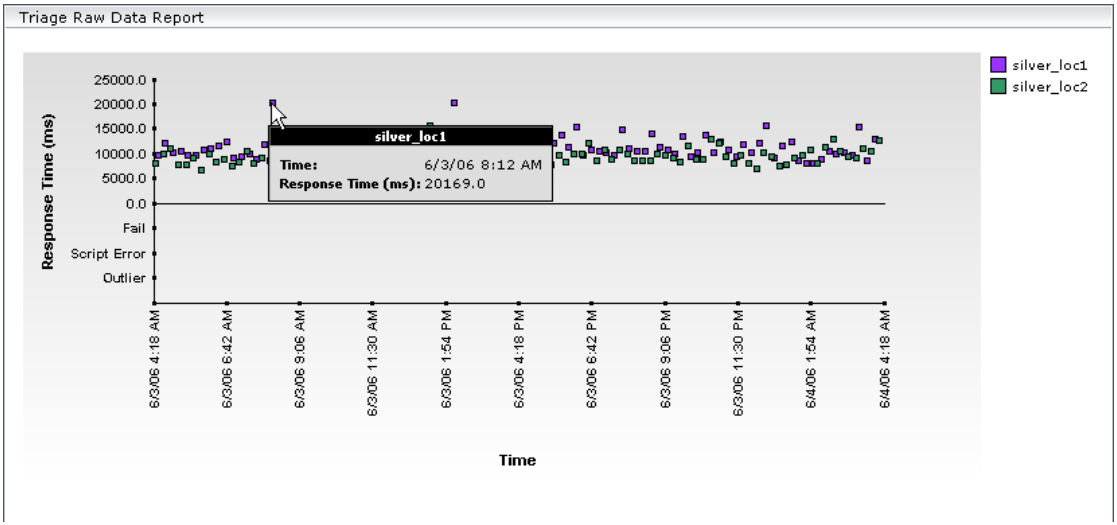
The Triage Raw Data report displays data for the first transaction and its locations, for the first profile on the list. (Click the **Profile** link to view the list of profiles.)

➤ Drill down from the Triage report (when the Triage Raw Data report opens in a new window).

The Triage Raw Data report displays data for the transactions and locations selected in the Triage report.

To work with the Triage Raw Data report:

1 To view a tooltip showing time and response time, hold the pointer over a data point.

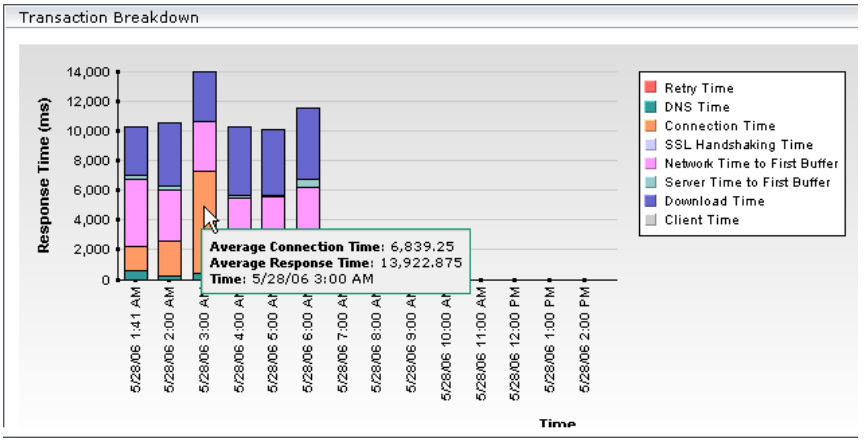


Failed transactions, script errors, and outlier data are shown below the raw data graph. To view a tooltip showing time and status, hold the pointer over a data point.

2 To verify location names, use the legend next to the table.

3 To view transaction breakdown data, scroll down to the Transaction Breakdown section. Each column in the Transaction Breakdown graph shows the average response time for all the transactions displayed in the

Triage Raw Data report above, for a specific time. This graph enables you to verify, for example, that at 9:00 AM a problem arose with the network.



Time granularity is defined as follows: on a time scale of 24 hours, points are displayed for each hour. On a time scale of one hour, points are displayed for each ten minutes. For a discussion of transaction breakdown, see "Understanding the Transaction Breakdown Reports" on page 52.

4 To view data for each period, hold the cursor over a column.

5 To verify breakdown categories, use the legend next to the table.

6 To view a table of errors that occurred during a profile run, over a specified time period, for the selected transaction and locations, scroll down to the Error Log section. The Error Log table includes detailed information about errors as follows:

Time. The time that the error occurred.

Category. Categories can be HTTP, General, Content, and Script.

Type. A description or code of the error that occurred during script execution.

Transaction. The name of the transaction that is in error.

Location. The name of the location of the transaction that is in error.

Script. The name of the script in which an error occurred.

File name. The name of the file in the script directory containing the script steps that were running when the error occurred.

Error line. The line in the file referenced in the File Name column at which the error occurred.

Error Message. The error message that Mercury Business Availability Center generates at the time of the error. If there is a partial message, point to it to view a tooltip with the full message. **Note:** For user-defined errors (error type -17999), Mercury Business Availability Center displays the user message.

Actions. For details on viewing and downloading snapshots, see "Snapshot on Error" on page 48. These buttons are enabled if the original Business Process Monitor script is configured to save snapshots. For details, see "Configuring Snapshot on Error" in *Business Process Monitor Administration*.

- ➤ To view more errors, click the **Next page** or **Last page** buttons.
- ➤ To view previous errors in the list, click the **Previous page** or **First page** buttons.

To modify the report view:

1. Select a new time range or granularity. For details, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.
2. Choose a different profile from the profile list.
3. To view the report filtered by a specific transaction, apply active filters by clicking the **Active Filters** link, and selecting another transaction. Note that you can select one transaction only to view in this report. For details on using Active Filters, see "Filtering Data Using Active Filters" in *Working with Applications*.
4. To display the Triage Raw Data report again, click **Generate**.

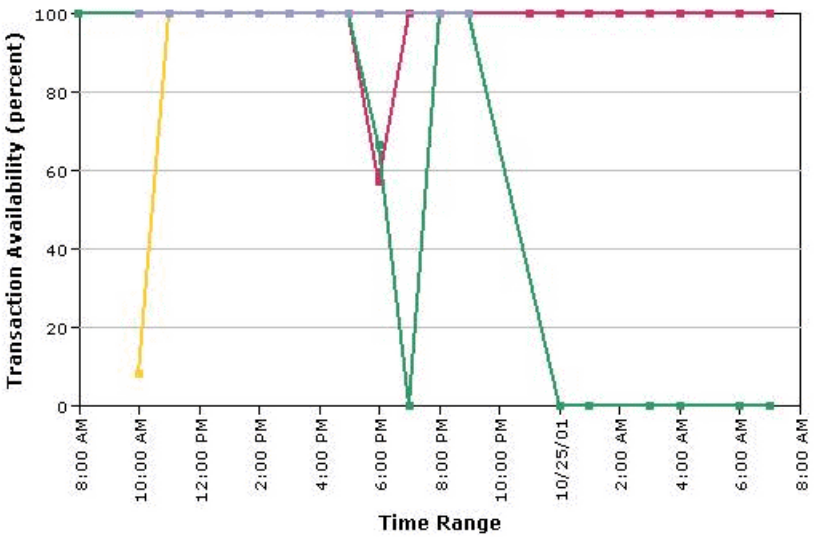
Incorporating a Triage Raw Data Report in a Custom Report

You can create a custom report from a Triage Raw Data report. Create a report, choose the Triage Report component, and select the Triage Raw Data report in the Add Component window. For details, see "Adding a Component to a Report" in *Application Administration*.

Availability over Time Report

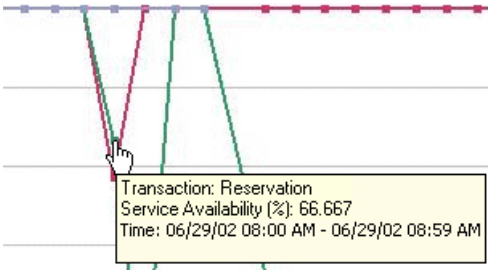
The Availability over Time report displays the percentage of successful transactions performed by all hosts in a profile—organized by transaction, location, or group—over time. The report can be viewed in either graph or table format.

The Availability over Time report helps you identify service availability problems and pinpoint their source. By breaking down the report by transaction, location, or group across different time frames, you can identify exactly where and when transaction failure rate is significant. For example, you determine that a transaction regularly fails during a particular time of day, which may indicate a problem with the transaction during periods of high Internet traffic.



Working with the Availability Over Time Report

➤ To view details about transaction availability at that point in time, place the cursor over any data point to display a tooltip containing information.



➤ To view the data in table format, click the **View as Table** tab.

The table displays service availability for the selected time frame, broken down by transaction, location, or group.

To focus on a specific time frame, transaction, location, or group, drill down in the table view. Click any link in a column or row header.

➤ To modify the report view, select **Transactions**, **Locations**, or **Groups** from the report view list, and click **Generate** to display the success rate of each transaction at each location, and for each group, across the selected time frame.

➤ To change the report time frame, use the **From** and **To** fields and the left and right arrows. Click **Generate** to generate the modified report.

➤ To change the active filters, click the **Active Filters** link, and select or clear check boxes, to view the report filtered by specific transactions, locations, or groups. Click **Generate** to generate the modified report.

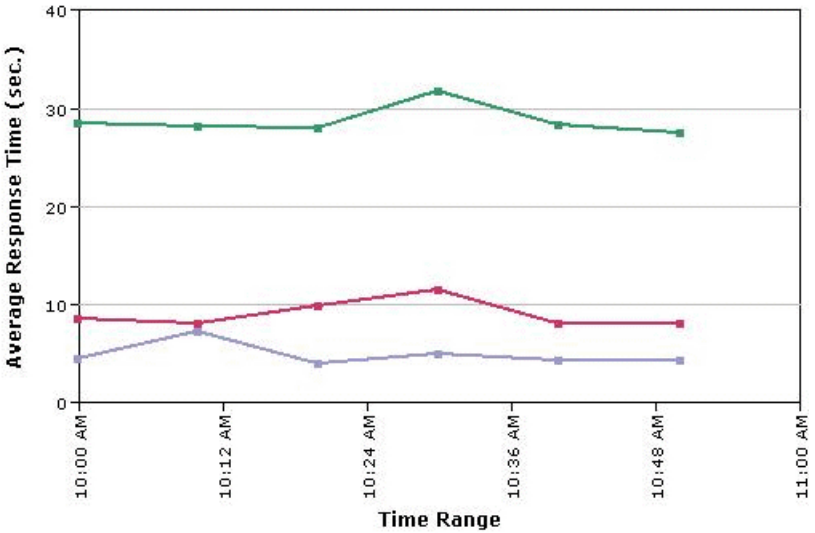
➤ To increase the time resolution for the selected transaction, location, or group, drill down in the graph view and click any time point in the graph.

➤ To focus on a specific transaction, location, or group, click any drill down link to the right of the report.

Response Time over Time Report

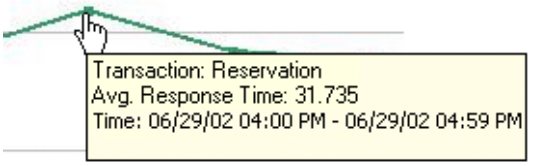
The Response Time over Time report displays the average response times (in seconds) of completed transactions—organized by transaction, location, or group—over time. The report can be viewed in either graph or table format.

The Response Time over Time report helps you identify response time problems and pinpoint their source. By breaking down the report by transaction, location, or group across different time frames, you can identify exactly where and when average transaction response times are too slow. For example, you might determine that a specific transaction's average response time is always higher on a certain day of the week, but only from a particular location. This might indicate a problem with the Internet Service Provider for that location during high Internet traffic periods.



Working with the Response Time over Time Report

➤ To view a tooltip containing details about the average response time of all completed transactions performed by hosts at the time period corresponding to that point, place your cursor over any data point.



➤ To view the data in table format, click the **View as Table** tab.

The table displays service availability for the selected time frame, broken down by transaction, location, or group.

➤ To focus on a specific time frame, transaction, location or group, drill down in the table view. Click any link in a column or row header.

➤ To modify the report view, select **Transactions**, **Locations**, or **Groups** from the report view list, and click **Generate** to display the success rate of each transaction at each location or for each group, across the selected time frame.

➤ To change the report time frame, use the **From** and **To** fields and the left and right arrows. Click **Generate** to generate the modified report.

➤ To change the active filters, click the **Active Filters** link, and select or clear check boxes, to view the report filtered by specific transactions, locations, or groups. Click **Generate** to generate the modified report.

➤ To increase the time resolution for the selected transaction, location, or group, drill down in the graph view and click any time point in the graph.

➤ To focus on a transaction, location, or group, click any drill down link to the right of the report.

Transaction Analysis Report

The Transaction Analysis report provides an in-depth picture of the performance of transactions. The report enables you to understand, for the selected profile and defined time frame:

- the average response times of your transactions over time
- whether poor transaction response times are being caused by network or server problems, or by client delays
- the availability level of your transactions
- how well your transactions performed relative to set transaction thresholds

---

Note: The Transaction Analysis report can be printed, sent by e-mail and exported to a Microsoft Excel file format. It cannot be exported to the .pdf format. For details about the formats it can be exported to, see "Sharing and Storing Reports" in *Working with Applications*.

Generating the Transaction Analysis Report and Sub-Reports

When you generate the Transaction Analysis report initially, the Performance Matrix is displayed. To analyze data for a specific time period or transaction, click a transaction, date, or cell within the main report. End User Management generates the sub-reports.

The Transaction Analysis report consists of the following components:

Report Category	Report Name	Description
Main report	Performance Matrix	Displays a color-coded representation of average transaction response times and failed transactions, over time. For details, see .

Report Category	Report Name	Description
Sub-reports	Average Response Times over Time	Displays average response times of successful transactions, over time. For details, see .
	Transaction Breakdown over Time	Displays a breakdown of average transaction response times, over time. For details, see .
	Service Availability over Time	Displays the percentage of successful transactions performed by all hosts in a profile, over time. For details, see .
	Overall Transaction Performance	Displays, for each transaction, the number and percentage of transaction instances whose response time falls into the OK, Minor, and Major threshhold ranges. In addition, displays the number and percentage of transaction instances that failed and how many of the failed instances are outliers. For details, see .
	Error Details	Displays a detailed list of transaction file errors that occurred while the selected Business Process profile ran during the specified time period. For details, see .

Error Summary Report

The Error Summary report provides detailed tables—organized by error type—of errors that occurred during a profile run, over the specified time period. Since not all errors cause transactions to fail, the Error Summary report includes errors for transactions that completed successfully as well as transactions that failed. The report also lists outlier transactions.

End User Management displays the following errors in the Error Summary page:

- **HTTP Errors.** Web server errors (for example, Error 404). These errors occur when the Web server indicates that it cannot respond to requests sent by the data collector.
- **Context Errors.** Errors in the context of the response generated for a request sent by a data collector (for example, an expected text or image that is not found).
- **General Errors.** All other error types.
- **Script Errors.** Transaction errors displayed in the Triage report. For details, see "Triage Report" on page 23.

Note: You can instruct Mercury Business Availability Center to display errors in either the HTTP Errors or Context Errors table, that by default appear in the General Errors table. For details, see "Modifying the Table in Which Errors Appear" on page 49.

For each error that occurs, End User Management displays the following information:

Error Type. A description or code of the error that occurred during script execution. Click the link to generate the Failed Transactions report. **Note:** The error code -17999 represents user-defined errors—errors defined in Mercury Virtual User Generator using the **lr_error_message** function.

Failed/Total Measurements. The number of transaction instances that failed due to the error, out of the total number of transaction instances that occurred during the specified time period.

Transactions/Total. The number of defined transactions that caused the error, out of the total number of transactions defined in the profile.

Locations/Total. The number of locations from which errors occurred, out of the total number of locations from which scripts ran.

This section includes the following topics:

- "Working with the Error Summary Report" on page 45
- "Outlier Transactions" on page 45

➤ "Failed Transactions Report" on page 46

➤ "Failed Transactions Report Filter" on page 47

➤ "Snapshot on Error" on page 48

➤ "Modifying the Table in Which Errors Appear" on page 49

Working with the Error Summary Report

For each error type, you can:

➤ drill down to the Failed Transactions report – for details, see "Failed Transactions Report" on page 46

➤ move errors displayed in the General Errors table to other error tables – for details, see "Modifying the Table in Which Errors Appear" on page 49

Outlier Transactions

The Outlier Transactions table provides information about the number of transactions that exceed their outlier value during a profile run. Mercury Business Availability Center classifies transactions as outliers if they are not completed within a specified time range. You set the outlier value in a profile's properties, in the Transaction Threshold settings. For details, see "Transaction Threshold Settings" in *End User Management Data Collector Configuration*.

End User Management provides the following information:

Outlier Total/Total Measurements – The number of outlier transaction instances, out of the total number of transaction instances that occurred during the specified time period.

Outlier Transactions/Total – The number of defined transactions that exceeded their outlier value, out of the total number of transactions defined in the profile.

Outlier Locations/Total – The number of locations from which transactions exceeded their outlier value, out of the total number of locations from which scripts ran.

Failed Transactions Report

The Failed Transactions report displays details about errors that occur during a script run. You also access the Snapshot on Error feature from the Failed Transaction report.

To generate the Failed Transactions report from the Error Summary report, click an error message in the Error Type column.

The Failed Transactions report provides some of the following information:

Time. The time and date at which the error occurred. If the report uses aggregated data, Mercury Business Availability Center displays the time as a link. Click the link to drill down to the time interval information until the raw error data is displayed, which includes Snapshot on Error information, if available. For details, see “Snapshot on Error” on page 48.

Transaction. The transaction for which the error occurred.

Location. The location at which the error occurred.

Script. The name of the script containing the transaction for which the error occurred.

File name. The name of the file in the script directory containing the script steps that were running when the error occurred.

Error line. The line in the file referenced in the File Name column at which the error occurred.

Message – The error message that Mercury Business Availability Center generated at the time of the error. If there is a partial message, point to it to view a tooltip with the full message. **Note:** For user-defined errors (error type -17999), Mercury Business Availability Center displays the user message.

Snapshot – A link that opens a window containing a snapshot of the application, as it would have been seen by a real user at the time of the error. A link that enables you to download the snapshot, in zipped format. For details, see "Snapshot on Error" on page 48.

Note: The following columns are not displayed when the Failed Transactions report uses aggregated data: File Name, Error Line, Snapshot. For details on data aggregation in Mercury Business Availability Center, see "Data Aggregation" in *Reference Information*.

You can also generate a Failed Transaction report from:

- the Transaction Analysis and Location Analysis reports – for details, see "Transaction Analysis Report" on page 42 and "Location Analysis Reports" on page 51. The report appears as a sub-report called Error Details.
- the Breakdown Summary report. Click the red **X** in the Errors column.

Failed Transactions Report Filter

When generated from the Error Summary report, the Failed Transactions report displays the **Display errors of this type only** option. If left selected, the report displays errors of the specified type (corresponding to the error type that was chosen in the Error Summary report). If cleared, upon report regeneration the report displays all error types. Note that once this option is cleared it cannot be reselected (to view a filtered report again, you must close the window and click a link in the Error Summary report again).

Snapshot on Error

When recording scripts with Mercury Virtual User Generator or QuickTest Professional (QTP), you can enable the Snapshot on Error option. For details, see below. Once enabled, during a script run Mercury Business Availability Center saves a snapshot of a page as it appears when an error occurs during the script run.

Mercury Business Availability Center supports Snapshot on Error for the following Mercury Virtual User Generator protocols:

- **Web protocols** – Oracle Web Applications 11i, PeopleSoft Enterprise, SAP-Web, Siebel-Web, and Web (HTTP/HTML)
- **Non-Web protocols** – Citrix_ICA, SAPGUI

You can access the recorded snapshot from the Failed Transaction report. There are two ways to access the snapshot:



- click the **View Snapshot** button to display the screen that is saved at the time of error. For Web protocols, the snapshot opens a new browser window and displays a page built from the HTML code that is saved at the time of error. Page resources, such as images, are displayed by linking to the original Web site—resources are not saved by Mercury Business Availability Center. For non-Web protocols, an image is displayed in the browser window.



- click the **Download Snapshot** button to download the snapshot in zipped format to a local or network drive. This method is recommended for viewing the actual HTML code of the saved page, for example, if the HTML code contains scripts which can be harmful if run. For Web protocols, to view the snapshot in a browser after unzipping it, you may need to add the BASE element to the HTML code specifying the original URL of the recorded Web site. This is necessary to see page resources if the original HTML page did not contain a BASE element. In addition, you may need to add the original URL to other HTML elements such as anchor tags and image source tags.

Note: When Mercury Business Availability Center records a snapshot for scripts recorded using one of the Web protocols, it saves only HTML code. Resources such as images and JavaScript are not saved. Thus, errors that occur due to missing resources may be difficult to trace later on from the snapshot, especially in cases where the missing resource problem has been fixed. For example, if an image resource is missing during a script run, causing an error to be recorded, but the missing image problem is later fixed, the image will be present when you open the snapshot of the page.

To enable the generation of snapshots when an error occurs in Mercury Virtual User Generator:

1. In the Mercury Virtual User Generator Run-Time Settings dialog box, select the **General: Miscellaneous** node.
2. In the Error Handling section, check that **Generate snapshot on error** is selected.
3. Click **OK** to close the Run-Time Settings dialog box.

To enable the generation of snapshots when an error occurs in QuickTest Professional:

1. In the Options dialog box, select the **Run** tab.
2. In the **Save step screen capture to results** box, select **On errors**.
3. Click **OK** to close the Options dialog box.

For additional information on configuring Snapshot on Error, see "Advanced Configuration Options" in *Business Process Monitor Administration*.

Modifying the Table in Which Errors Appear

By default, Mercury Business Availability Center displays errors in the General Errors table. You can change this configuration so that the errors are moved to one of the other error tables.

To modify the table in which errors appear:

1. Locate the following file on the Centers Server:
MercuryAM\AppServer\resources\TransactionError.properties
2. Locate the error message in this file that you want to move to the Context or HTTP Errors table.
3. Copy the value at the beginning of the row. For example, to add the error "The requested image not found" to the Context Errors table, locate:

```
-27987=The requested image not found
```

Copy **-27987**.

4. Locate the following file on the Centers Server:
MercuryAM\conf\settings\diagnostics.xml.
5. Search for the string:

```
# The two following settings define contents of sections "Context Errors"
and "HTTP Errors"
```

6. To list the error in the Context Errors table, locate the value list for the Context Errors setting.

   To list the error in the HTTP Errors table, locate the value list for the HTTP Errors setting.
7. Paste the error code that you copied from the **TransactionError.properties** file into the value list, separating entries with commas. For example, if you copied **-27987** to the Context Errors setting, the value list appears as follows:

```
<value type="string">
    -27987,-27979,-27730,-27729,-27195,-27190,-27187,-27127
  </value>
```

8. Save the **diagnostics.xml** file.

Location Analysis Reports

The Location Analysis report provides an in-depth picture of the performance of locations. The report enables you to understand, for the selected profile and defined time frame:

- the average response times of your transactions over time for each location in the profile
- how well your locations performed relative to the set transaction thresholds

Generating the Location Analysis Report and Sub-Reports

When you generate the Location Analysis report, Mercury Business Availability Center displays the Performance Matrix. To analyze data for a specific time period or transaction, click a location, date, or cell within the main report. Mercury Business Availability Center generates the sub-reports.

The Location Analysis report consists of the following components:

Report Category	Report Name	Description
Main report	Performance Matrix	Displays, over the defined time range, average response times of successful transactions for each location in the selected profile. For details, see "Performance Matrix Report" on page 18.

Report Category	Report Name	Description
Sub-reports	Average Response Time over Time	Displays, for the selected location(s), average response times of successful transactions, over time. For details, see "Response Time over Time Report" on page 40.
	Overall Location Performance	Displays, for each location, the number and percentage of transaction instances whose response times fell into the OK, Minor, and Critical threshold ranges. In addition, displays the number and percentage of transaction instances that failed and how many of the failed instances were outliers. For details, see "Location Performance" on page 12.
	Error Details	Displays a detailed list of script errors that occurred while the selected Business Process Monitor profile ran during the specified time period. For details, see "Failed Transactions Report" on page 46.

Understanding the Transaction Breakdown Reports

The transaction breakdown reports help you determine whether poor transaction response times are caused by network or server problems, or by client delays, and to pinpoint exactly when the problems are occurring. Transaction Breakdown reports display Business Process Monitor and Client Monitor data collected by scripts recorded using the Web (HTTP/HTML) protocol.

For details on the transaction breakdown reports, see "Breakdown over Time Report" on page 57 and "Breakdown Summary Report" on page 59. The Triage report also includes a transaction breakdown. For details, see "Triage Report" on page 23.

Note: Transaction breakdown is not supported by Business Process Monitors running scripts recorded in wininet mode in Mercury Virtual User Generator.

This section includes the following topics:

- "Understanding How Mercury Business Availability Center Breaks Down Transaction Response Times" on page 53
- "Understanding Transaction Breakdown Categories" on page 54
- "Understanding Download Time" on page 57

Understanding How Mercury Business Availability Center Breaks Down Transaction Response Times

When Mercury Business Availability Center runs a Business Process Monitor or Client Monitor script and measures response time for a specific transaction, Mercury Business Availability Center collects breakdown data—information about network/server activity during the transaction—for each component of every Web page accessed in the transaction.

Because Mercury Business Availability Center runs the script over multiple connections (in the same way a browser does when you access any URL), at any given moment in time there is typically an overlap in the various breakdown categories.

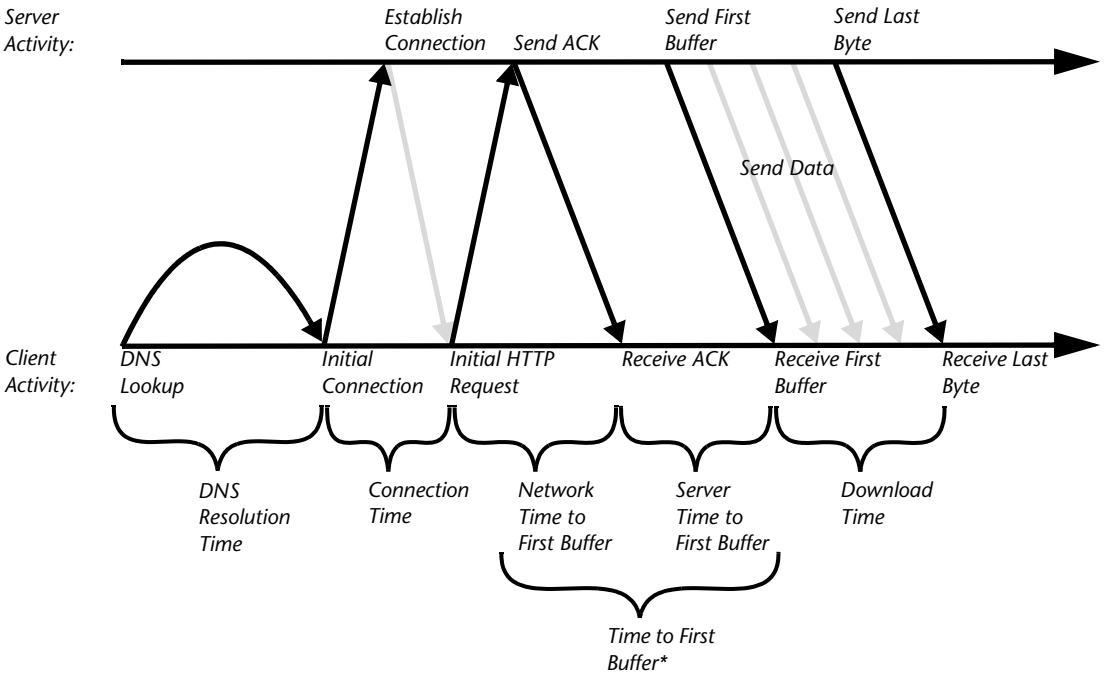
Mercury Business Availability Center uses a weighted algorithm to display the breakdown data that it collects. Every breakdown category for every element of the Web page is taken into consideration, and weight is given to the element according to its value relative to the other elements in the concurrent time period. For example, the DNS time for each element of the Web page is collected, weighted, and then displayed under the DNS time category.

Understanding Transaction Breakdown Categories

The transaction breakdown reports display a breakdown of average transaction response times (in milliseconds) over time, for the selected time frame. Response times are broken down by retry time, DNS resolution time, connection time, network time to first buffer, server time to first buffer, download time, and client time. If your site uses SSL authentication, SSL handshaking time appears in the chart after connection time.

The diagram below illustrates the relationship between the report's main breakdown categories (shown along the bottom of the diagram) and client/server activity during transaction execution.

Note that retry time, SSL handshaking time, and client time are not shown in this diagram (they are described in the table on page 55).



** Mercury Business Availability Center combines Network Time to First Buffer and Server Time to First Buffer*

The following table describes the report's breakdown categories. Times are calculated by taking the average of all transaction runs within the specified time period.

Name	Description
Retry Time	Displays the overall amount of time that passes from the moment an HTTP request is started until the moment an HTTP or TCP error message is returned. Retry time only relates to HTTP or TCP errors that execute a retry after the error.
DNS Resolution	Displays the average amount of time needed to resolve the DNS name to an IP address, using the closest DNS server. The DNS Lookup measurement is a good indicator of slow DNS resolution or other problems with the DNS server.
Connection Time	Displays the average amount of time needed to establish an initial connection with the Web server performing the transaction. The connection measurement is a good indicator of problems along the network or whether the server is responsive to requests.
SSL Handshaking Time	Displays the average amount of time taken to establish an SSL connection (includes the client hello, server hello, client public key transfer, server certificate transfer, and other—partially optional—stages). After this point, all the communication between the client and server is encrypted. The SSL handshaking measurement is only applicable for HTTPS communications.
Network Time to First Buffer	Displays the average amount of time that passes from the moment the first HTTP request is sent until receipt of ACK. The network measurement is a good indicator of network quality (look at the time/size ratio to calculate download rate).

Name	Description
Server Time to First Buffer	Displays the average amount of time that passes from the receipt of ACK of the initial HTTP request (usually GET) until the first buffer is successfully received back from the Web server. The server time to first buffer measurement is a good indicator of Web server delay. **Note:** Because server time to first buffer is being measured from the client, network time may influence this measurement if there is a change in network performance from the time the initial HTTP request is sent until the time the first buffer is sent.
Download Time	Displays the time from the receipt of the first buffer until the last byte arrives. Download time is a combination of server and network time, since the server typically sends data over multiple connections, and therefore is usually working while data is being transmitted over the network. For more details, see "Understanding Download Time" on page 57.
Client Time	Displays the average amount of time that passes while a request is delayed on the client machine. Client-related delays can include browser think time, CPU think time, HTML page processing time, time needed to open sockets, application delays caused by heavy applets, and so forth. **Note:** Client time is calculated by subtracting all other measured times from the total transaction time.

Note: In certain circumstances, for example, when the Business Process Monitor is using a proxy server, the transaction breakdown mechanism cannot differentiate between server time to first buffer and network time to first buffer. In these cases, the report displays the time between initial HTTP request and receipt of first buffer as Time to First Buffer.

In addition, the Client Monitor does not measure server time. Reports generated from monitor data show the time to first buffer only.

Understanding Download Time

When a Business Process Monitor running a script communicates with a Web server (specified by the URL(s) in the script), communication is carried out, by default, over four connections simultaneously.

As the Web page is retrieved, its various components (images, applets, and so forth) travel in data packets from server to client across these multiple connections.

As a result, at any point along the time line after the server sends the first buffer until the client receives the last byte for the page, data packets may be traveling over the network through some of the connections while others are being processed by the server through the remaining connections. The download time in the report represents the sum total of the time when network resources and server resources are in use at the same time, between the time the client receives the first buffer and the last byte.

Breakdown over Time Report

The Breakdown over Time report helps you determine whether poor transaction response times are being caused by network or server problems, or by client delays, and enables you to pinpoint exactly when the problems are occurring. Using the time range selector and active filters, you can highlight the exact time and source of a poorly performing transaction.

For information on the breakdown categories used in the report, see "Understanding the Transaction Breakdown Reports" on page 52.

This section contains the following topics:

➤ "Working with Breakdown over Time Report Data" on page 58

➤ "Correlating Breakdown over Time Report Data with Other Reports" on page 58

Working with Breakdown over Time Report Data

The Breakdown over Time report's color-coded graph enables you to quickly differentiate between retry time, DNS resolution time, connection time, SSL handshaking time (if relevant), network time to first buffer, server time to first buffer, download time, and client time.

For example, you might use the report to determine that download time is higher than usual for a transaction named Search_Flights. You could generate the Breakdown over Time report, filtered to the transaction Search_Flights, to determine the exact hour at which download time was slow. You could then view the for the same time period to determine whether there were problems with the network during this time period. In addition, you could check during the same time period.

Correlating Breakdown over Time Report Data with Other Reports

You can cross-reference transaction breakdown data with data in other reports. For example:

➤ To analyze the source of high download time, you can analyze server performance in reports to pinpoint potential server-side problems. For details, see .

➤ To analyze the source of slow network times, click anywhere in the transaction breakdown bar except the Retry Time, Server Time to First Buffer, or Download segments to open the WebTrace by Location report for the current time period. To ensure meaningful correlation between the transaction breakdown data and the WebTrace data, it is recommended that you configure WebTrace to access the same server(s) that your transactions are accessing. For details on the WebTrace over Time report, see . For details on configuring WebTrace monitors, see "Defining Traceroute Monitors and Editing WebTrace Monitors" in *Monitor Environment Setup*.

You can:

- Place your cursor over a color-coded segment to get statistics relevant to that portion of the bar.
- Click the **View as Table** tab, to view the data in table format.

  The table displays transaction breakdown information in table format, distributed over the selected time frame. Click the drilldown links in the table to view WebTrace data.
- Modify the report time frame and click **Generate** to generate the modified report.
- Apply active filters. Click the **Active Filters** link, and select or clear check boxes to view the report filtered by specific transactions, locations, or groups.

Breakdown Summary Report

The Breakdown Summary report helps you determine whether poor transaction response times are being caused by network or server problems, or by client delays. The report can be organized by transaction, location, or group, and can be viewed in either graph or table format.

For information on the breakdown categories used in the report, see "Understanding the Transaction Breakdown Reports" on page 52.

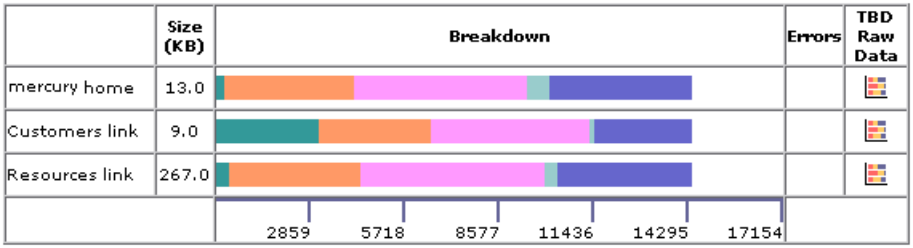
This section contains the following topics:

- "Working with Breakdown Summary Report Data" on page 60
- "Correlating Breakdown over Time Report Data with other Mercury Business Availability Center Reports" on page 61
- "Using the Error and TBD Raw Data Links" on page 61
- "Further Analyzing Breakdown Summary Report Data" on page 64

Working with Breakdown Summary Report Data

The Breakdown Summary report's color-coded graphs breaks down transaction times into retry time, DNS resolution time, connection time, SSL handshaking time (if relevant), network time to first buffer, server time to first buffer, download time, and client time. The report further displays, for the selected time frame, the size (in KB) of all pages in the transaction, and the average time it takes for each transaction to be completed (table format only).

In graph format, the report's x-axis is not a time line, but rather an indicator of transaction times in milliseconds. Each colored bar represents the total time for its corresponding measurement.



By correlating transaction response time information with Breakdown Summary report data, you can assess whether poor transaction response times are being caused by DNS resolution or connection problems, network latency or server delay, or client delay.

For example, using the Min./Max. Response Time report, you may determine that average response time for a transaction being run from a particular location is close to the maximum transaction time, indicating poor response times for the transaction at that location. By viewing the Breakdown Summary report for that transaction and location, you may discover that server time to first buffer is unusually high. This could indicate a problem with the Web server serving the region in which the host is located.

Furthermore, you can calculate the download rate by looking at the size measurement and time measurement. This can help you assess whether the transaction is too large or too slow.

Correlating Breakdown over Time Report Data with other Mercury Business Availability Center Reports

You can cross-reference transaction breakdown data with data in other Mercury Business Availability Center reports. For example:

- to analyze the source of high download time, analyze server performance in the System Availability Management reports to pinpoint potential server-side problems. For details, see "Cross-Performance Report" in *Using System Availability Management*.
- to analyze the source of slow network times, click anywhere in the transaction breakdown bar except the Retry Time, Server Time to First Buffer, or Download segments to open the WebTrace by Location report for the current time period. To provide meaningful correlation between the transaction breakdown data and the WebTrace data, it is recommended that you configure WebTrace to access the same server(s) that your transactions are accessing. For details on the WebTrace over Time report, see "WebTrace by Location Report" on page 173. For details on configuring WebTrace addresses, see "Defining Traceroute Monitors and Editing WebTrace Monitors" in *End User Management Data Collector Configuration*.
- to analyze the source of slow Server Time to First Buffer or Download times, click the appropriate segment to open Mercury Diagnostics (a licensed version of Mercury Diagnostics is required). For details, refer to *Mercury Diagnostics Installation and User's Guide*.
- to trace the cause of retry time, click the **Retry Time** segment to open the Failed Transactions table, which details transaction errors for the defined time range. For details, see "Failed Transactions Report" on page 46.

Using the Error and TBD Raw Data Links

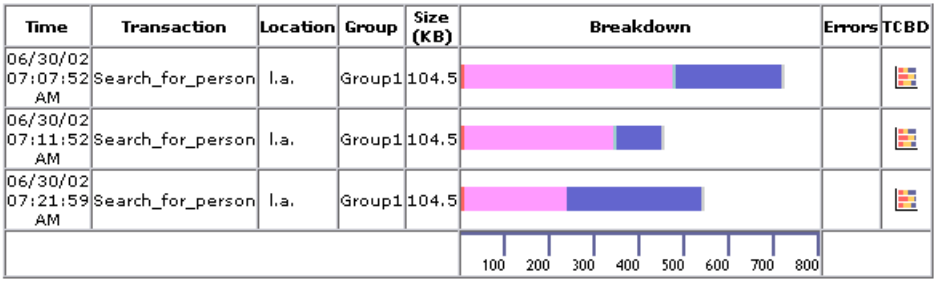
In addition to the breakdown bars, the report displays links in the far right columns for the following scenarios:

- if errors occurred while downloading some of the page components, the report displays a red **X** in the Errors column. Click the red **X** to open the Failed Transactions table, which details page component download errors for the defined time range. For details, see "Failed Transactions Report" on page 46.

Note: To view errors that occurred while downloading page components in the Failed Transactions table, you must have enabled transaction breakdown error reporting in the profile (for the transaction monitor containing the transaction with errors). For details on enabling or disabling transaction breakdown error reporting, see "Enable/Disable Reporting of Additional Error Information" in *End User Management Data Collector Configuration*.

➤ if you enabled Page Component Breakdown for the transaction monitor when creating the profile, and if page component breakdown data exists for the selected time range, the report displays an icon in the TBD Raw Data column (TBD = **transaction breakdown**). For details on enabling Page Component Breakdown and setting the page component breakdown data sampling rate, see "Enable/Disable Page Component Breakdown (Business Process Profiles Only)" in *End User Management Data Collector Configuration*.

Click the icon to drill down to the Transaction Breakdown Raw Data report, showing a summary of every instance of the transaction that occurred during the selected time range. Click segments of the bar to drill down, as described in "Correlating Breakdown over Time Report Data with other Mercury Business Availability Center Reports" on page 61.



To drill down further to the Component Breakdown report for a specific transaction instance, click any icon in the TCBD column (TCBD = **transaction component breakdown**). Note that Mercury Business Availability Center only saves complete Component Breakdown data for a sample of transaction instances.

The Component Breakdown report breaks down the transaction by page component. This enables you to analyze whether slow response times are being caused by a particular component of your Web page (for example, an image that is too large). For detail on the Page Component Breakdown report, see "Page Component Breakdown Tool" on page 178.

Page	Component	Component Size (KB)	Total Time (ms)	Breakdown
http://mportal.merc...	http://d...nder.asp	32.3	50.0	
	http://d...ortal.js	0.1	10.0	
	http://d...ortal.js	0.1	10.0	
	http://d...blue.gif	0.2	110.0	
	http://d...trns.gif	0.1	0.0	
	http://d...nder.gif	4.6	10.0	
http://mportal.merc...	http://d...ormation	27.0	511.0	
	http://d...ortal.js	0.1	10.0	
	http://d...rnav.gif	0.3	0.0	
	http://d...nder.gif	2.8	0.0	
	http://d...c_hp.gif	0.3	151.0	
	http://d...vbot.gif	0.3	10.0	
	http://d...pict.gif	0.4	10.0	
				100 200 300 400 500 600 700 800

Note: You can also generate an on-demand Page Component Breakdown report using the Page Component Breakdown tool. For details, see "Page Component Breakdown Tool" on page 178.

Further Analyzing Breakdown Summary Report Data

You can further analyze the Breakdown Summary report data as described below:

- place your cursor over a color-coded portion of any bar in the Breakdown column to get statistics relevant to that portion of the bar
- to view the data in table format, click the **View as Table** link

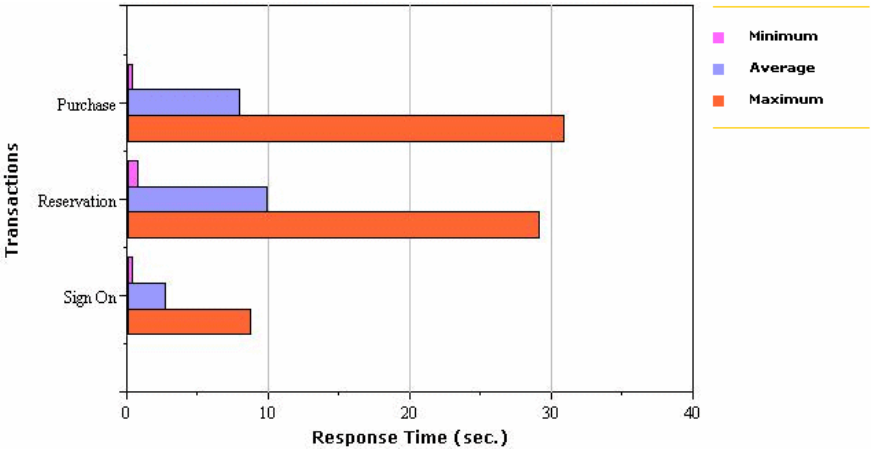
  The table displays transaction breakdown information in table format, distributed over the selected time frame. Click the drill down links in the table to view Failed Transaction, WebTrace, or Diagnostics (if available) data.
- to modify the report view, select **Transactions**, **Locations**, or **Groups** from the report view list, and click **Generate**:

Select:	To...
Transaction	Display the breakdown by transaction.
Location	Display the breakdown by location.
Group	Display the breakdown by group.

- modify the report time frame and click **Generate** to generate the modified report
- apply active filters. Click the **Active Filters** link, and select or clear check boxes to view the report filtered by specific transactions, locations, or groups

Min./Max. Response Time Report

The Min./Max. Response Time report displays the minimum, average, and maximum response time (in seconds) of completed transactions—organized by transaction, location, or group—for the selected time frame. The report can be viewed in either graph or table format.



Analyzing the Min./Max. Response Time Report

The Min./Max. Response Time report helps you identify the best- and worst-case response time scenarios, relative to average response time. Maximum response time is a particularly important measurement, as slow response times translate to a poor end-user experience.

By breaking down the report by transaction, location, or group across different time frames, you can identify exactly where and when maximum transaction response time is too slow, relative to the average. For example, you may determine that a specific transaction, being run in a group emulating Mozilla browsers, always returns a response time well above the average. This may indicate a problem with the HTML code that only affects users running Mozilla.

Further Analyzing Min./Max. Response Time Report Data

You can further analyze the Min./Max. Response Time report data as described below:

In addition to the minimum, average, and maximum response times by transaction, location, or group measurements, you can view the total number of counted transactions.

To view the total number of counted transactions:

1. Drill down in the table view by clicking any link in a row header to focus on a transaction, location, or group.
2. To modify the report view, select **Transactions**, **Locations**, or **Groups** from the report view list, and click **Generate**:

Select:	To...
Transaction	Display the minimum, average, and maximum response time for each defined transaction.
Location	Display the minimum, average, and maximum response time at each location.
Group	Display the minimum, average, and maximum response time for each group.

3. Modify the report time frame and click **Generate** to generate the modified report.
4. Apply active filters. Click the **Active Filters** link, and select or clear check boxes to view the report filtered by specific transactions, locations, or groups.
5. Drill down in the graph view. Click any bar chart in the report to focus on the corresponding transaction, location, or group.

Desktop Performance Report

The Desktop Performance report displays the availability, performance, and activity monitoring results for all Client Monitors running on machines registered with Mercury Business Availability Center. You use the report to view the worst- or best-performing Client Monitor results.

Performance results are graded OK, Minor, or Major according to the transaction thresholds defined in Monitor Administration. For details on setting thresholds, see "Transaction Threshold Settings" in *End User Management Data Collector Configuration*.

Note that if no Client Monitor profile has been defined, the link to the Desktop Performance report does not appear in the Business Process tab.

Choosing Desktop Performance Report Criteria

When generating the Desktop Performance Report, you can choose from the following criteria:

- **Show the x least/most available desktops (transaction success)** – the list is sorted by availability, according to the following calculation:

  (OK + Warning + Poor) / (OK + Warning + Poor + Failed)

- **Show the x worst/best performing desktops (transaction response time)** – the list is sorted by response time, according to the following calculation:

  (OK + (Warning x 0.5)) / (OK + Warning + Poor)

- **Show the x least/most active desktops (number of transactions)** – the list is sorted according to the number of transactions that ran during the specified time period.

Note: Any desktops running zero transactions are not listed when the report is sorted by least available desktops or least active desktops. Any desktops showing an availability of 0% are not listed when the reported is sorted by the worst-performing desktops.

Understanding the Desktop Performance Report

The Desktop Performance report displays the following information:

Desktop Name	Desktop Address	Location	Performance	Availability %	Failed Transactions	Total Transactions
WAYBUS_Obs	151.161.28.87	M2-247		90 %	67	722
Raisin	151.161.28.44	M2-247		94 %	25	441
USA	151.161.28.82	M2-248		97 %	31	1211
conquest	151.161.28.98	M2-248		99 %	18	7598
Root	151.161.28.145	M2-252		99 %	15	2502

- **Desktop Name** – the name of the machine on which the Client Monitor Agent is running.
- **Desktop IP Address** – the IP address of the machine on which the Client Monitor Agent is running.
- **Location** – the location of the Client Monitor Agent.
- **Performance** – desktop quality, sorted if **Show the x worst/best performing desktops** is selected. To see the OK, Minor, and Major percentages, hold the cursor over a color in the Performance bar.
- **Availability** – the percentage of time that the desktop was available.
- **Failed transactions** – the number of transactions that did not succeed, that is, that are not included in the OK, Minor, and Major calculations.
- **Total transactions** – the total number of transactions monitored by the Client Monitor Agent.

Further Analyzing Desktop Performance Report Data

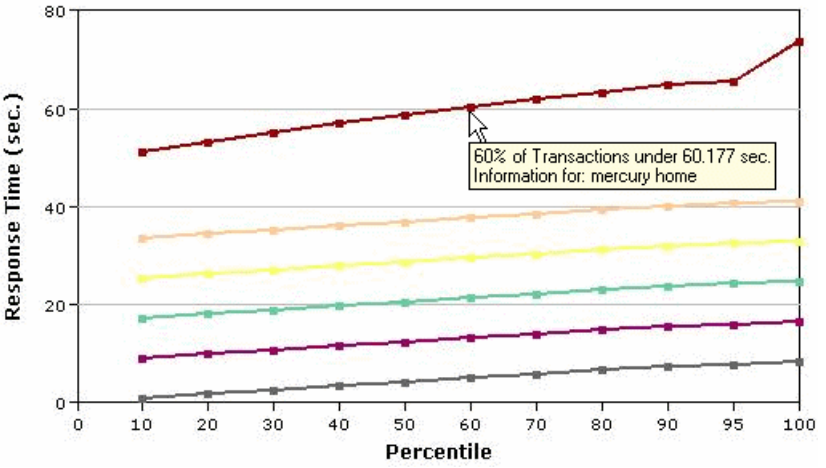
You can further analyze the Desktop Performance report data as described below:

- modify the report time frame and click **Generate** to generate the modified report
- apply active filters. Click the **Active Filters** link, and select or clear check boxes to view the report filtered by specific transactions, locations, groups, or desktops.

➤ to focus on a particular desktop, you can filter out data from other desktops: Click the **Active Filters** link, and choose the **Desktops** tab. Select **Specific Desktop**, and enter the name of the desktop. Click **OK**. You can also filter the list of results to focus on specific transactions, locations, or groups.

Response Time by Percentile Report

The Response Time by Percentile displays, for the defined time range, the specific response time value that all measured response time values are equal to or below, for the 10th to 100th percentile, in 10% increments. You can view the data in either chart or table format.



In the above chart, 60% of the transactions that ran during the defined time range had response times equal to or below 60.177 seconds.

The Response Time by Percentile data helps you identify response time problems and pinpoint their source. The data enables you to determine whether the highest or lowest response times are not typical of response times in general. For example, if the top 10 percent of transaction response times are significantly higher (for example, because they ran during a server reboot), there would be a sharp increase in the chart slope between the 90th and 100th percentile.

The data also enables you to spot response time trends. For example if the slope of the line suddenly increases at the 50th percentile point, something has caused transaction response times to significantly increase during that time period.

By filtering the data by transaction, location, or group across different time frames, you can identify exactly where and when transaction response times are too slow. You configure filter settings in the Custom Report Manager.

You can further analyze the Response Time by Percentile data as described below:

- place your cursor over any small square along the chart to view a tooltip containing details about the specific response time value that all response time values were equal to or below, at the selected percentile.
- modify the report time frame and click **Generate** to generate the modified report.
- drill down in the chart view. Click any drill down link to the right of the report, to focus on that transaction, location, or group.
- drill down in the table view. Click any link in a row header to focus on a specific transaction, location or group.
- select the table view in the Custom Report Manager to display the report in table format.

  The table displays, for the 10th to 100th percentile (in 10 percent increments), the specific response time value that all response time values were equal to or below. You can view the table broken down by transaction, location, or group.
- apply component filters in the Custom Report Manager. Click the **Component Filters** button, and select or clear check boxes to view the report filtered by specific transactions, locations, or groups.

5

Real User Monitor Reports

You use Mercury Real User Monitor reports to view page, transaction, end-user, server, and global statistic data collected by Real User Monitor, as well as a log of user sessions, information on sessions over time, and a summary of errors and events.

This chapter describes:	On page:
Overview of Real User Monitor Reports	72
Working with Real User Monitor Reports	75
Global Statistics Report	86
Page Summary Report	94
Transaction Summary Report	113
End User Summary Report	129
Server Summary Report	133
Session Analyzer Report	139
Event Count Over Time Report	150
Event Summary Report	152
Business Process Distribution Report	155
Network Latency Report	160
HTTP Error Codes	162

Note:

- To view Real User Monitor reports, you must first perform the steps described in *Real User Monitor Administration*.
- The availability of report data to a specific user is dependent on the access permissions granted that user. For details on granting permissions, see "Configuring User Permissions" in *Platform Administration*.
- In the Session Analyzer, Event Count Over Time, and Event Summary reports, the data is relevant to a specific application that you select when generating the report, whereas in all the other reports, the data is relevant to all of the applications configured for the Real User Monitor engine.

Overview of Real User Monitor Reports

Real User Monitor reports enable you to monitor the experience of real users that access your application, regardless of the location of these users. This helps you track real-user performance and availability, and assess the business impact of your application on real users across multiple domains and geographical regions.

For details on working with reports, see "Working in Reports" in *Working with Applications*.

There are ten types of Real User Monitor reports:

Global Statistics

The Global Statistics report contains six tables displaying general page, end-user, and broken link data that is not related to the specific pages and end-users that you define for Real User Monitor in Monitor Administration. To configure monitoring settings for Global Statistics report data, see "Data Reporting Settings" in *End User Management Data Collector Configuration*.

Page Summary

The Page Summary report displays data for the monitored Web pages that you configure in Monitor Administration. For information on configuring Web pages to be monitored, see "Configuring Pages" in *End User Management Data Collector Configuration*.

Transaction Summary

The Transaction Summary report displays data for monitored transactions that you configure in Monitor Administration. For information on configuring transactions to be monitored, see "Configuring Transactions" in *End User Management Data Collector Configuration*.

End User Summary

The End User Summary report displays data for monitored end-user groups that you configure in Monitor Administration. For information on configuring end-user groups to be monitored, see "Configuring End-User Groups" in *End User Management Data Collector Configuration*.

Server Summary

The Server Summary report displays data for the servers that are monitored by the Real User Monitor probe. For information on configuring the probe to monitor specific servers, see "Configuring a Probe" in *End User Management Data Collector Configuration*. To assign a specific name to a monitored server, see "Defining a Server Name" in *End User Management Data Collector Configuration*.

Session Analyzer

The Session Analyzer report displays data for all sessions in monitored applications that you configure in Monitor Administration. Sessions in applications that have not been configured for monitoring are also reported as part of a default entity for other applications in the Real User Monitor engine. For information on configuring applications to be monitored, see "Configuring Applications" in *End User Management Data Collector Configuration*.

Event Count Over Time

The Event Count Over Time report displays data for all events in monitored applications that you configure in Monitor Administration, broken down by time intervals. For information on configuring applications to be monitored, see "Configuring Applications" in *End User Management Data Collector Configuration*.

Event Summary

The Event Summary report displays a summary of events in monitored applications that you configure in Monitor Administration. For information on configuring applications to be monitored, see "Configuring Applications" in *End User Management Data Collector Configuration*.

Business Process Distribution

The Business Process Distribution report shows transaction run and transaction response time data over time for the transactions that you configure in Monitor Administration. For information on configuring transactions to be monitored, see "Configuring Transactions" in *End User Management Data Collector Configuration*.

Network Latency Report

The Network Latency report shows the average network latency (defined as the time it takes for a packet of data to get from one designated point to another and return to the original point) per end-user location for the transactions that you configure in Monitor Administration. For information on configuring transactions to be monitored, see "Configuring Transactions" in *End User Management Data Collector Configuration*.

Note: You can also create custom reports and trend reports using Real User Monitor data. For details on creating these reports, see "Configuring and Viewing User Reports" in *Working with Applications*.

Working with Real User Monitor Reports

When generating reports, you can specify various report settings, including time range and resolution. You can also print a report you generate, e-mail the report, or open the report in Microsoft Excel or PDF format. For the Session Analyzer, Event Count Over Time, Event Summary, and Network Latency reports, you can also open the report in XML format, publish the report, or save the report to the report repository. For details on working with reports, see "Working in Reports" in *Working with Applications*.

Note:

- When working with the Real User Monitor summary reports, if you select **Week**, **Month**, **Quarter**, **Year**, **Past Week**, **Past Month**, **Past Quarter**, or **Past Year** from the **View** box, Mercury Business Availability Center rounds the query to full days, 12 AM to 12 AM, based on the time zone set for the database (set by the database administrator in Platform Administration). The query is based only on aggregated data—not raw data—and can therefore be processed more quickly. The data is displayed according to the time zone set for the user, which is indicated on the right-hand side of the report title bar.
- Data for servers (which can be seen in the Server Summary, Server Over Time, and Global Statistics reports) as well as data for end-user groups (which can be seen in the End User Summary, End User Over Time, and Global Statistics reports) is aggregated by the Real User Monitor engine for each five minute period, and is then reported as such to Mercury Business Availability Center. This means that you will not see a real picture of such data if you view one of these reports using a time breakdown of less than five minutes.

Modifying the Maximum Number of Rows Displayed in a Table

By default, each table in a report displays a maximum of 20 rows. If you are a system administrator, you can change the default number of rows displayed by modifying the **Max Table Rows in Real User Monitor Reports** setting. To access this setting, click **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, select **End User/System Availability Management** in the **Applications** context, and scroll down to the **End User/System Availability Management - Data** table.

Modifying the Maximum Number of Rows Returned for the Session Analyzer Report and Event Log

By default, the maximum number of rows that are returned from the database for the Session Analyzer report and the Event Log, which is accessed by drilling down from the Event Summary report, is 200. If you are a system administrator, you can change the default number of rows displayed by modifying the **Max rows returned from the database in EUM Reports** setting. To access this setting, click **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, select **End User/System Availability Management** in the **Applications** context, and scroll down to the **End User/System Availability Management - Data** table.

Enabling Summary Rows

If you are a system administrator, you can configure Mercury Business Availability Center to display a summary row in Real User Monitor summary reports. To access this setting, click **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, select **End User/System Availability Management** in the **Applications** context, and scroll down to the **End User/System Availability Management - Data** table. Setting the option **Show Summary Row in Real User Monitor Summary Reports** to **true** enables the summary row to be displayed. Note that enabling the summary row may cause some delay in generating the summary reports.

Note: The summary row takes into account pages that you cannot view in the table if you have activated the thresholds filter. It does not take into account pages that have been filtered out using the other active filter tabs.

Customizing Real User Monitor Reports

All the Real User Monitor reports can be configured for auto generation. In addition, the Session Analyzer, Event Count Over Time, and Event Summary reports, as well as the Session Details, Pages Details and Event Log pages accessed when drilling down within reports, can be customized to achieve different behavior, looks, and displays. The features available for customization in these reports and pages are:

- The addition of headers and footers.
- Changing report elements for different looks and displays.

For details on customizing reports, see "Customizing Reports" in *Platform Administration*.

Drilling Down Within Real User Monitor Reports

In each of the reports, except the Global Summary report, it is possible to drill down to view more detailed information about end-user groups, pages, events, transactions, servers, and sessions, depending on the specific report.

When you drill down to a more detailed view, the report is regenerated so that the detailed view contains the most up to date data.

When returning to the original report by clicking on the breadcrumb at the top of the page, the report is once again regenerated to display the most up to date data. This is not applicable to the Session Analyzer, Event Count Over Time, and Event Summary reports, which do not get regenerated and for which the original report is redisplayed. (For information on breadcrumbs, see "Navigating Mercury Business Availability Center" in *Getting Started with Mercury Business Availability Center*.)

Drilling Down to Mercury Diagnostics Reports

If Mercury Diagnostics has been registered and enabled on your Mercury Business Availability Center system, you can drill down directly to the Mercury Diagnostics Server Requests view from the Real User Monitor Page Summary report and the Page Summary Over Time report. For details on registering and enabling Mercury Diagnostics in Mercury Business Availability Center, see "Mercury Diagnostics and Mercury Business Availability Center Integration" in *Application Administration*. For details on working with the Mercury Diagnostics Server Requests view, refer to the *Mercury Diagnostics Installation and User's Guide*.

Notes and Limitations

- If the URL of a page you have configured for monitoring in Monitor Administration has passed through a Web server that uses URL rewriting, the URL in Real User Monitor will differ from the corresponding URL in Mercury Diagnostics and a match will not be found when drilling down.
- If an application is installed on multiple servers working behind a load balancer, the URL of a page in Real User Monitor will have multiple corresponding URLs in Mercury Diagnostics. In such a case, when you drill down to the Server Requests view in Mercury Diagnostics all the corresponding URLs will be displayed, but only one of those URLs will be selected.
- When you drill down to the Server Requests view in Mercury Diagnostics from a Real User Monitor report, you will only view server requests that are included in the slowest 100 server requests in Mercury Diagnostics.
- Parameters aggregation is enabled by default in the Diagnostics Probe points file. If you have turned off parameter aggregation in the Probe points file, and the URL that you are drilling down from in the Real User Monitor report includes a parameter, an exact match will not be found when drilling down and you will have to manually locate the server request in the Server Requests view in Mercury Diagnostics.
- If the application server handling a particular page is not monitored by a Diagnostics probe, there will be no data displayed when you click the **View Diagnostics Data** button.

Using the Real User Monitor Active Filters

Active filters, which can be configured for each of the reports except the Global Summary report, enable you to filter specific components from reports, for the duration of a Web session. You can then pinpoint problem areas or focus on specific areas that you have already determined to be problematic.

The following active filter tabs are available for the Real User Monitor reports:

- **Pages/Transactions** (available in the Page Summary and Transaction Summary reports respectively) – enables you to filter the pages or transactions displayed in the report according to the wildcard expressions you enter. You can choose instead to select the groups and specific pages/transactions within the groups for which you want the report to display data.
- **Servers** (available in the Server Summary report) – enables you to filter the servers displayed in the report according to the wildcard expressions you enter.
- **Events** (available in the Session Analyzer and Event Count Over Time reports) – enables you to filter the events displayed in the report according to the type of events you select.
- **End Users** (available for the Session Analyzer report) – enables you to filter the end-users displayed in the report according to a specific user name, host name, or single IP address.
- **End User Groups** (available for all reports except the Global Statistics and Server Summary reports) – enables you to filter the end-users displayed in the report according to the end-user groups that you select. In some of the reports you can also filter the end-user groups according to the wildcard expressions you enter, or by entering a range of IP addresses.
- **Thresholds** (available in all the summary reports) – enables you to filter the report according to the performance, or availability of the pages, transactions, end-user groups, or servers in the report.

➤ **Advanced** – enables you to filter the report according to the categories and filters you defined on the Measurement Filters page, accessible from Platform Administration's Data Collection tab. For details on measurement filters, see "Working with Measurement Filters" in *Platform Administration*.

To apply active filters to a report:

1 Click the **Active Filters** link. The Active Filters window opens and a tab for each filter available for the report is displayed.

The table below lists the filters available for each report.

	Pages	Trans-actions	Servers	Thresh-olds	Ad-vanced	End Users	End User Groups	Events
Global Statistics								
Page Summary	✓			✓	✓		✓	
Transaction Summary		✓		✓	✓		✓	
End User Summary				✓	✓		✓	
Server Summary			✓	✓	✓			
Session Analyzer						✓	✓	✓
Event Count Over Time							✓	✓
Event Summary							✓	

2 In the **Pages** and **Transactions** tabs, choose whether you want to view data for pages/transactions that meet the criteria of a specific wildcard expression, or for pages/transactions that you specifically select.

➤ If you select **Wildcard**, enter the wildcard expression according to which you want to filter the page/transactions displayed in the report.

- If you enter an asterisk (*) in this box, all pages/transactions will be displayed in the report.
- If you enter ***X** in this box, all pages/transactions that end with the string **X** will be displayed in the report.
- If you enter **X*** in this box, all pages/transactions that begin with the string **X** will be displayed in the report.
- If you enter ***X*** in this box, all pages/transactions that contain the string **X** will be displayed in the report.

Note: If the Mercury Business Availability Center databases are installed on an Oracle Server, the wildcard expressions are case sensitive. On an MSSQL Server, the wildcard expressions are case insensitive. For further details on the Mercury Business Availability Center databases, see "Introduction to Preparing the Database Environment" in *Preparing the Database Environment*.

➤ If you select **Pages**/**Transactions**, choose one or more groups from the list on the left and one or more pages/transactions within the groups from the list on the right. The pages/transactions you select will be displayed in the report. Note that by default, you cannot select more than 30 pages/transactions.

3 In the **Servers** tab, enter the wildcard expression according to which you want to filter the servers displayed in the report. For an explanation of the wildcard expressions that can be used, see step 2.

4 In the **Events** tab, you can filter sessions displayed in the report according to errors and events that occurred in the sessions. By default, all sessions are displayed. However, you can choose to view the following only:

➤ sessions that include slow pages (pages that exceeded their page time threshold)

- ➤ sessions with HTTP or application errors
- ➤ sessions that include selected types of events or errors

Note: For details on configuring HTTP errors, see "Defining HTTP Global Error Events" in *End User Management Data Collector Configuration*. For details on configuring events, see "Configuring Events" in *End User Management Data Collector Configuration*.

---

5 In the **Thresholds** tab, you can choose to filter the list of pages, transactions, end-user groups, or servers displayed in the report according to their performance or availability, based on the threshold levels you defined in Monitor Administration. By default, all pages, transactions, end-user groups, and servers are displayed. However, you can choose to view the following only:

- ➤ pages for which availability, performance, or server performance was poor or low
- ➤ transactions for which availability, total performance, net performance, or server performance was poor or low
- ➤ end-user groups for which performance was poor
- ➤ servers for which availability was low

Note: The thresholds filter operates using the threshold that was set at the time of the data sampling. For example, if you set a filter to show only pages for which availability was low, stipulate **Past day** as your time period, and modify the availability threshold from 80% to 90% mid-day, Real User Monitor uses the 80% threshold for data samples from the first half of the day and the 90% threshold for data samples from the second half of the day. Thus, both the first and second thresholds are taken into account.

---

6 In the **Advanced** tab, you can choose to filter the list of pages, transactions, end-user groups, or servers displayed in the report according to the categories and filters you defined on the Measurement Filters page in Platform Administration's Data Collection tab. (For details on creating filters, see "Working with Measurement Filters" in *Platform Administration*.)

- To display data that meets the criteria of all of the selected filters, select **Show measurements that match all of the following filters**.
- To display data that meets the criteria of at least one of the selected filters, select **Show measurements that match one of the following filters**.
- From the **Category** box, choose the category within which you want to select filters. Note that you can choose **All categories** and then select the filters you want to apply to the report.

7 In the **End Users** tab, you can filter the end-user displayed in the report by entering a specific user name, host name or single IP address.

8 In the **End User Groups** tab, you can choose whether you want to view data for end-users that meet the criteria of a specific wildcard expression, or for a group of end-users that you specifically select.

- If you select **End User Group Name** or **Wildcard**, enter the wildcard expression according to which you want to filter the end-user group names displayed in the report. For an explanation of the wildcard expressions that can be used, see step 2.
- If you select **End User Groups**, choose one or more end-user group containers from the list displayed in the left pane and one or more end-user groups included in the selected containers from the list displayed in the right pane. The end-user groups you select will be displayed in the report. Note that by default, you cannot select more than 30 end-user groups.
- In the **End User Groups** tab in the Session Analyzer, Event Count Over Time and Event Summary reports, you can also filter end-user groups by specifying a location, or a range of IP addresses.

9 In the **Servers** tab, enter the wildcard expression according to which you want to filter the servers displayed in the report. For an explanation of the wildcard expressions that can be used, see step 2.

10 Once you have selected all the active filters you want to apply to a report, click **OK** to save your settings and close the Active Filters window.

11 Click **Generate** to generate the report using the filters you defined.



Note: When a selection is to be made from a list of check boxes within a filter tab, you can use the **Select all**, **Invert selection**, and **Select none** buttons to help you make your selections.

Note: If more than one filter, or more than one option within a filter, is set for a report, the data displayed in the report must match all the filters and options set.

In the Session Analyzer and Event Count Over Time reports, if more than one event type is selected for inclusion in the report, the data displayed in the report must match at least one of the selected event types.

Aggregating Real User Monitor Data

The Real User Monitor engine sends data samples to Mercury Business Availability Center, which aggregates the data for use in Real User Monitor reports. For details on Mercury Business Availability Center data aggregation, see “Data Aggregation” in *Reference Information*.

There are nine data sample types that the Real User Monitor engine aggregates itself, before sending them to Mercury Business Availability Center. Once received in Mercury Business Availability Center, these pre-aggregated data samples are further aggregated by Mercury Business Availability Center on a daily basis. The following table lists the data sample types, the Real User Monitor report for which they are used, and their aggregation period in Real User Monitor:

Data Sample Type	Real User Monitor Report	Aggregation Period in Real User Monitor
Top Domain	Global Statistics	Every hour
Top Page	Global Statistics	Every hour
Missing Component	Global Statistics	Every five minutes
Page with Most Errors	Global Statistics	Every five minutes
Slow Domain	Global Statistics	Every five minutes
Slow Page	Global Statistics	Every five minutes
Domain	End User Summary	Every five minutes
Page	Page Summary	Every five minutes
Server	Server Summary	Every five minutes

You can change the aggregation period of these data sample types in the Real User Monitor engine JMX console. For details on changing the aggregation period, see "Configuring Real User Monitor Aggregation" in *Real User Monitor Administration*.

Global Statistics Report

The Global Statistics report contains the following tables:

- Most Popular Pages – see the next section
- Most Active End Users – see page 88
- Slowest End Users – see page 89
- Pages with Slowest Server Time – see page 90
- Pages with Most Errors – see page 92
- Broken Links – see page 93

The data displayed in the above tables is based on all data collected from the selected engine and not on the specific pages and end-user groups that you configured for Real User Monitor in Monitor Administration. The data is collected according to the settings defined for the engine in Monitor Administration. For information on configuring these settings, see "Configuring General Settings" in *End User Management Data Collector Configuration*.

Note: Each table in the Global Statistics report displays only 20 rows by default, even though you may have instructed Real User Monitor to collect more than 20 pages, end-user groups, or broken links. For details on modifying the maximum number of rows displayed in a table, see "Modifying the Maximum Number of Rows Displayed in a Table" on page 76.

Most Popular Pages

The Most Popular Pages table displays data for the pages that received the highest number of hits. In calculating the most popular pages, Real User Monitor takes into account which pages were most popular during each one-hour interval and the number of intervals for which the pages were most popular.

The table contains the following columns:

Column	Explanation
Page	Displays the URLs of the most popular pages.
Hits	Displays the total number of requests that each page received for the entire amount of time that it was most popular.
Defined	Indicates whether a page was defined in Monitor Administration at the time at which the data sample was compiled by the Real User Monitor engine.



If you are a system administrator, you can click the **Define Page** button if a page is not defined in Monitor Administration and you want to define the page's properties and add it to the list of configured pages in Monitor Administration. (For details on configuring pages in Monitor Administration, see "Configuring Pages" in *End User Management Data Collector Configuration*.)

In the Define Page dialog box that opens, enter the name you want to assign the page, edit the URL of the page (if necessary), and select the group to which you want to assign the page. The newly defined page is added to the page group you stipulated in Monitor Administration. Note that this page will only be listed as defined when the next data sample is compiled by the Real User Monitor engine.

Note:

- By default, asterisks in URLs are treated as wildcards. To define an asterisk as a literal and not as a wildcard, precede it with a backslash (\). For example, **my*str**.

- When you add a page using the Define Page dialog box, the page acquires the default settings for page thresholds that you configure in Monitor Administration. If you want to change any of the page's default settings, you must do so in Monitor Administration.

Most Active End Users

The Most Active End Users table displays data for the end-user groups with the highest number of page requests. In calculating the most active end-users, Real User Monitor takes into account which end-user groups were most active during each one-hour interval and the number of intervals for which the end-user groups were most active.

The table contains the following columns:

Column	Explanation
End User	Displays the names and IP addresses of the most active end-user groups.
End-User Location	Displays the geographic location of each end-user group.
Page Hits	Displays the total number of page hits generated by each end-user group for the entire amount of time that it was most active.
HTTP Traffic	Displays the number of kilobytes that each end-user group sent to, and received from, the server(s) via HTTP.

Column	Explanation
HTTPS Traffic	Displays the number of kilobytes that each end-user group sent to, and received from, the server(s) via HTTPS.
Latency	Displays the average network latency (the round trip time for a packet), in milliseconds, for each end-user group.
Defined	Indicates whether a page was defined in Monitor Administration at the time at which the data sample was compiled by the Real User Monitor engine.

Slowest End Users

The Slowest End Users table displays data for the end-user groups that experienced the highest average network latency. In calculating the slowest end-users, Real User Monitor takes into account which end-user groups were slowest during each five-minute interval and the number of intervals for which the end-user groups were slowest.

The table contains the following columns:

Column	Explanation
End User	Displays the names or IP addresses of the slowest end-user groups.
End-User Location	Displays the geographic location of each end-user group.
Page Hits	Displays the total number of page hits generated by each end-user group for the entire amount of time that it was one of the slowest end-users.
HTTP Traffic	Displays the number of kilobytes that each end-user group sent to, and received from, the server(s) via HTTP.

Column	Explanation
HTTPS Traffic	Displays the number of kilobytes that each end-user group sent to, and received from, the server(s) via HTTPS.
Defined	Indicates whether a page was defined in Monitor Administration at the time at which the data sample was compiled by the Real User Monitor engine.

Pages with Slowest Server Time

The Pages with Slowest Server Time table displays data for the pages with the longest server time. In calculating the pages with the slowest server time, Real User Monitor takes into account which pages had the slowest server time during each five-minute interval, and the number of intervals for which the pages were slowest.

Note: It is possible that a page included in the Pages with Slowest Server Time table will have a number of hits that would seem to qualify it for inclusion in the Most Popular Pages table, but it is not included. This is due to the different aggregation schedule between the Slowest Pages (aggregated every five minutes) and the Most Popular Pages (aggregated every hour).

The table contains the following columns:

Column	Explanation
Page URL	Displays the URLs of the slowest pages.
Server Time	Displays the average amount of time, in seconds, that it took the server to process the requests for each page.

Column	Explanation
Download Time	Displays the average amount of time it took to download each page.
Hits	Displays the total number of hits that each page received for the entire amount of time that it was one of the slowest pages.



If you are a system administrator, you can click the **Define Page** button if a page is not defined in Monitor Administration and you want to define the page's properties and add it to the list of configured pages in Monitor Administration. (For details on configuring pages in Monitor Administration, see "Configuring Pages" in *End User Management Data Collector Configuration*.)

In the Define Page dialog box that opens, enter the name you want to assign the page, edit the URL of the page (if necessary), and select the group to which you want to assign the page. The newly defined page is added to the page group you stipulated in Monitor Administration. Note that this page will only be listed as defined when the next data sample is compiled by the Real User Monitor engine.

Note:

- By default, asterisks in URLs are treated as wildcards. To define an asterisk as a literal and not as a wildcard, precede it with a backslash (\). For example, **my*str**.

- When you add a page using the Define Page dialog box, the page acquires the default settings for page thresholds that you configure in Monitor Administration. If you want to change any of the page's default settings, you must do so in Monitor Administration.

Pages with Most Errors

The Pages with Most Errors table displays data for the pages on which the most HTTP and application errors occurred. In calculating the pages with most errors, Real User Monitor takes into account which pages had the most errors during each five-minute interval and the number of intervals for which the pages had most errors.

The table contains the following columns:

Column	Explanation
Page	Displays the URLs of the pages with most errors.
Total Errors	Displays the total number of HTTP and application errors that occurred on each page.
HTTP Errors	Displays the total number of HTTP errors that occurred on each page.
Application Errors	Displays the total number of application errors that occurred on each page.



If you are a system administrator, you can click the **Define Page** button if a page is not defined in Monitor Administration and you want to define the page's properties and add it to the list of configured pages in Monitor Administration. (For details on configuring pages in Monitor Administration, see "Configuring Pages" in *End User Management Data Collector Configuration*.)

In the Define Page dialog box that opens, enter the name you want to assign the page, edit the URL of the page (if necessary), and select the group to which you want to assign the page. The newly defined page is added to the page group you stipulated in Monitor Administration. Note that this page will only be listed as defined when the next data sample is compiled by the Real User Monitor engine.

Note:

➤ By default, asterisks in URLs are treated as wildcards. To define an asterisk as a literal and not as a wildcard, precede it with a backslash (\). For example, **my*str**.

➤ When you add a page using the Define Page dialog box, the page acquires the default settings for page thresholds that you configure in Monitor Administration. If you want to change any of the page's default settings, you must do so in Monitor Administration.

Broken Links

The Broken Links table displays data for the broken links encountered on specific host machines that you configure for Real User Monitor in Monitor Administration, experienced most frequently by end-users. In calculating the most frequent broken links, Real User Monitor takes into account which broken links were most frequent during each five-minute interval and the number of intervals for which the broken links were most frequent. The table contains the following columns:

Column	Explanation
Page URL	Displays the URLs of the pages with the most frequent broken links.
Referring URL	Displays the URL from which each broken link was accessed.
# of Occurrences	Displays the total number of occurrences of each broken link for the entire amount of time that it was considered a frequent broken link.
First Occurrence	Displays the time at which an end-user group first experienced the broken link.
Last Occurrence	Displays the time at which an end-user group last experienced the broken link.

Page Summary Report

The Page Summary report displays data for specific Web pages that were configured for Real User Monitor in Monitor Administration. For information on configuring Web pages to be monitored, see "Configuring Pages" in *End User Management Data Collector Configuration*. The Page Summary report contains the following tabs:

- General Tab – see the next section
- Availability Tab – see page 98
- Performance Tab – see page 100
- Server Performance Tab – see page 102

From each tab, you can click to view the following:

- "Page Broken Down by End-Users" on page 104
- "Page Over Time" on page 105
- "Event Summary Report" on page 152
- "Servers by Page Summary" on page 111
- "Mercury Diagnostics Server Requests View" on page 113

Note: You can set an active filter for the Page Summary report. For information on setting active filters, see "Using the Real User Monitor Active Filters" on page 79.

General Tab

The General tab displays general data related to each configured Web page that was monitored. It contains the following columns:

Column	Explanation
Page	Displays the names you assigned the Web pages in Monitor Administration.
Availability	Displays the percentage of requests for which each page was available. This column is color-coded, based on the page's availability in relation to the page availability threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical **Note:** If a page is unavailable, its data is not included in the page performance calculations.
Page Time	Displays the average amount of time, in seconds, it took for each page to download. This column is color-coded, based on the page's download time in relation to the page time threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Server Time	Displays the average amount of time, in seconds, that it took the server to process the requests for each page. This column is color-coded, based on the page's server time in relation to the server time threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Hits	Displays the total number of requests that each page received.
Informational Events	Displays the number of informational events that occurred on the page, based on the informational events you defined for the page, or application, in Monitor Administration.

Column	Explanation
Page Size	Displays the average downloaded size, in kilobytes, of each page.
# of Components	Displays the average number of page components that were downloaded for each page.

Viewing the Summary Row

If summary rows have been enabled (for details, see "Enabling Summary Rows" on page 76), you can view the following:

- **Total Availability** – the average availability of all pages (that is, the total number of successful hits for all pages divided by the total number of hits for all pages)
- **Total Page Time** – the average page time of all pages
- **Total Server Time** – the average server time of all pages
- **Total Hits** – the sum of all the hits to each page
- **Total Informational Events** – the sum of all the informational events that occurred in each page

Viewing Data for Each End-User Group that Accessed a Page



To view data for each end-user group that accessed a page, click the **View End Users** button in the row of the page for which you want to view this data. The Page Broken Down by End-Users page opens. For details on this page, see "Page Broken Down by End-Users" on page 104.

Viewing Data Over Time for a Page



To view data over time for a page, click the **View Data over Time** button in the row of the page for which you want to view data over a period of time. The Page Over Time page opens. For details on this page, see "Page Over Time" on page 105.

Viewing the Event Summary Report for a Page



To view the Event Summary report, click the View Event Summary Report button in the row of the page for which you want to view event summary data. The Event Summary Report opens. For details on this report, see "Event Summary Report" on page 152.

Viewing the Servers by Page Summary for a Page



To view a summary of the servers used in accessing a page, click the View Servers by Page Summary Report button in the row of the page for which you want to view server summary data. The Servers by Page Summary report opens. For details on this report, see "Servers by Page Summary" on page 111.

Viewing the Mercury Diagnostics Server Requests View for a Page



To drill down to the Mercury Diagnostics Server Requests view for a specific page, click the **View Diagnostics Data** button in the row of the page for which you want to view this data. For details on working with the Mercury Diagnostics Server Requests view, refer to the *Mercury Diagnostics Installation and User's Guide*.

Availability Tab

The Availability tab displays page availability data for each configured Web page that was monitored. It contains the following columns:

Column	Explanation
Page	Displays the names you assigned the Web pages in Monitor Administration.
Availability	Displays the percentage of requests for which each page was available. This column is color-coded, based on the page's availability in relation to the page availability threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical **Note:** If a page is unavailable, its data is not included in the page performance calculations.
Availability Threshold	Displays the availability threshold configured for each page in Monitor Administration.
Hits	Displays the total number of requests that each page received.
Unavailable Hits	Displays the number of hits for which each page was unavailable.
HTTP Errors	Displays the number of HTTP errors encountered by the page, based on the HTTP errors you defined for the Real User Monitor engine in Monitor Administration.
Application Errors	Displays the number of application errors encountered by the page, based on the application errors you defined for the page, or the application, in Monitor Administration.
Stopped Pages	Displays the number of hits for which each page was unavailable because page downloading was stopped.

Viewing the Summary Row

If summary rows have been enabled (for details, see "Enabling Summary Rows" on page 76), you can view the following:

- **Total Availability** – the average availability of all pages (that is, the total number of successful hits for all pages divided by the total number of hits for all pages)
- **Total Hits** – the sum of all the hits to each page
- **Total Unavailable Hits** – the sum of all the unavailable hits to each page
- **Total HTTP Errors** – the sum of all the http errors for each page
- **Total Application** – the sum of all the application errors for each page
- **Total Stopped Pages** – the sum of all the stopped pages for each page

Viewing Data for Each End-User Group that Accessed a Page



To view data for each end-user group that accessed a page, click the **View End Users** button in the row of the page for which you want to view this data. The Page Broken Down by End-Users page opens. For details on this page, see "Page Broken Down by End-Users" on page 104.

Viewing Data Over Time for a Page



To view data over time for a page, click the **View Data over Time** button in the row of the page for which you want to view data over a period of time. The Page Over Time page opens. For details on this page, see "Page Over Time" on page 105.

Viewing the Event Summary Report for a Page



To view the Event Summary report, click the View Event Summary Report button in the row of the page for which you want to view event summary data. The Event Summary Report opens. For details on this report, see "Event Summary Report" on page 152.

Viewing the Servers by Page Summary for a Page



To view a summary of the servers used in accessing a page, click the View Servers by Page Summary Report button in the row of the page for which you want to view server summary data. The Servers by Page Summary report opens. For details on this report, see "Servers by Page Summary" on page 111.

Viewing the Mercury Diagnostics Server Requests View for a Page



To drill down to the Mercury Diagnostics Server Requests view for a specific page, click the **View Diagnostics Data** button in the row of the page for which you want to view this data. For details on working with the Mercury Diagnostics Server Requests view, refer to the *Mercury Diagnostics Installation and User's Guide*.

Performance Tab

The Performance tab displays page performance data for each configured Web page that was monitored. It contains the following columns:

Column	Explanation
Page	Displays the names you assigned the Web pages in Monitor Administration.
Page Time	Displays the average amount of time, in seconds, it took for each page to download. This column is color-coded, based on the page's download time in relation to the page time threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Page Time Threshold	Displays the page time threshold configured for each page in Monitor Administration.
Server Time	Displays the average amount of time, in seconds, that it took the server to process the requests for each page.
Network Time	Displays the average amount of time, in seconds, that each page's requests were delayed on the network.
Client Time	Displays the average amount of time, in seconds, that each page's requests were delayed on the client machine.

Column	Explanation
Hits	Displays the total number of requests that each page received.
Slow Hits	Displays, for each page, the total number of hits whose page time exceeded the configured page time threshold.
Page Time of Slow Hits	Displays the average amount of time, in seconds, that it took to download each page's slow page requests.

Viewing the Summary Row

If summary rows have been enabled (for details, see "Enabling Summary Rows" on page 76), you can view the following:

- **Total Page Time** – the average page time of all pages
- **Total Server Time** – the average server time of all pages
- **Total Network Time** – the average network time of all pages
- **Total Client Time** – the average client time of all pages
- **Total Hits** – the sum of all the hits to each page
- **Total Slow Hits** – the sum of all the slow hits to each page
- **Total Page Time of Slow Hits** – the average page time of all slow page requests

Viewing Data for Each End-User Group that Accessed a Page



To view data for each end-user group that accessed a page, click the **View End Users** button in the row of the page for which you want to view this data. The Page Broken Down by End-Users page opens. For details on this page, see "Page Broken Down by End-Users" on page 104.

Viewing Data Over Time for a Page



To view data over time for a page, click the **View Data over Time** button in the row of the page for which you want to view data over a period of time. The Page Over Time page opens. For details on this page, see "Page Over Time" on page 105.

Viewing the Event Summary Report for a Page



To view the Event Summary report, click the View Event Summary Report button in the row of the page for which you want to view event summary data. The Event Summary Report opens.For details on this report, see "Event Summary Report" on page 152.

Viewing the Servers by Page Summary for a Page



To view a summary of the servers used in accessing a page, click the View Servers by Page Summary Report button in the row of the page for which you want to view server summary data. The Servers by Page Summary report opens. For details on this report, see "Servers by Page Summary" on page 111.

Viewing the Mercury Diagnostics Server Requests View for a Page



To drill down to the Mercury Diagnostics Server Requests view for a specific page, click the **View Diagnostics Data** button in the row of the page for which you want to view this data. For details on working with the Mercury Diagnostics Server Requests view, refer to the *Mercury Diagnostics Installation and User's Guide*.

Server Performance Tab

The Server Performance tab displays server performance data for each configured Web page that was monitored. It contains the following columns:

Column	Explanation
Page	Displays the names you assigned the Web pages in Monitor Administration.
Server Time	Displays the average amount of time, in seconds, that it took the server to process the requests for each page. This column is color-coded, based on the page's server time in relation to the server time threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical

Column	Explanation
Server Time Threshold	Displays the server time threshold configured for each page in Monitor Administration.
Page Time	Displays the average amount of time, in seconds, it took for each page to download.
Hits	Displays the total number of requests that each page received.
Slow Hits	Displays, for each page, the total number of hits whose server time exceeded the configured server time threshold.
Server Time of Slow Hits	Displays the average server time, in seconds, for each page's slow hits.

Viewing the Summary Row

If summary rows have been enabled (for details, see "Enabling Summary Rows" on page 76), you can view the following:

- **Total Server Time** – the average server time of all pages
- **Total Page Time** – the average page time of all pages
- **Total Hits** – the sum of all the hits to each page
- **Total Slow Hits** – the sum of all the slow hits to each page
- **Total Server Time of Slow Hits** – the average server time of all slow hits

Viewing Data for Each End-User Group that Accessed a Page



To view data for each end-user group that accessed a page, click the **View End Users** button in the row of the page for which you want to view this data. The Page Broken Down by End-Users page opens. For details on this page, see "Page Broken Down by End-Users" on page 104.

Viewing Data Over Time for a Page



To view data over time for a page, click the **View Data over Time** button in the row of the page for which you want to view data over a period of time. The Page Over Time page opens. For details on this page, see "Page Over Time" on page 105.

Viewing the Event Summary Report for a Page



To view the Event Summary report, click the View Event Summary Report button in the row of the page for which you want to view event summary data. The Event Summary Report opens. For details on this report, see "Event Summary Report" on page 152.

Viewing the Servers by Page Summary for a Page



To view a summary of the servers used in accessing a page, click the View Servers by Page Summary Report button in the row of the page for which you want to view server summary data. The Servers by Page Summary report opens. For details on this report, see "Servers by Page Summary" on page 111.

Viewing the Mercury Diagnostics Server Requests View for a Page



To drill down to the Mercury Diagnostics Server Requests view for a specific page, click the **View Diagnostics Data** button in the row of the page for which you want to view this data. For details on working with the Mercury Diagnostics Server Requests view, refer to the *Mercury Diagnostics Installation and User's Guide*.

Page Broken Down by End-Users

The Page Broken Down by End Users page displays general, availability, performance, or server performance data for each end-user group that accessed the page you selected, depending on the table from which you accessed the Page Broken Down by End-Users page. The columns in each table (except for the first column) are identical to those displayed for the same table in the main Page Summary report.

Note that the thresholds active filter you set for the Page Summary report is not relevant for the Page Broken Down by End-Users tables. You must set a separate thresholds active filter for these tables. For information on setting an active filter, see "Using the Real User Monitor Active Filters" on page 79.

To return to the corresponding main Page Summary report, click the **Page Summary** link in the breadcrumb at the top of the page. For information on breadcrumbs, see "Navigating Mercury Business Availability Center" in *Getting Started with Mercury Business Availability Center*.

Viewing the Event Summary Report for Each End-User Group

You can view the Event Summary report for each end-user group for the page you selected.

To view the Event Summary report for each end-user group for the page you selected:



On the Page Broken Down by End-Users page, click the View Event Summary Report button.in the row of the end-user group for which you want to view the Event Summary report. The Event Summary Report opens in the **View as Graph tab**, displaying pie charts of the end-user group's events for the selected page. The data may be viewed as a table by moving to the **View as Table** tab. For details on this report, see "Event Summary Report" on page 152.

Viewing Data Over Time for Each End-User Group

You can view a graph of each end-user group's page access over time.

To view a graph of each end-user group's page access over time:



On the Page Broken Down by End-Users page, click the **View Data over Time** button.in the row of the end-user group for which you want to view information over a period of time. The End-User Page Access Over Time page opens, displaying a graph of the end-user group's general, availability, performance, or server performance activity vis-a-vis the selected page, over the course of time. For details on these graphs, see "Page Over Time" below.

To return to the Page Broken Down by End-Users table from which you accessed the End-User Page Access Over Time graph, click the **Page Broken Down by End Users** link in the breadcrumb at the top of the page. To return to the corresponding table in the main Page Summary report, click the **Page Summary** link in the breadcrumb at the top of the page. For information on breadcrumbs, see "Navigating Mercury Business Availability Center" in *Getting Started with Mercury Business Availability Center*.

Page Over Time

The Page Over Time page displays a graph of the general, availability, performance, or server performance data over the course of time for each page, depending on the table from which you accessed the Page Over Time page.

To return to the corresponding main Page Summary report, click the **Page Summary** link in the breadcrumb at the top of the page. For information on breadcrumbs, see "Navigating Mercury Business Availability Center" in *Getting Started with Mercury Business Availability Center*.

Viewing the Mercury Diagnostics Server Requests View for a Page for a Specific Time

If Mercury Diagnostics has been registered and enabled on your Mercury Business Availability Center system (for details see "Drilling Down to Mercury Diagnostics Reports" on page 78), you can drill down to the Mercury Diagnostics Server Requests view for a specific page at a specific time.

To drill down to the Mercury Diagnostics Server Requests view for a specific page at a specific time, in the table displayed in any of the tabs (general, availability, performance, and server performance), click the **View Diagnostics Data** button in the row of the time for which you want to view this data.



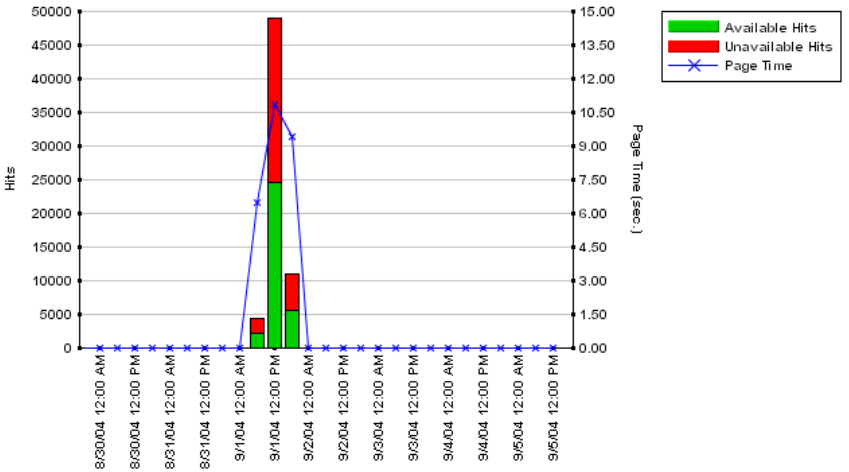
For details on working with the Mercury Diagnostics Server Requests view, refer to the *Mercury Diagnostics Installation and User's Guide*.

General Graph

The x-axis displays the time division units for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

The left y-axis displays page hit units. The bars indicate the number of available and unavailable page hits, according to the color coding in the legend, at each point over the course of the defined time period. The right y-axis displays page time units (seconds). The line connecting the data points indicates the page time at each point over the course of the defined time period.

For example, the graph below shows page hits and page time over the course of a week. On September 1, at approximately 6:00 AM, there were about 2100 available hits and 2100 unavailable hits and the average page time was about 6.5 seconds. At 12:00 PM on the same day, there were about 24,500 available hits and 24,500 unavailable hits and the average page time was about 11 seconds. At 6:00 PM, there were about 5500 available hits and 5500 unavailable hits and the average page time was about 9.5 seconds.



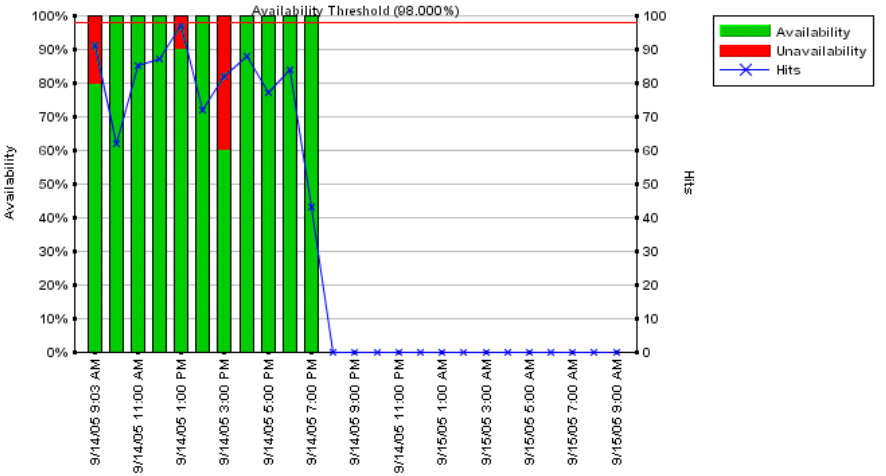
The table underneath the graph displays available hits, unavailable hits, and page time, in addition to server time, network time, client time, http errors, and application errors, for each point over the course of the defined time period.

Availability Graph

The x-axis displays the time division units for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

The left y-axis displays page availability percentage units. The bars indicate the percentage of available and unavailable hits, according to the color coding in the legend, at each point over the course of the defined time period. The right y-axis displays page hit units. The line connecting the data points indicates the number of page hits at each point over the course of the defined time period. The horizontal red Availability Threshold line displays the page availability threshold that you configured in Monitor Administration.

For example, the graph below shows page availability and the number of page hits over the course of a day. On September 14, at approximately 9:00 AM, 80 percent of the 91 page hits were available. At 1:00 PM on the same day, 90 percent of the 97 page hits at that time were available. At 3:00 PM, 60 percent of the 82 page hits were available. At these times, page availability was less than the threshold configured in Monitor Administration (98%). At all the other times for which there were hits, availability was 100 percent.



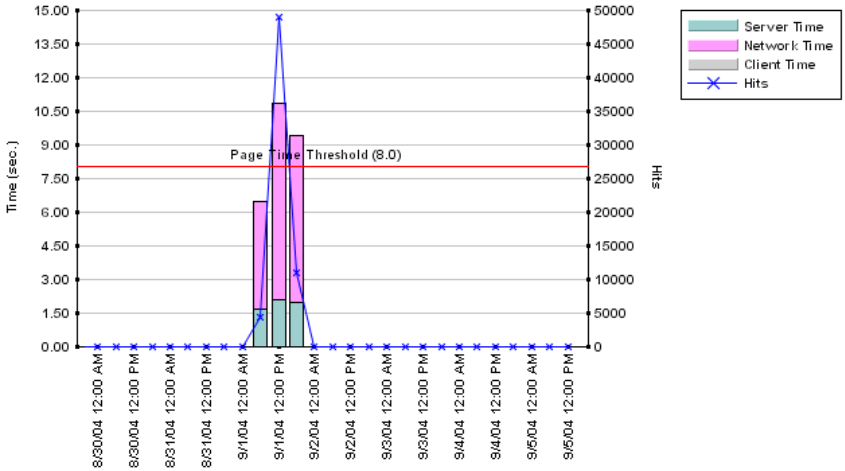
The table underneath the graph displays the data shown in the graph as well as page time, server time, network time, and client time for each point over the course of the defined time period.

Performance Graph

The x-axis displays the time division units for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

The left y-axis displays page time units (seconds). The bars indicate various statuses, according to the color coding in the legend, at each point over the course of the defined time period. The right y-axis displays page hit units. The line connecting the data points indicates the number of page hits at each point over the course of the defined time period. The horizontal red Page Time Threshold line displays the page time threshold that you configured in Monitor Administration.

For example, the graph below shows page time and the number of page hits over the course of a week. On September 1, at approximately 6:00 AM, there were just under 5000 hits with an average page time of approximately 6.5 seconds. At 12:00 PM on the same day, there were about 50,000 hits with an average page time of approximately 11 seconds. At 6:00 PM, there were just over 10,000 hits with an average page time of approximately 9.5 seconds. Page time surpassed the threshold configured in Monitor Administration (8 seconds) at 12:00 and 6:00 PM.



The table underneath the graph displays the data shown in the graph as well as available and unavailable hits, server errors, requests refused, bad requests, and requests not found, for each point over the course of the defined time period.

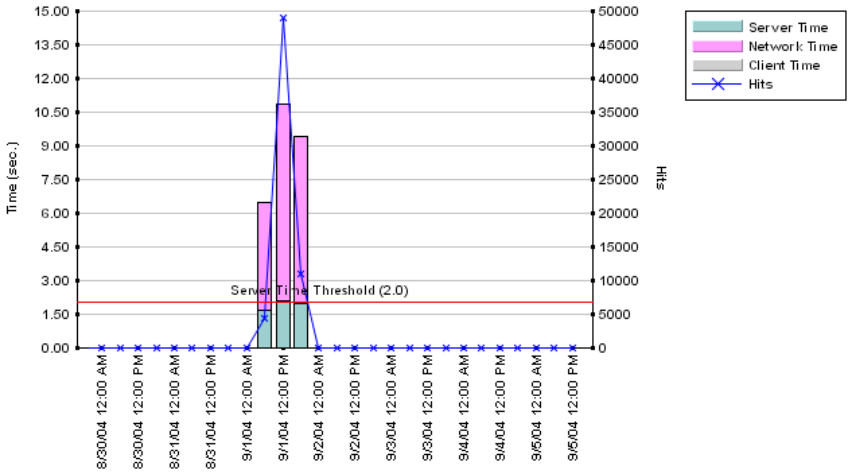
Server Performance Graph

The x-axis displays the time division units for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

The left y-axis displays server time units (seconds). The bars indicate various statuses, according to the color coding in the legend, at each point over the course of the defined time period. The right y-axis displays page hit units. The line connecting the data points indicates the number of page hits at each point over the course of the defined time period. The horizontal red Server Time Threshold line displays the page server time threshold that you configured in Monitor Administration.

For example, the following graph shows server time and the number of page hits over the course of a week. On September 1, at approximately 6:00 AM, there were just under 5000 hits with an average server time of approximately 1.6 seconds. At 12:00 PM on the same day, there were about 50,000 hits with an average server time of approximately 2 seconds.

At 6:00 PM, there were just over 10,000 hits with an average server time of just under 2 seconds. Page server time surpassed the threshold configured in Monitor Administration (2 seconds) at 12:00 PM.



The table underneath the graph displays the data shown in the graph as well as available and unavailable hits, server errors, requests refused, bad requests, and requests not found, for each point over the course of the defined time period.

Servers by Page Summary

The Servers by Page Summary report displays a table showing each server used in accessing the page for which you are viewing data. For each server, the following columns are displayed:

Column	Description
Server Name	Displays the name of the server as defined in Monitor Administration.
Server IP	Displays the IP address of the server.

Column	Description
Page Time	Displays the average amount of time, in seconds, it took for the page to download. This column is color-coded, based on the page's download time in relation to the page time threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Page Threshold	Displays the page time threshold configured for the page in Monitor Administration.
Server Time	Displays the average amount of time, in seconds, that it took the server to process the requests for the page. This column is color-coded, based on the page's server time in relation to the server time threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Server Time Threshold	Displays the server time threshold configured for the page in Monitor Administration.
Hits	Displays the total number of requests that the page received.
Slow Hits	Displays the total number of hits whose page time exceeded the configured page time threshold.
Server Time Slow Hits	Displays the average server time, in seconds, for the page's slow hits.

To return to the corresponding main Page Summary report, click the **Page Summary** link in the breadcrumb at the top of the page. For information on breadcrumbs, see "Navigating Mercury Business Availability Center" in *Getting Started with Mercury Business Availability Center*.

Note:

- The report uses the same time range as that selected for the main Page Summary report, but will not exceed 24 hours. If the time range selected is longer than 24 hours, the last 24 hour period of the time range is used.
- The report uses raw Real User Monitor data.

Mercury Diagnostics Server Requests View

If Mercury Diagnostics has been registered and enabled on your Mercury Business Availability Center system (for details see "Drilling Down to Mercury Diagnostics Reports" on page 78), you can drill down to the Mercury Diagnostics Server Requests view for a specific page.

For details on working with the Mercury Diagnostics Server Requests view, refer to the *Mercury Diagnostics Installation and User's Guide*.

Transaction Summary Report

The Transaction Summary report displays data for specific transactions that were configured for Real User Monitor in Monitor Administration. For information on configuring transactions to be monitored, see "Configuring Transactions" in *End User Management Data Collector Configuration*.

The Transaction Summary report contains the following tabs:

- General Tab – see the next section
- Availability Tab – see page 116
- Total Performance Tab – see page 118
- Net Performance Tab – see page 119
- Server Performance Tab – see page 121

From each tab, you can click to view the following:

- Transaction Broken Down by End Users – see page 122
- Transaction Over Time – see page 123

Note: You can set an active filter for the Transaction Summary report. For information on setting active filters, see "Using the Real User Monitor Active Filters" on page 79.

General Tab

The General tab displays general data for each configured transaction that was monitored. It contains the following columns:

Column	Explanation
Transaction	Displays the names you assigned the transactions in Monitor Administration.
Availability	Displays the percentage of transactions for which there were no availability problems. This column is color-coded, based on the transaction's availability in relation to the transaction availability threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical **Note:** If a transaction is unavailable, its data is not included in the transaction performance calculations.
Total Time	Displays an average of the overall transaction time (from the start of the first page to the end of the last page), in seconds, for each transaction. This column is color-coded, based on the transaction's total time in relation to the total time threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical

Column	Explanation
Think Time	Displays the total think time in seconds, for each transaction.
Net Time	Displays the total download time of all the pages included in the transaction (in Monitor Administration, you define for each page included in the transaction whether this includes download time only, or both download time and think time), in seconds, for each transaction. This column is color-coded, based on the transaction's net time in relation to the net time threshold you configured in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Client Time	Displays the total time, in seconds, that each page included in the transaction was delayed on the client machine.
Network Time	Displays the total time, in seconds, that each page included in the transaction was delayed on the network.
Server Time	Displays the total server time of all the pages included in the transaction. This column is color-coded, based on the transaction's server time in relation to the transaction server time threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Transaction Runs	Displays the total number of run instances for each transaction.
Transaction Size	Displays the size, in kilobytes, of each transaction.

Viewing the Summary Row

If summary rows have been enabled (for details, see "Enabling Summary Rows" on page 76), you can view the following:

➤ **Total Availability** – the average availability of all transactions (that is, the total number of successful transaction runs for all transactions divided by the total number of transaction run requests for all transactions)

- **Total Total Time** – the average total transaction time of all transactions
- **Total Net Time** – the average net time of all transactions
- **Total Server Time** – the average server time of all transactions
- **Total Transaction Runs** – the sum of all the transaction run instances for each transaction

Viewing Data for Each End-User Group that Ran a Transaction



To view data for each end-user group that ran a transaction, click the **View End Users** button in the row of the transaction for which you want to view this data. The Transaction Broken Down by End Users page opens. For details on this page, see "Transaction Broken Down by End Users" on page 122.

Viewing Data Over Time for a Transaction



To view data over time for a transaction, click the **View Data over Time** button in the row of the transaction for which you want to view data over a period of time. The Transaction Over Time page opens. For details on this page, see "Transaction Over Time" on page 123.

Availability Tab

The Availability tab displays transaction availability data for each configured transaction that was monitored. It contains the following columns:

Column	Explanation
Transaction	Displays the names you assigned the transactions in Monitor Administration.
Availability	Displays the percentage of transactions for which there were no availability problems. This column is color-coded, based on the transaction's availability in relation to the transaction availability threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical **Note:** If a transaction is unavailable, its data is not included in the transaction performance calculations.

Column	Explanation
Availability Threshold	Displays the availability threshold configured for each transaction in Monitor Administration.
Unavailable Runs	Displays, for each transaction, the total number of transaction run instances for which availability problems occurred.
Transaction Runs	Displays the total number of run instances for each transaction.

Viewing the Summary Row

If summary rows have been enabled (for details, see "Enabling Summary Rows" on page 76), you can view the following:

- **Total Availability** – the average availability of all transactions (that is, the total number of successful transaction runs for all transactions divided by the total number of transaction run requests for all transactions)
- **Total Unavailable Runs** – the sum of all the unavailable transaction run instances for each transaction
- **Total Transaction Runs** – the sum of all the transaction run instances for each transaction

Viewing Data for Each End-User Group that Ran a Transaction



To view data for each end-user group that ran a transaction, click the **View End Users** button in the row of the transaction for which you want to view this data. The Transaction Broken Down by End Users page opens. For details on this page, see "Transaction Broken Down by End Users" on page 122.

Viewing Data Over Time for a Transaction



To view data over time for a transaction, click the **View Data over Time** button in the row of the transaction for which you want to view data over a period of time. The Transaction Over Time page opens. For details on this page, see "Transaction Over Time" on page 123.

Total Performance Tab

The Total Performance tab displays data for the entire duration (run time and think time) of each configured transaction that was monitored. It contains the following columns:

Column	Explanation
Transaction	Displays the names you assigned the transactions in Monitor Administration.
Total Time	Displays an average of the overall transaction time (from the start of the first page to the end of the last page), in seconds, for each transaction. This column is color-coded, based on the transaction's total time in relation to the total time threshold you configured in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Total Time Threshold	Displays the total transaction time threshold configured for each transaction in Monitor Administration.
Transaction Runs	Displays the total number of run instances for each transaction.
Slow Transaction Runs	Displays, for each transaction, the number of run instances whose total transaction time exceeded the configured total time threshold.
Total Time of Slow Transaction Runs	Displays the average total transaction time, in seconds, of each transaction's slow runs.

Viewing the Summary Row

If summary rows have been enabled (for details, see "Enabling Summary Rows" on page 76), you can view the following:

- **Total Time** – the average total transaction time of all transactions
- **Total Transaction Runs** – the sum of all the transaction run instances for each transaction
- **Total Slow Transaction Runs** – the sum of all the slow transaction runs for each transaction

Viewing Data for Each End-User Group that Ran a Transaction



To view data for each end-user group that ran a transaction, click the **View End Users** button in the row of the transaction for which you want to view this data. The Transaction Broken Down by End Users page opens. For details on this page, see "Transaction Broken Down by End Users" on page 122.

Viewing Data Over Time for a Transaction



To view data over time for a transaction, click the **View Data over Time** button in the row of the transaction for which you want to view data over a period of time. The Transaction Over Time page opens. For details on this page, see "Transaction Over Time" on page 123.

Net Performance Tab

The Net Performance tab displays data for the net duration (excluding think time) of each configured transaction that was monitored. It contains the following columns:

Column	Explanation
Transaction	Displays the names you assigned the transactions in Monitor Administration.
Net Time	Displays the total download time of all the pages included in the transaction (in Monitor Administration, you define for each page included in the transaction whether this includes download time only, or both download time and think time), in seconds, for each transaction. This column is color-coded, based on the transaction's net time in relation to the net time threshold you configured in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Net Time Threshold	Displays the net time threshold configured for each transaction in Monitor Administration.
Server Time	Displays the total server time of all the pages included in the transaction.

Column	Explanation
Network Time	Displays the total time, in seconds, that each page included in the transaction was delayed on the network.
Client Time	Displays the total time, in seconds, that each page included in the transaction was delayed on the client machine.
Transaction Runs	Displays the total number of run instances for each transaction.
Slow Transaction Runs	Displays, for each transaction, the number of run instances whose net transaction time exceeded the configured net time threshold.
Net Time of Slow Transaction Runs	Displays the average net transaction time, in seconds, of each transaction's slow runs.

Viewing the Summary Row

If summary rows have been enabled (for details, see "Enabling Summary Rows" on page 76), you can view the following:

- **Total Net Time** – the average net time of all transactions
- **Total Server Time** – the average server time of all transactions
- **Total Network Time** – the average network time of all transactions
- **Total Client Time** – the average client time of all transactions
- **Total Transaction Runs** – the sum of all the transaction run instances for each transaction
- **Total Slow Transaction Runs** – the sum of all the slow transaction runs for each transaction

Viewing Data for Each End-User Group that Ran a Transaction



To view data for each end-user group that ran a transaction, click the **View End Users** button in the row of the transaction for which you want to view this data. The Transaction Broken Down by End Users page opens. For details on this page, see "Transaction Broken Down by End Users" on page 122.

Viewing Data Over Time for a Transaction



To view data over time for a transaction, click the **View Data over Time** button in the row of the transaction for which you want to view data over a period of time. The Transaction Over Time page opens. For details on this page, see "Transaction Over Time" on page 123.

Server Performance Tab

The Server Performance tab displays server performance data for each configured transaction that was monitored. It contains the following columns:

Column	Explanation
Transaction	Displays the names you assigned the transactions in Monitor Administration.
Server Time	Displays the total server time of all the pages included in the transaction. This column is color-coded, based on the transaction's server time in relation to the transaction server time threshold you configured in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Server Time Threshold	Displays the server time threshold configured for each transaction defined in Monitor Administration.
Net Time	Displays the total download time of all the pages included in the transaction (in Monitor Administration, you define for each page included in the transaction whether this includes download time only, or both download time and think time), in seconds, for each transaction.
Transaction Runs	Displays the total number of run instances for each transaction.
Slow Transaction Runs	Displays, for each transaction, the number of run instances whose server time exceeded the configured transaction server time threshold.
Server Time of Slow Transaction Runs	Displays the average server time, in seconds, of each transaction's slow runs.

Viewing the Summary Row

If summary rows have been enabled (for details, see "Enabling Summary Rows" on page 76), you can view the following:

- **Total Server Time** – the average server time of all transactions
- **Total Net Time** – the average net time of all transactions
- **Total Transaction Runs** – the sum of all the transaction run instances for each transaction
- **Total Slow Transaction Runs** – the sum of all the slow transaction runs for each transaction

Viewing Data for Each End-User Group that Ran a Transaction



To view data for each end-user group that ran a transaction, click the **View End Users** button in the row of the transaction for which you want to view this data. The Transaction Broken Down by End Users page opens. For details on this page, see "Transaction Broken Down by End Users" on page 122.

Viewing Data Over Time for a Transaction



To view data over time for a transaction, click the **View Data over Time** button in the row of the transaction for which you want to view data over a period of time. The Transaction Over Time page opens. For details on this page, see "Transaction Over Time" on page 123.

Transaction Broken Down by End Users

The Transaction Broken Down by End Users page displays general, availability, total performance, net performance, or server performance data for each end-user group that ran the transaction you selected, depending on the table from which you accessed the Transaction Broken Down by End Users page. The columns in each table (except for the first column) are identical to those displayed for the same table in the main Transaction Summary report.

Note that the thresholds active filter you set for the Transaction Summary report is not relevant for the Transaction Broken Down by End Users tables. You must set a separate thresholds active filter for these tables. For information on setting an active filter, see "Using the Real User Monitor Active Filters" on page 79.

To return to the corresponding main Transaction Summary report, click the **Transaction Summary** link in the breadcrumb at the top of the page. For information on breadcrumbs, see "Navigating Mercury Business Availability Center" in *Getting Started with Mercury Business Availability Center*.

Viewing Data Over Time for Each End-User Group

You can view a graph of each end-user group's transaction activity over time.

To view a graph of each end-user group's transaction activity over time:



On the Transaction Broken Down by End Users page, in the row of the end-user group for which you want to view information over a period of time, click the **View Data over Time** button. The End-User Transaction Activity Over Time page opens, displaying a graph of the end-user group's general, availability, total performance, net performance, or server performance activity vis-a-vis the selected transaction, over the course of time. For details on these graphs, see "Transaction Over Time" below.

To return to the Transaction Broken Down by End Users table from which you accessed the End-User Transaction Activity Over Time graph, click the **Transaction Broken Down by End Users** link in the breadcrumb at the top of the page. To return to the corresponding table in the main Transaction Summary report, click the **Transaction Summary** link in the breadcrumb at the top of the page. For information on breadcrumbs, see "Navigating Mercury Business Availability Center" in *Getting Started with Mercury Business Availability Center*.

Transaction Over Time

The Transaction Over Time page displays a graph of general, availability, total performance, net performance, or server performance data for each transaction over the course of time, depending on the table from which you accessed the Transaction Over Time page.

The table underneath each graph displays transaction runs, availability, total time, net time, network time, server time, and client time for each point over the course of the defined time period.

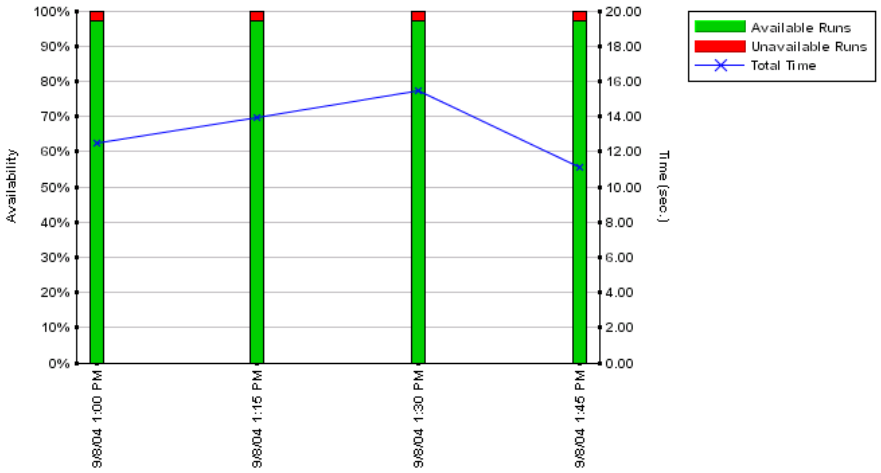
To return to the corresponding main Transaction Summary report, click the **Transaction Summary** link in the breadcrumb at the top of the page. For information on breadcrumbs, see "Navigating Mercury Business Availability Center" in *Getting Started with Mercury Business Availability Center*.

General Graph

The x-axis displays the time division units for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

The left y-axis displays transaction availability percentage units. The bars indicate the percentage of available and unavailable transaction runs, according to the color coding in the legend, at each point over the course of the defined time period. The right y-axis displays total transaction time units (seconds). The line connecting the data points indicates the total time of the transaction at each point over the course of the defined time period.

For example, the graph below shows transaction availability and total transaction time over the course of an hour. At 1:00 PM, the average total time of the transaction runs was approximately 12.5 seconds. At 1:15 PM, the average total time of the transaction runs increased to about 14 seconds. At 1:30 PM, the average total time of the transaction runs increased further to about 15.5 seconds. Finally, at 1:45 PM, the average total time of the transaction runs decreased to approximately 11 seconds. Transaction availability remained steady at 97 percent throughout the hour.

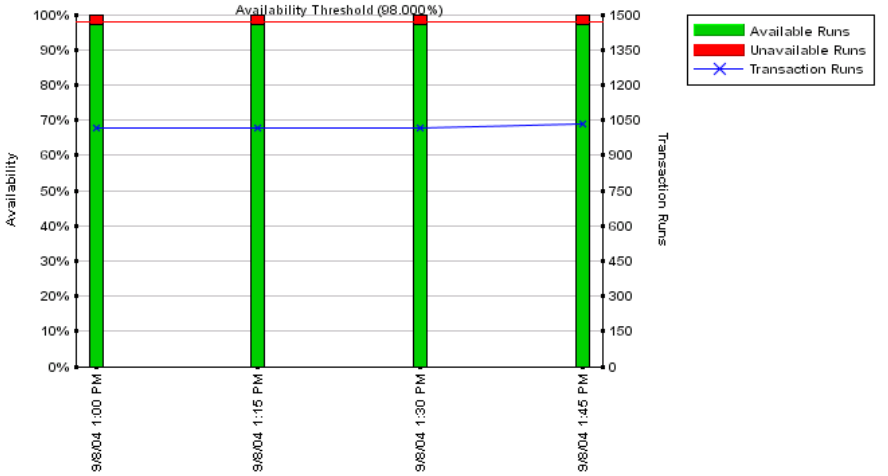


Availability Graph

The x-axis displays the time division units for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

The left y-axis displays transaction availability percentage units. The bars indicate the percentage of available and unavailable transaction runs, according to the color coding in the legend, at each point over the course of the defined time period. The right y-axis displays transaction run units. The line connecting the data points indicates the number of transaction runs at each point over the course of the defined time period. The horizontal red Availability Threshold line displays the transaction availability threshold that you configured in Monitor Administration.

For example, the graph below shows transaction availability and the number of transaction runs over the course of an hour. At each point during this period of time, there were approximately 1000 transaction runs. Transaction availability remained steady at 97 percent—just beneath the threshold configured in Monitor Administration (98%).

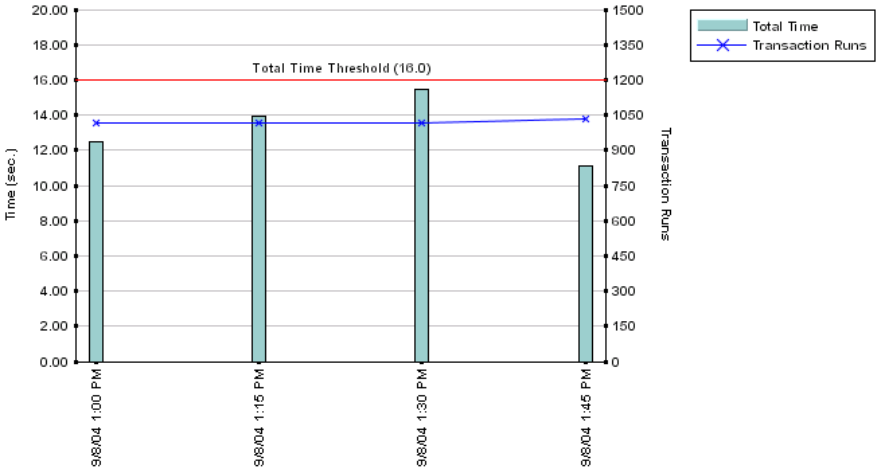


Total Performance Graph

The x-axis displays the time division units for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

The left y-axis displays total transaction time units (seconds). The bars indicate the total transaction time of the transaction runs, at each point over the course of the defined time period. The right y-axis displays transaction run units. The line connecting the data points indicates the number of transaction runs at each point over the course of the defined time period.

For example, the graph below shows total transaction time and the number of transaction runs over the course of an hour. While at each point during this period of time there were approximately 1000 transaction runs, the average total transaction time fluctuated from about 12.5 seconds at 1:00 PM, to just under 14 seconds at 1:15 PM, to approximately 15.5 seconds at 1:30 PM, and then decreased to about 11 seconds at 1:45 PM. Throughout this period of time, the total transaction run time did not rise above 16 seconds, the threshold configured in Monitor Administration.

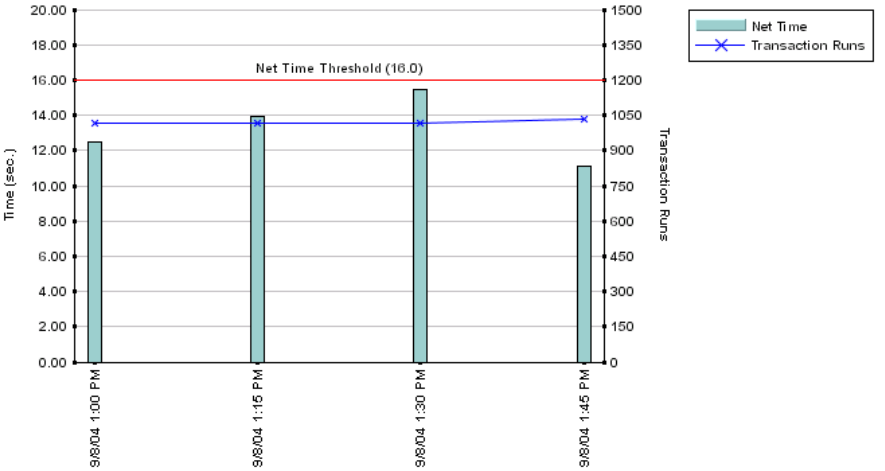


Net Performance Graph

The x-axis displays the time division units for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

The left y-axis displays net transaction time units (seconds). The bars indicate the net transaction time of the transaction runs, at each point over the course of the defined time period. The right y-axis displays transaction run units. The line connecting the data points indicates the number of transaction runs at each point over the course of the defined time period.

For example, the graph below shows net transaction time and the number of transaction runs over the course of an hour. While at each point during this period of time there were approximately 1000 transaction runs, the average net transaction time (which was the same as the total transaction time in this case) fluctuated from about 12.5 seconds at 1:00 PM, to just under 14 seconds at 1:15 PM, to approximately 15.5 seconds at 1:30 PM, and then decreased to about 11 seconds at 1:45 PM. Throughout this period of time, the total transaction run time did not rise above 16 seconds, the threshold configured in Monitor Administration.

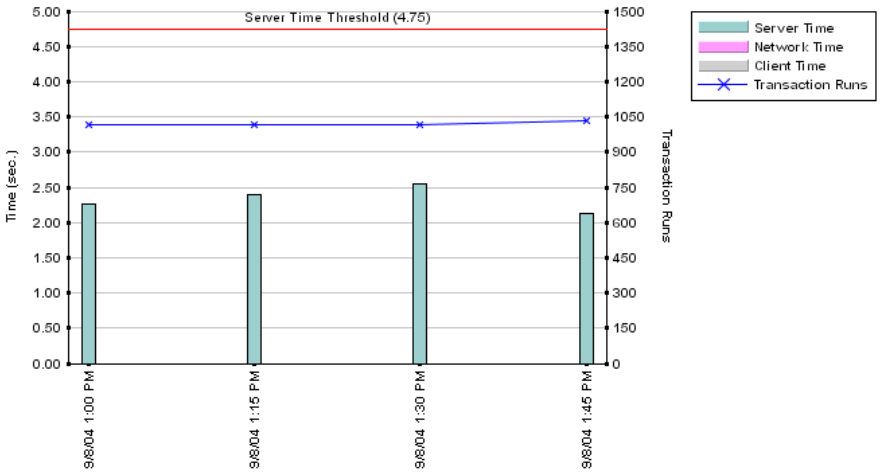


Server Performance Graph

The x-axis displays the time division units for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

The left y-axis displays transaction server time units (seconds). The bars indicate various statuses of the transaction runs, according to the color coding in the legend, at each point over the course of the defined time period. The right y-axis displays transaction run units. The line connecting the data points indicates the number of transaction runs at each point over the course of the defined time period.

For example, the graph below shows transaction server time and the number of transaction runs over the course of an hour. While at each point during this period of time there were approximately 1000 transaction runs, the average transaction server time fluctuated slightly from 2.25 seconds at 1:00 PM, to 2.4 seconds at 1:15 PM, to 2.55 seconds at 1:30 PM, to just over 2.1 seconds at 1:45 PM. Throughout this period of time, the server time did not rise above 4.75 seconds, the threshold configured in Monitor Administration.



End User Summary Report

The End User Summary report displays data for specific end-user groups that were configured for Real User Monitor in Monitor Administration. For information on configuring end-user groups to be monitored, see "Configuring End-User Groups" in *End User Management Data Collector Configuration*.

Note: You can set an active filter for the End User Summary report. For information on setting active filters, see "Using the Real User Monitor Active Filters" on page 79.

The End User Summary report contains the following columns:

Column	Explanation
End User	Displays the names the end-users groups that were defined in Monitor Administration, as well as the end-user group IP addresses.
End-User Location	Displays the geographic location of each end-user group.
Latency	Displays the average network latency, in milliseconds, for each configured end-user group. This column is color-coded, based on the end-user group's latency in relation to the end-user latency threshold you configured in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Latency Threshold	Displays the latency threshold configured for each end-user group in Monitor Administration.
Page Hits	Displays the total number of page hits generated by each end-user group.
Slow Page Hits	Displays, for each end-user group, the total number of pages whose average network latency exceeded the configured latency threshold.
Slow Pages Latency	Displays the average latency, in milliseconds, of each end-user group's slow page hits.
HTTP Traffic	Displays the number of kilobytes that each end-user group sent to, and received from, the server (s) via HTTP.
HTTPS Traffic	Displays the number of kilobytes that each end-user group sent to, and received from, the server(s) via HTTPS.

Viewing the Summary Row

If summary rows have been enabled (for details, see "Enabling Summary Rows" on page 76), you can view the following:

- **Total Slow Page Hits** – the sum of all the slow page hits for each end-user group
- **Total HTTP Traffic** – the sum of all the sent and received HTTP kilobytes for each end-user group
- **Total HTTPS Traffic** – the sum of all the sent and received HTTPS kilobytes for each end-user group

Viewing Data Over Time

You can view a graph and table displaying data over time for each end-user group.

To view data over time for an end-user group:

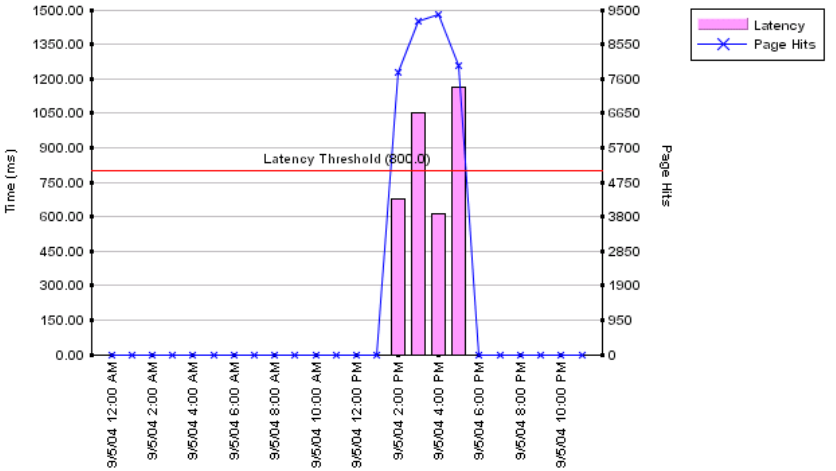


Click the **View Data over Time** button in the row of the end-user group for which you want to view information over a period of time. The End User Over Time page opens, displaying a graph and table of the end-user group's connections and latency over the course of time.

The x-axis displays the time division units for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

The left y-axis displays network latency time units (milliseconds). The bars indicate the network latency at each point over the course of the defined time period. The right y-axis displays total page hits. The line connecting the data points indicates how many page hits there were at each point over the course of the defined time period. The horizontal red Latency Threshold line displays the end-user latency threshold that you configured in Monitor Administration.

For example, the graph below shows network latency and total page hits over the course of a day. At 2:00 PM on September 5, when there were approximately 7800 end-user page hits, network latency was about 700 milliseconds. At 3:00 PM, when there were approximately 9000 end-user page hits, network latency rose above the latency threshold configured in Monitor Administration (800 milliseconds), to about 1 second. At 4:00 PM, there were approximately the same number of end-user page hits, but network latency remained below the latency threshold at approximately 600 milliseconds. At 5:00 PM, the number of end-user page hits decreased to approximately 8000. However, network latency rose above the latency threshold to just over 1100 milliseconds.



The table underneath the graph contains the same information as the graph, in a table format.

To return to the main End User Summary report, click the **End User Summary** link in the breadcrumb at the top of the page. For information on breadcrumbs, see "Navigating Mercury Business Availability Center" in *Getting Started with Mercury Business Availability Center*.

Server Summary Report

The Server Summary report displays data for the servers that are monitored by the Real User Monitor probe. For information on configuring the probe to monitor specific servers, see "Configuring a Probe" in *End User Management Data Collector Configuration*. To assign a specific name to a monitored server, see "Defining a Server Name" in *End User Management Data Collector Configuration*.

Note: You can set an active filter for the Server Summary report. For information on setting active filters, see "Using the Real User Monitor Active Filters" on page 79.

The Server Summary report contains the following columns:

Column	Explanation
Server Name	Displays the names you assigned the monitored servers in Monitor Administration.
IP Address	Displays the IP address of each server.
Server Availability	Displays the percentage of requests for which each server was available. This column is color-coded, based on the server's availability in relation to the server availability threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical
HTTP Traffic	Displays the number of megabytes transmitted to and from each server via HTTP.
HTTPS Traffic	Displays the number of megabytes transmitted to and from each server via HTTPS.
Hits	Displays the total number of page requests received by each server.

Column	Explanation
Component Hits	Displays the total number of component requests received by each server.
Components Causing Server Errors	Displays, for each server, the total number of component requests that encountered internal server problems.

Viewing the Summary Row

If summary rows have been enabled (for details, see "Enabling Summary Rows" on page 76), you can view the following:

- **Total Availability** – the average availability of all servers (that is, the total number of successful hits for all servers divided by the total number of hits for all servers)
- **Total HTTP Traffic** – the sum of all the sent and received HTTP megabytes for each server
- **Total HTTPS Traffic** – the sum of all the sent and received HTTPS megabytes for each server
- **Total Hits** – the sum of all the hits to each server
- **Total Component Hits** – the sum of all the component hits to each server
- **Total Components Causing Server Errors** – the sum of all the components causing server errors for each server

Viewing Data Over Time

You can view a graph and table displaying data over time for each server.

To view data over time for a server:

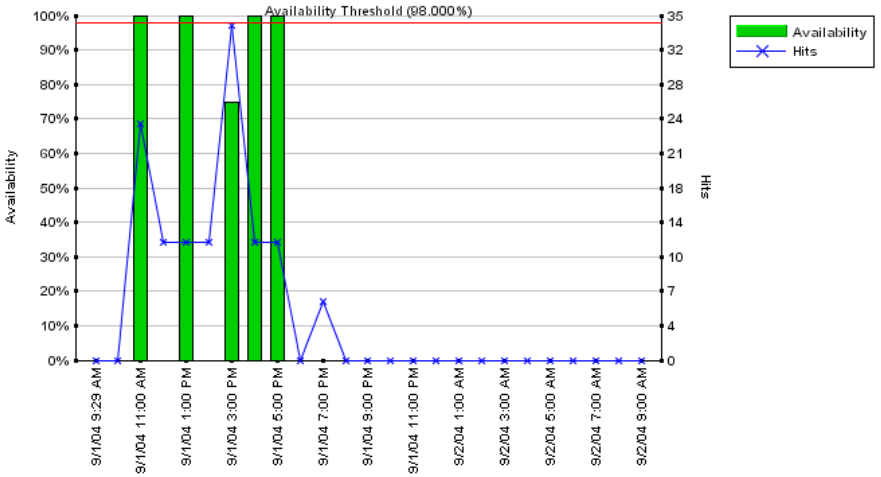


Click the **View Data over Time** button in the row of the server for which you want to view information over a period of time. The Server Over Time page opens, displaying a graph and table of the server's page hits and availability over the course of time.

The x-axis displays the time division units for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

The left y-axis displays server availability percentage units. The bars indicate the server's availability at each point over the course of the defined time period. The right y-axis displays server page hit units. The line connecting the data points indicates how many page hits were received by the server at each point over the course of the defined time period. The horizontal red Availability Threshold line displays the server availability threshold that you configured in Monitor Administration.

For example, the graph below shows server availability and page hits over the course of a day. While server availability was 100 percent at 11:00 AM, 1:00 PM, 4:00 PM, and 5:00 PM, the server was not available at all at 12:00 PM, 2:00 PM, and 7:00 PM, and was only 75 percent available (below the server availability threshold defined in Monitor Administration) at 3:00 PM.



The table underneath the graph contains the same information as the graph, in a table format.

To return to the main Server Summary report, click the **Server Summary** link in the breadcrumb at the top of the page. For information on breadcrumbs, see "Navigating Mercury Business Availability Center" in *Getting Started with Mercury Business Availability Center*.

Viewing Pages by Server

You can view a summary of pages that you configured for monitoring in Monitor Administration, that were hit by a specific server. For information on configuring pages to be monitored, see "Configuring Pages" in *End User Management Data Collector Configuration*.

To view the summary of monitored pages hit by a server:



Click the **View Pages by Server Summary Report** button in the row of the server for which you want to view page summary data. The Pages by Server Summary report opens, displaying a table showing each page hit by the server for which you are viewing data. For each page, the following columns are displayed:

Column	Description
Page	Displays the page name configured for the page in Monitor Administration.
Page Size	Displays the size of the page in Kilobytes.
Availability	Displays the percentage of requests for which each page was available. The page availability may be different from the server availability in the main Server Summary report as page and server availability are not based on the same criteria.
Page Time	Displays the average amount of time, in seconds, it took for the page to download. This column is color-coded, based on the page's download time in relation to the page time threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Page Threshold	Displays the page time threshold configured for the page in Monitor Administration.

Column	Description
Server Time	Displays the average amount of time, in seconds, that it took the server to process the requests for the page. This column is color-coded, based on the page's server time in relation to the server time threshold you defined in Monitor Administration. ➤ Green = OK ➤ Red = Critical
Server Time Threshold	Displays the server time threshold configured for the page in Monitor Administration.
Hits	Displays the total number of requests that the page received.
Slow Hits	Displays the total number of hits whose page time exceeded the configured page time threshold.
Server Time Slow Hits	Displays the average server time, in seconds, for the page's slow hits.

To return to the corresponding main Server Summary report, click the **Server Summary** link in the breadcrumb at the top of the page. For information on breadcrumbs, see "Navigating Mercury Business Availability Center" in *Getting Started with Mercury Business Availability Center*.

Note:

- The report uses the same time range as that selected for the main Server Summary report, but will not exceed 24 hours. If the time range selected is longer than 24 hours, the last 24 hour period of the time range is used.
- The report uses raw Real User Monitor data.

Session Analyzer Report

The Session Analyzer report displays session data for specific applications that were configured for Real User Monitor in Monitor Administration. Sessions in applications that have not been configured for monitoring are also reported as part of a default entity for other applications, called **<engine name>'s other applications**. For example, for a configured Real User Monitor engine called **myengine**, the default entity for non-monitored applications is **myengine's other applications**. For information on configuring applications to be monitored, see "Configuring Applications" in *End User Management Data Collector Configuration*.

Note:

- You can set an active filter for the Session Analyzer report. For information on setting active filters, see "Using the Real User Monitor Active Filters" on page 79.
- You can customize the Session Analyzer report. By default, the Session Analyzer report is not set to be auto generated. For details on customizing reports, see "Customizing Reports" in *Platform Administration*.

The Session Analyzer report contains the following columns:

Column	Explanation
Start Time	Displays the date and time the session was started.
End User Group	Displays the end-user group to which the end-user who initiated the session belongs, as configured in Monitor Administration.
End User	Displays the name of the end-user who initiated the session, or an IP address or computer name if the end-user name is not found.
Duration	Displays the length of time that the session was active.

Column	Explanation
Application Errors	Displays the number of application errors encountered during the session, based on the application error events you defined for the application in Monitor Administration. If the number of application errors is greater than 0 it is displayed in red.
HTTP Errors	Displays the number of HTTP errors encountered during the session, based on the global HTTP error events you defined in Monitor Administration. If the number of HTTP errors is greater than 0 it is displayed in red
Events	Displays the number of application events encountered during the session, based on the a events you defined for the application in Monitor Administration.
Slow Pages	Displays, for each session, the total number of pages whose page time exceeded its configured threshold. If the number of slow pages is greater than 0 it is displayed in red
Page Hits	Displays the total number of page hits generated during each session.

Viewing Deep Transaction Tracing Data

If you have deployed Bristol TransactionVision's Deep Transaction Tracing package in Mercury Business Availability Center, you can view TransactionVision's Transaction Tracking Report to see detailed information of the session at component level. For details on deploying the Deep Transaction Tracing package, see "Deployment and Set Up for Deep Transaction Tracing" in *Application Administration*.

To view the Transaction Tracking Report:



Click the **View Deep Transaction Tracing Data** button in the row of the session for which you want to view the Transaction Tracking Report. The Transaction Tracking report opens showing transaction details for the session. For more details on the Transaction Tracking Report, refer to the

TransactionVision documentation, available from the Help menu in the TransactionVision application.

Viewing Session Details

You can view details of a session in order to see property, event, and page data for the session.

When you view session details, the report is regenerated and contains the most current data for the selected session. This means that if the session was still open when the Session Analyzer report was generated, the data included in the Session Detail page will be more up to date and may differ from that included in the Session Analyzer report for the same session.

When viewing session details, all the pages that are included in all monitored application sessions that started on the same day as the application session for which you are viewing data, and that are part of the entire application server session, are displayed. For example, in Monitor Administration you configure three applications. My_application_A consists of page_1, page_2, and page_3, my_application_B consists of page_4, page_5, and page_6, and my_application_C consists of page_7, page_8, and page_9. You log in to Mercury Business Availability Center and at 11:59 PM you hit page_1. After midnight (that is, when the date has changed) you hit all the other pages. You then log out of Mercury Business Availability Center. You run the Session Analyzer report for my_application_B and the session described above is included in the report and shows 3 page hits (page_4, page_5, and page_6), but when you drill down to view session details, all the pages from my_application_B and my_application_C are displayed and not only the pages for my_application_B. The pages for my_application_A are not displayed as the application session was started on the previous day to the requested application (my_application_B).

Note:

- Events displayed when viewing session details are the events that occurred only on the pages configured in Monitor Administration as being part of the application.
- When clicking on the breadcrumb to return to the Session Analyzer report, the report is not regenerated and the original Session Analyzer report is redisplayed.

To view details of a session:



Click the **View Session Details** button in the row of the session for which you want to view details. The Session Detail page opens and contains the following panes:

- Properties – see next section
- General Events – see page 143
- Pages – see page 143

Properties

The Properties pane displays the following data about the session:

Field	Explanation
Start Time	Displays the date and time the session was started.
Overall Traffic	Displays the total number of kilobytes sent from and received by the session.
Duration	Displays the total time that the session was open.
Operating System	Displays the operating system of the machine on which the end-user initiated the session.
Browser	Displays the browser used by the end-user to initiate the session.
Location	Displays the name of the location of the end-user who initiated the session.

Field	Explanation
End User Group	Displays the end-user group to which the end-user who initiated the session belongs, as configured by you in Monitor Administration.
Client IP	Displays the IP address of the end-user who initiated the session.
Computer Name	Displays the host name of the machine of the end-user who initiated the session.
User Name	Displays the name of the end-user who initiated the session.
Server IP	Displays the IP address of the server (or load balancer) reached by the end-user.
Arrived From	Displays the page from which the end-user reached the session.

General Events

The Events pane displays a table with data about events configured in Monitor Administration that occurred in the session. The table includes two columns, the first shows the event name and the second shows the event description.

Pages

The Pages pane displays a table of all the pages that were hit during the session. The table contains the following columns:

Column	Explanation
Start Time	Displays the date and time the page was hit.
Application	Displays the application session in which the page was hit. This field is highlighted for the selected application session.
Page	Displays the name of the page that was hit, as defined by you in Monitor Administration, or its URL if no name is defined.

Column	Explanation
Events	Displays the name of events that occurred on the page, based on the events you defined for the page in Monitor Administration.
Page Time	Displays the amount of time, in seconds, it took for the page to download.

Viewing Page Details

You can view details of a page.

To view details of a page:



Click the **View Page Details** button in the row of the page for which you want to view details. The Page Detail page opens and contains the following panes:

- General – see next section
- Events – see page 145
- URL Parameters – see page 145

General

The General pane contains the following data about the page:

Field	Explanation
Page	Displays the name configured for the page in Monitor Administration, or blank if the page has not been configured.
URL	Displays the URL of the page.
Server IP	Displays the IP address of the server on which the page was located.
Server Name	Displays the name of the server on which the page was located.
Start Time	Displays the date and time the page was hit.

Field	Explanation
Number of Components	Displays the number of components included in the page.
Page Time	Displays the total amount of time, in seconds, from when the page was requested until it finished loading.
Page Threshold	Displays the page time threshold configured for the page in Monitor Administration.
Server Time	Displays the amount of time, in seconds, that it took the server to process the request for the page.
Server Threshold	Displays the server time threshold configured for the page in Monitor Administration.
Network Time	Displays the amount of time, in seconds, that the page was active on the network.
Client Time	Displays the amount of time, in seconds, that the page was active on the client machine.
Page Size	Displays the downloaded size, in kilobytes, of the page.
HTTP Method	Displays the HTTP method used to access the page.
Stopped	Displays whether or not the page downloading was stopped by the end-user.

Events

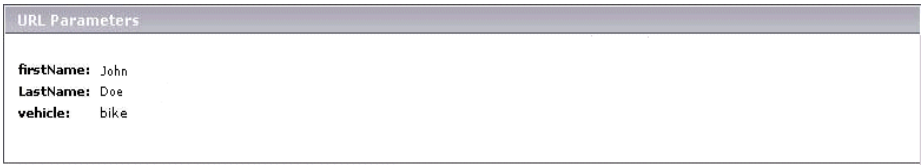
The Events pane displays a table with data about events configured in Monitor Administration that occurred on the page. The table includes two columns, the first shows the event name and the second shows the event description.

URL Parameters

The URL Parameters pane displays the names and values of any parameters that were included in the page's URL, which is displayed in the General pane.

For example, the URL Parameters pane below would be displayed for the following URL:

http://www.myDomain.com:8080/application1/page3.jsp?firstName=John&lastName=Doe&vehicle=bike



Viewing Deep Transaction Tracing Data

If you have deployed Bristol TransactionVision's Deep Transaction Tracing package in Mercury Business Availability Center, you can view TransactionVision's Transaction Tracking Report to see detailed information of the page at component level. For details on deploying the Deep Transaction Tracing package, see "Deployment and Set Up for Deep Transaction Tracing" in *Application Administration*.

To view the Transaction Tracking Report:



Click the **View Deep Transaction Tracing Data** button in the row of the page for which you want to view the Transaction Tracking Report. The Transaction Tracking report opens showing transaction details for the page. For more details on the Transaction Tracking Report, refer to the TransactionVision documentation, available from the Help menu in the TransactionVision application.

Viewing Snapshot Details

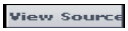
You can view snapshots of pages, if the Real User Monitor engine has been configured to take snapshots of pages on error in Monitor Administration (for details, see "Configuring Real User Monitor Engine Settings" in *End User Management Data Collector Configuration*), and the application has been configured to enable snapshots (for details, see "Configuring Applications" in *End User Management Data Collector Configuration*).

By default, page snapshots are displayed as HTML. If you are a system administrator, you can configure Mercury Business Availability Center to display snapshots as images by changing the **Show Snapshot as an Image** setting to **true**. To access this setting, click **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, select **End User/System Availability Management** in the **Applications** context, and scroll down to the **End User/System Availability Management - Data** table.

To view a snapshot of a page:



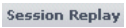
Click the **View Snapshot of Page** button in the row of the page for which you want to view the snapshot. The Page Snapshot page opens displaying a picture of the page accessed by the user when the error occurred.



To view the HTML source code of the snapshot, click the **View Source** button at the bottom of the snapshot. A new window opens displaying the source code.

Note: If no snapshot exists for the page, the **View Snapshot of Page** button is disabled.

To replay a session:



To view a session flow page by page, click the **Session Replay** button above the table of pages. The Session Flow window opens, displaying two panes. In the left hand pane, a list of all the pages in the session is displayed, as well as entry for the session properties. Click on the item in the list you want to view.

In the right pane are two tabs. If you click **Session properties** in the left pane list, the **Properties** tab displays general session properties (for details, see "Properties" on page 142) and the **General Events** tab displays the name and description of configured events that occurred in the session. If you click a page in the left pane list, the **Snapshot View** tab displays the snapshot of the page, if it exists, and the **Details** tab displays general page details and configured events that occurred on the page (for details, see "Viewing Page Details" on page 144). To view the HTML source code of a snapshot, click



the **View Source** button at the bottom of the snapshot. A new window opens displaying the source code.



To browse the snapshots, click the **Previous** and **Next** buttons above the left pane.



To download all the snapshots to a zip file, click the **Download** button above the left pane.

Note: If the snapshot requested is one of an HTTP Not Found error (HTTP error code 404), in some instances the link to the referring machine will be to a Mercury Business Availability Center server machine instead of to the original Web server machine that reported the error. This is due to an html script that generates a link being stored in the snapshot, rather than the actual link itself.

Defining a Page



If you are a system administrator, you can click the **Define Page** button if a page is not defined in Monitor Administration and you want to define the page's properties and add it to the list of configured pages in Monitor Administration. (For details on configuring pages in Monitor Administration, see "Configuring Pages" in *End User Management Data Collector Configuration*.)

In the Define Page dialog box that opens, enter the name you want to assign the page, edit the URL of the page (if necessary), and select the group to which you want to assign the page. The URL displayed is a URL suggested by Mercury Business Availability Center that will allow improved correlation (that is, more possibilities for matching pages to the URL). If you do not want to use the suggested URL, clear the **Use suggested URL for improved correlation** check box to revert to the page's original URL.

The newly defined page is added to the page group you stipulated in Monitor Administration. Note that this page will only be listed as defined when the next data sample is compiled by the Real User Monitor engine.

Note:

- By default, asterisks in URLs are treated as wildcards. To define an asterisk as a literal and not as a wildcard, precede it with a backslash (\). For example, **my*str**.

- When you add a page using the Define Page dialog box, the page acquires the default settings for page thresholds that you configure in Monitor Administration. If you want to change any of the page's default settings, you must do so in Monitor Administration.

Event Count Over Time Report

The Event Count Over Time report displays data for all events, or sessions with events, in monitored applications that you configured in Monitor Administration, broken down by time intervals. For information on configuring applications to be monitored, see "Configuring Applications" in *End User Management Data Collector Configuration*.

Note:

You can set an active filter for the Event Count report. For information on setting active filters, see "Using the Real User Monitor Active Filters" on page 79.

You can customize the Event Count Over Time report. For details on customizing reports, see "Customizing Reports" in *Platform Administration*.

The data in the Event Count Over Time report can be viewed either as a graph, or as a table, by clicking on the appropriate tab. The report opens in the graph view by default.

You can choose to view individual events, or sessions with events, in the report by selecting the appropriate option before generating the report.

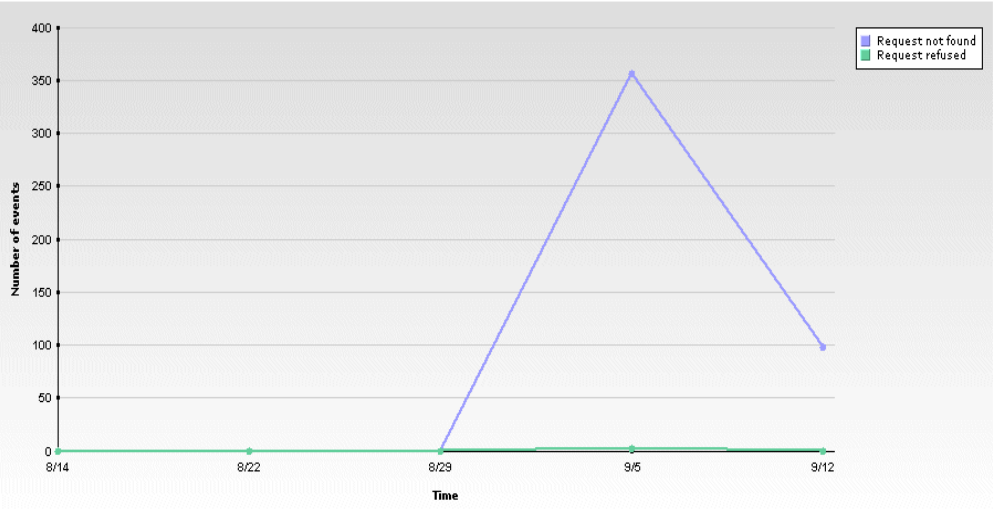
Viewing the Event Count Over Time Report as a Graph

The x-axis displays the time division units for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

The y-axis displays events or sessions, depending on the selection you made.

A different colored line on the graph is shown for each type of event that you configured for the monitored application. For information on configuring applications to be monitored, see "Configuring Applications" in *End User Management Data Collector Configuration*.

For example, the graph below shows the number of events that occurred in a monitored application over the course of a month. During the week of September 5, the monitored application encountered 356 **Request not found** events, as indicated by the purple line, and 2 **Request refused** events, as indicated by the green line.



You can click on an individual point to obtain more detailed information for a specific event type. For example, if you click on the highest point on the purple line in the graph above, you will see another graph showing **Request not found events** only, for a time period of the week of September 5 at one day intervals.

You can keep drilling down for more detailed information until you reach an exact date and time for an individual event. The minimum time range to which you can drill down is one minute.

Viewing the Event Count Over Time Report as a Table

The table shows a column for each time division unit for the time range that you defined when generating the report. For details on modifying a report's time range, see "Choosing the Tracking Range and Granularity" in *Working with Applications*.

Each row in the table represents a different event type configured for the monitored application selected, or a different HTTP error event type configured for the Real User Monitor engine. For information on configuring applications to be monitored, see "Configuring Applications" in *End User Management Data Collector Configuration*. For information on configuring HTTP errors to be monitored, see "Configuring Real User Monitor Engine Settings" in *End User Management Data Collector Configuration*.

The number of events that occurred for each event type at each time division unit is displayed. You can click on an individual number in order to obtain more detailed information for that specific event type over a shorter time range.

You can keep drilling down for more detailed information until you reach an exact date and time for an individual event. The minimum time range to which you can drill down is one minute.

Event Summary Report

The Event Summary report displays a summary of events in monitored applications that you configured in Monitor Administration. For information on configuring applications to be monitored, see "Configuring Applications" in *End User Management Data Collector Configuration*.

Note: You can set an active filter for the Event Summary report. For information on setting active filters, see "Using the Real User Monitor Active Filters" on page 79.

Note: You can customize the Event Summary report. For details on customizing reports, see "Customizing Reports" in *Platform Administration*.

The data in the Event Summary report can be viewed either as a graph, or as a table, by clicking on the appropriate tab. The report opens in the **View as Graph** tab by default.

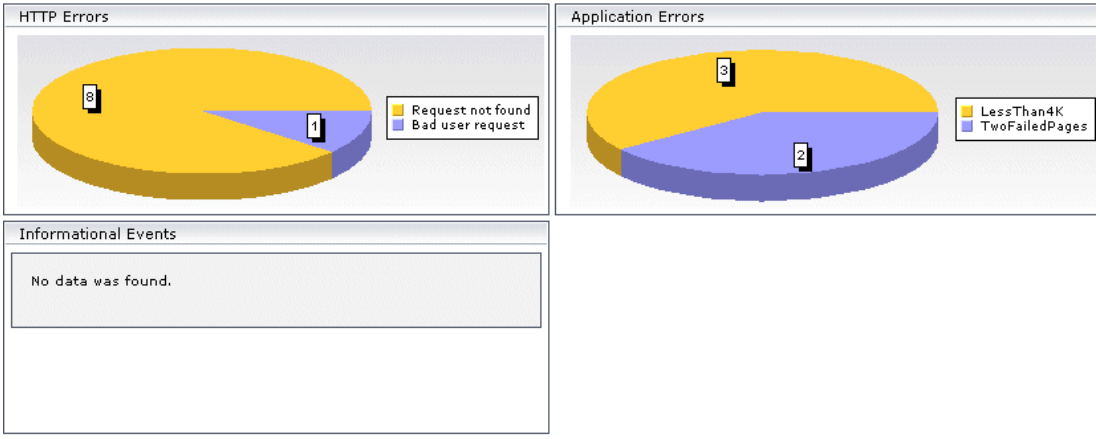
The Event Summary report shows data for informational events, application errors, and http errors, but you can deselect any of these options prior to generating the report by clearing the relevant check box.

Viewing the Event Summary report as a Graph

The Event Summary report contains three panes, one each for informational events, application errors, and http errors. If you deselect any of these options prior to generating the report, that specific pane will not be displayed.

Each pane displays a pie chart with color-coded slices for each type of event included in the pane's main event type, for which there is data. Up to 10 different slices can be displayed per chart.

For example, the graph below shows the event summary for a monitored application over the period of a month. Out of a total of 9 HTTP Errors that occurred, 8 were of a type called **Request not found** and 1 was of a type called **Bad user request**. Out of a total of 5 Application Errors that occurred, 3 were of a type called **LessThan4K** and 2 were of a type called **TwoFailedPages**. There were no informational events recorded for the application during the month.



To view the Event Log for a specific type of event, click on the slice in the pie chart that represents the event or error for which you want to view event log data. The Event Log opens. For details on this report, see "Event Log" on page 154.

Viewing the Event Summary report as a Table

The Event Summary report contains three tables, one each for informational events, application errors, and http errors. If you deselect any of these options prior to generating the report, that specific table will not be displayed.

Each table includes a row for every type of event included in the table's main event type, for which there is data. There are two columns, one displaying the number of events that occurred in the monitored application during the time range you specified for the report and the second displaying the number of sessions in which these events occurred.

To view the Event Log for a specific type of event, click on the **View Event Log** button in the row of the event type for which you want to view event log data. The Event Log opens. For details on this report, see "Event Log" below.

Event Log

The Event Log is a table with a row for each event of the specific type being viewed. The table includes the following columns:

Column	Explanation
Time	Displays the date and time that the event occurred.
Page	Displays the URL of the page on which the event occurred.
End User	Displays the name of the end-user group that hit the page on which the event occurred.
Event Description	Displays the event description as you configured in Monitor Administration.

Viewing Session Details

You can view details of a session in order to see property, event, and page data for the session.

To view details of a session:



Click the **View Session Details** button in the row of the session for which you want to view details. The Session Detail page opens and contains the following panes:

- Properties - see page 142
- General Events - see page 143
- Pages - see page 143

Business Process Distribution Report

The Business Process Distribution report shows transaction run and transaction response time data over time for the transactions that you configure in Monitor Administration. For information on configuring transactions to be monitored, see "Configuring Transactions" in *End User Management Data Collector Configuration*.

You choose the transactions to include in the Business Process Distribution report, by using one of two filter options – **Show X transactions...** or **Transaction Selection**:

- **Show X transactions...** – Choose the number of real-user transactions you want the report to display and the criteria according to which you want End User Management to select the transactions it displays.

  You can choose to display the transactions:

  - **with the greatest number of runs** – If you select this option, End User Management displays the real-user transactions that experienced the highest total number of run instances.
  - **with the worst response times** – If you select this option, End User Management displays the real-user transactions that experienced the greatest overall transaction time.

- **with the highest session popularity** – If you select this option, End User Management displays the real-user transactions that were most popular among the sessions. Note that popularity is determined by dividing the number of unique sessions running a transaction by the total number of sessions.
- **with the lowest availability** – If you select this option, End User Management displays the real-user transactions that experienced the lowest transaction availability.

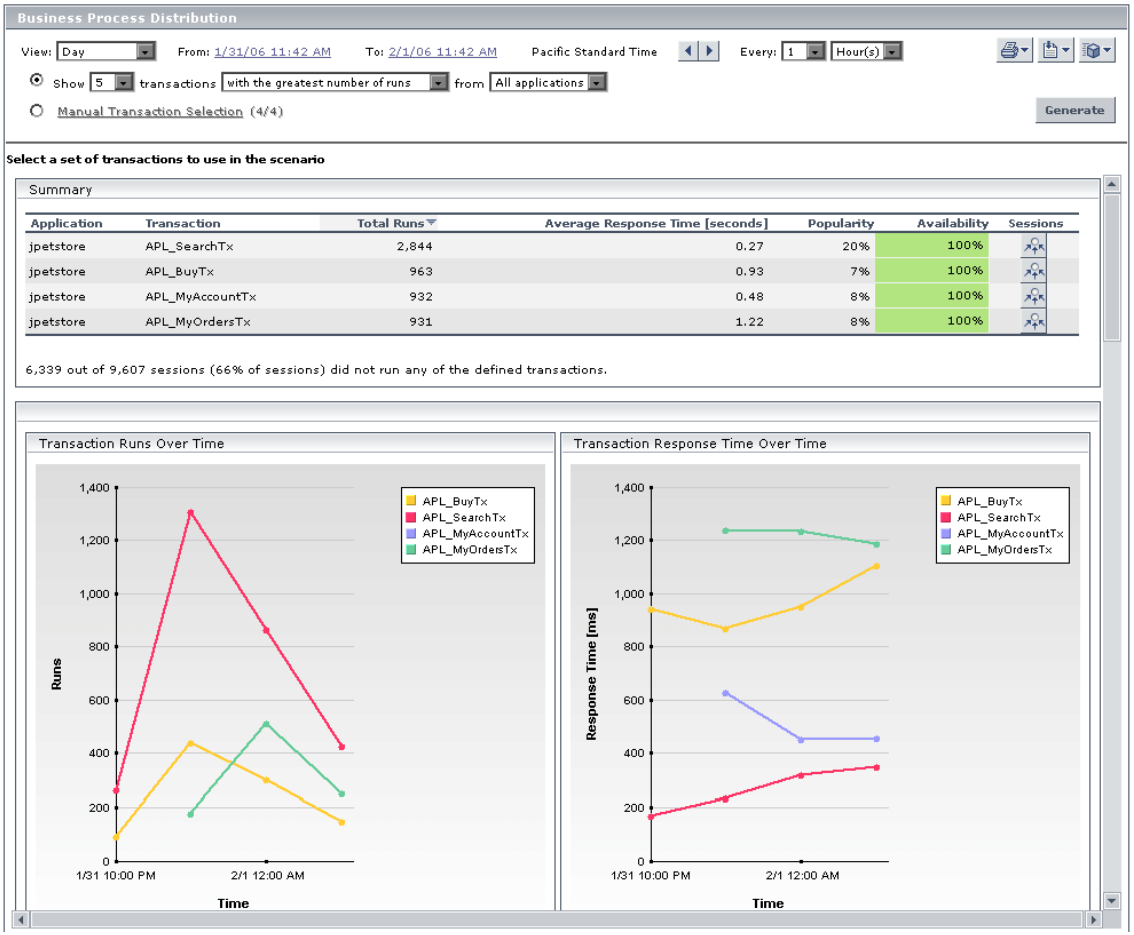
You can choose to display the transactions from all monitored applications that meet the selected criteria, or you can choose to display only transactions that were defined for a specific application.

- **Transaction Selection** – In the Select Transactions dialog box, choose **All applications** to display the transactions from all monitored applications, or choose a specific application to display only transactions that were defined for that application. Select the transaction(s) for which you want to view data, and click the first arrow. To view data for all the transactions listed, click the second arrow. Click **OK** to close the dialog box and save your settings.

When you click the **Generate** button, the Business Process Distribution report displays the following:

- a Summary table listing each transaction, the application with which the transaction is associated, the total number of run instances for the transaction, the average total transaction time, the percentage of sessions in which the transaction was run, and the transaction's availability. (Note that the color-coding of the Availability column is based on the transaction's availability in relation to the transaction availability threshold you defined in Monitor Administration.)
- the percentage of sessions in which the displayed transactions were run, which provides you with an indication of the number of sessions covered by the Real User Monitor transactions you configured
- the Transaction Runs Over Time graph

➤ the Transaction Response Time Over Time graph

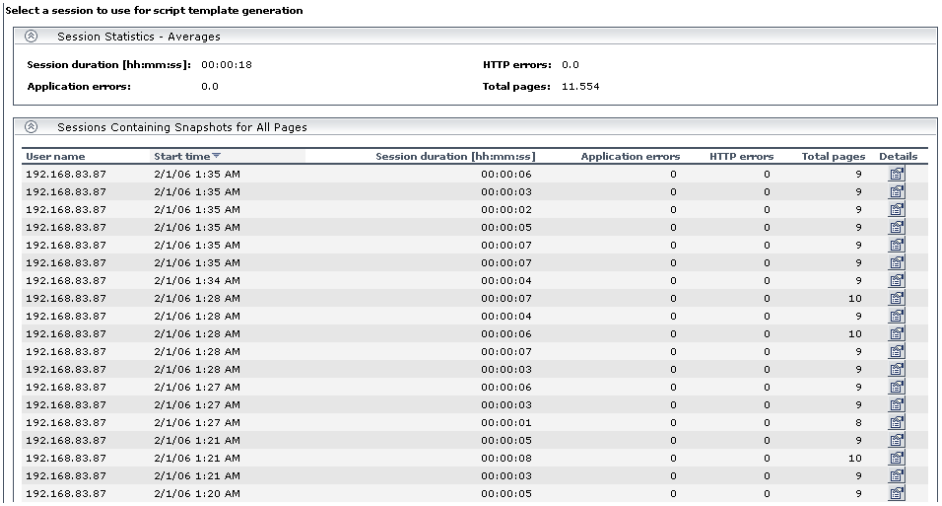


Analyzing the Business Process Distribution Report

You use the Business Process Distribution report to pinpoint the Real User Monitor transactions with the greatest number of runs and the highest session popularity. You then drill down in this report to view the individual sessions in which these transactions were run. You can also use the Business Process Distribution report to pinpoint the transactions that were problematic in terms of response time and availability and drill down so that you can isolate the sessions, and pages within the sessions, that were problematic.

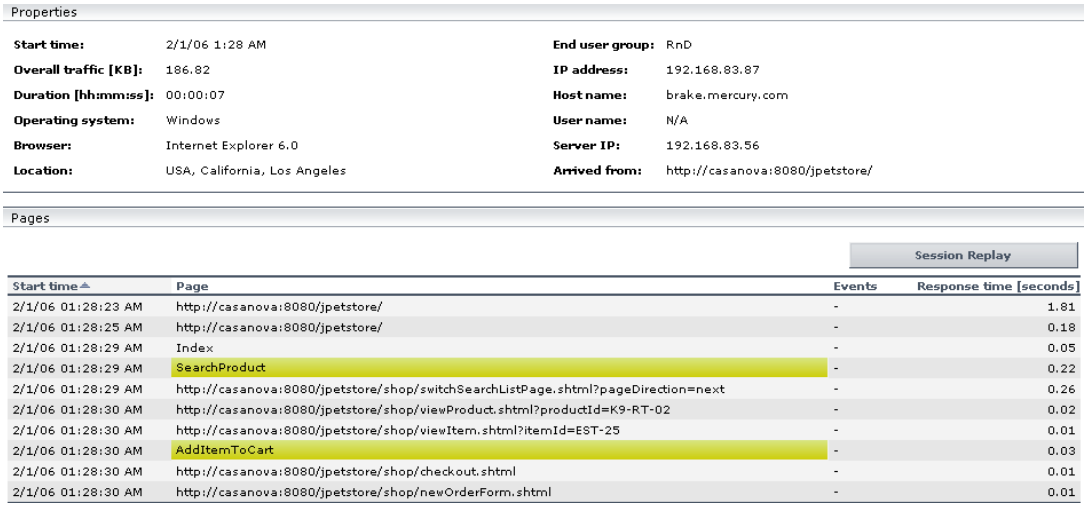
To analyze the Business Process Distribution report:

1 Select a transaction, based on the total number of runs for the transaction as well as the transaction's session popularity (or response time/availability data), and click the **View Sessions** button. The Sessions page opens, displaying data for each session in which the selected transaction was run and a transaction snapshot was collected, as well as certain key statistic averages of all the displayed sessions.



For additional information on the Sessions page, see the "Session Analyzer Report" on page 139.

2 Select a session, based on page hit and error data, and click the **View Session Details** button. The Session Details page opens, displaying general session and event information as well a list of all the pages accessed as part of the session and the events and response time for each page. The pages that were included in the selected transaction's definition are highlighted.



Properties

Start time:	2/1/06 1:28 AM	**End user group:**	RnD
Overall traffic [KB]:	186.82	**IP address:**	192.168.83.87
Duration [hh:mm:ss]:	00:00:07	**Host name:**	brake.mercury.com
Operating system:	Windows	**User name:**	N/A
Browser:	Internet Explorer 6.0	**Server IP:**	192.168.83.56
Location:	USA, California, Los Angeles	**Arrived from:**	http://casanova:8080/jpetstore/

Pages

Session Replay

Start time	Page	Events	Response time [seconds]
2/1/06 01:28:23 AM	http://casanova:8080/jpetstore/	-	1.81
2/1/06 01:28:25 AM	http://casanova:8080/jpetstore/	-	0.18
2/1/06 01:28:29 AM	Index	-	0.05
2/1/06 01:28:29 AM	SearchProduct	-	0.22
2/1/06 01:28:29 AM	http://casanova:8080/jpetstore/shop/switchSearchListPage.shtml?pageDirection=next	-	0.26
2/1/06 01:28:30 AM	http://casanova:8080/jpetstore/shop/viewProduct.shtml?productId=K9-RT-02	-	0.02
2/1/06 01:28:30 AM	http://casanova:8080/jpetstore/shop/viewItem.shtml?itemId=EST-25	-	0.01
2/1/06 01:28:30 AM	AddItemToCart	-	0.03
2/1/06 01:28:30 AM	http://casanova:8080/jpetstore/shop/checkout.shtml	-	0.01
2/1/06 01:28:30 AM	http://casanova:8080/jpetstore/shop/newOrderForm.shtml	-	0.01

Note: Event data is displayed only if you configured events for the application with which the transaction you are viewing is associated. For information on events and their configuration, see "Configuring Events" in *End User Management Data Collector Configuration*.

For additional information on the Session Details page, see "Viewing Session Details" on page 141.

Replaying a Session

Session Replay

To view a session flow page by page in your Web browser, click the **Session Replay** button above the table of pages. The Session Flow window opens, displaying two panes. In the left hand pane, a list of all the pages in the session is displayed, as well as entry for the session properties. Click on the item in the list you want to view.

In the right pane are two tabs. If you click **Session properties** in the left pane list, the **Properties** tab displays general session properties (for details, see "Properties" on page 142) and the **General Events** tab displays the name and description of configured events that occurred in the session. If you click a page in the left pane list, the **Snapshot View** tab displays the snapshot of the page, if it exists, and the **Details** tab displays general page details and configured events that occurred on the page (for details, see "Viewing Page Details" on page 144). To view the HTML source code of a snapshot, click



the **View Source** button at the bottom of the snapshot. A new window opens displaying the source code.



To browse the snapshots, click the **Previous** and **Next** buttons above the left pane.



To download all the snapshots to a zip file, click the **Download** button above the left pane.

Network Latency Report

The Network Latency report shows the average network latency (defined as the time it takes for a packet of data to get from one designated point to another and return to the original point) per end-user location for the transactions that you configured in Monitor Administration. For information on configuring transactions to be monitored, see "Configuring Transactions" in *End User Management Data Collector Configuration*.

The data in the Network Latency report can be viewed either as a graph, or as a table, by clicking on the appropriate tab. The report opens in the graph view by default.

You choose the transactions and locations to include in the Network Latency report. By default, transactions displayed in a Business Process Distribution report previously run in the same session will be selected for the Network Latency report (for details on the Business Process Distribution report, see "Business Process Distribution Report" on page 155.

To display data for a different group of transactions, click the **Manual Transaction Selection** link, select the transaction(s) for which you want to view data, and click the first arrow. To select all the transactions listed, click the second arrow. Click **OK** to close the dialog box and save your settings.

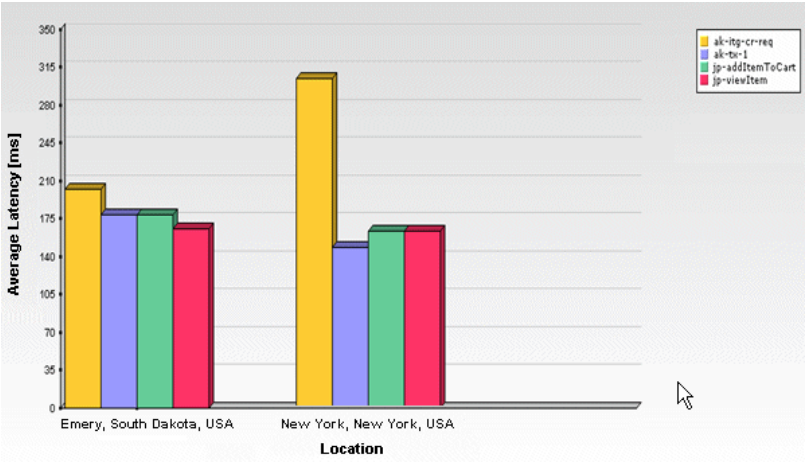
To select the locations you want to view in the report, click the **Location Selection** link. In the Select Locations dialog box, select the location(s) for which you want to view data, and click the first arrow. To select all the locations listed, click the second arrow. Click **OK** to close the dialog box and save your settings. Only locations that have been configured in Monitor Administration and included in data received from Real User Monitor will be displayed. For details on configuring locations for end-user groups, see "Configuring End-User Groups" in *End User Management Data Collector Configuration*.

Viewing the Network Latency Report as a Graph

The x-axis displays transactions by location. The bars indicate the selected transactions, according to the color coding in the legend, grouped by the selected locations.

The y-axis displays average latency in milliseconds.

For example, the graph below shows the network latency report for four selected transactions in two locations. The monitored transaction called ak-itg-cr-req shows a network latency of 205 milliseconds in Emery, South Dakota and 310 milliseconds in New York.



Hold the mouse over a bar in the graph to display the average latency for that transaction in the specific location.

Viewing the Network Latency Report as a Table

The table displays a column for each transaction and a row for each location. The average latency for each transaction in each location is displayed. In addition, the average latency of all the transactions at a location, the average latency of each transaction across all locations, and an overall average latency of all transactions across all locations are displayed.

HTTP Error Codes

The following tables show the various categories of HTTP errors and the error codes they include that are predefined in Mercury Business Availability Center. For information on configuring HTTP error codes, see "Defining HTTP Global Error Events" in *End User Management Data Collector Configuration*.

The following codes indicate bad user requests:

Code	Description
400	Bad Request
405	Method Not Allowed
406	Not Acceptable
408	Request Timeout
411	Length Required
414	Request - URI Too Large
416	Requested range not satisfiable
417	Expectation Failed

The following codes indicate refused requests:

Code	Description
401	Unauthorized
402	Payment Required
403	Forbidden
407	Proxy Authentication Required
409	Conflict
410	Gone
412	Precondition Failed
413	Request Entity Too Large
415	Unsupported Media Type

The following code indicates requests not found:

Code	Description
404	Not Found

The following codes indicate server errors:

Code	Description
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Timeout
505	HTTP Version not supported

6

Alert Reports

Mercury Business Availability Center sends alerts according to the alert trigger criteria you specify when creating alert schemes. Every alert that Mercury Business Availability Center sends is logged to the database. You view information about the alerts that have been sent in Alert reports.

This chapter describes:	On page:
About Alert Reports	166
Alert Log	167
Alert Count over Time Report	169

About Alert Reports

Alert reports enable you to track alerts that are triggered by Mercury Business Availability Center during a Business Process Monitor or Client Monitor profile run, and to view information about alerts that you integrate into Mercury Business Availability Center through SiteScope EMS monitors.

The following Alert reports are available:

Category	Description	For Details, See...
Alert Log	Tracks all alert details for alerts sent by Mercury Business Availability Center for Business Process Monitor or Client Monitor profiles.	page 167
Alert Count Over Time	Displays, for the selected profile, the number of alerts that occurred over a specified time range, organized by severity, source, or type.	page 169

For details on working with reports (choosing the time range, selecting the profile, saving and sharing reports, and so forth), see "Working in Reports" in *Working with Applications*.

For details on creating Mercury Business Availability Center alerts, see "Creating Alert Schemes" in *Platform Administration*.

Note: If you have Real User Monitor installed and integrated with Mercury Business Availability Center, Mercury Business Availability Center displays the Real User Monitor Alert Log. For details on installing and working with Real User Monitor, see "Introducing Real User Monitor Administration" in *Real User Monitor Administration*. For details on configuring Real User Monitor in Mercury Business Availability Center, see "Configuring the Real User Monitor" in *End User Management Data Collector Configuration*.

Alert Log

The Alert Log tracks all alert details for alerts sent by Mercury Business Availability Center during the specified time range, for the selected Business Process Monitor or Client Monitor profile.

Severity	Time	Alert Name	Alert Source	Alert Action	Alert Type	Alert Details
	11/01/01 06:12:23 PM	search_book Poor	Application Management	No Recipients; Send Snmp Trap to 207.232.12.205	Transactional event	Profile Name: sanit...Details
	11/01/01 06:11:00 PM	Transaction response time relative to threshold for specified percentage of transactions is as specified	Application Management	Notify Manager	Transactional event	Profile Name: sanit...Details
	11/01/01 06:10:25 PM	Transactions fail+pos	Application Management	Logged Only - No recipients	Transactional event	Profile Name: sanit...Details
	11/01/01 06:09:00 PM	Availability is less than 100 percent	Application Management	No Recipients; Send Snmp Trap to 207.232.12.205	Transactional event	Profile Name: sanit...Details

Working With the Alert Log

The Alert Log enables you to track all alerts logged by Mercury Business Availability Center for Business Process Monitor, Client Monitor profiles, or Real User Monitor, regardless of the action specified for the alert in the alert scheme. For example, the Alert Log lists alerts that are not sent to specified recipients and alerts that trigger an executable file.

In addition, you can view alerts sent via your organization's enterprise management systems (if configured in EMS profiles).

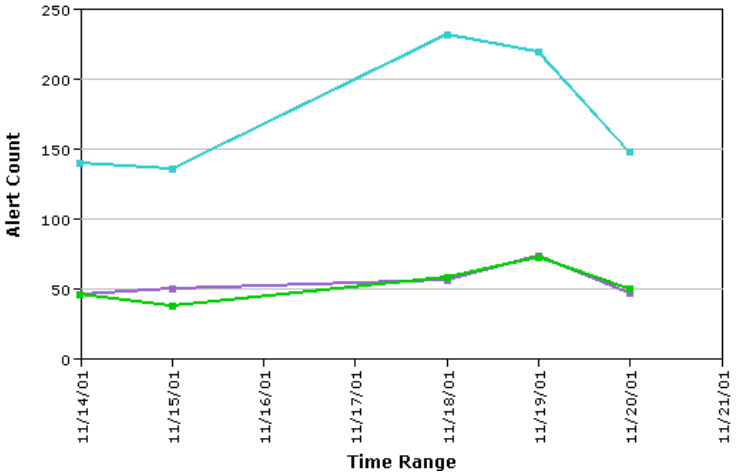
The Alert Log displays up to 20 entries per page. If there are more than 20 entries, use the navigation links at the top or bottom of the screen to move through the Alert Log.

The Alert Log page lists all alerts logged by Mercury Business Availability Center, and displays the following information:

- **Severity** – displays an icon that represents the alert severity label you selected for the alert in the alert scheme
- **Time –** displays the date and time that Mercury Business Availability Center logged the alert
- **Alert Name –** displays the alert name that you specified in your alert scheme
- **Alert Action** – displays alert notification information, for example, the recipients who received the alert. You specify alert recipients in your alert schemes.
- **Alert Type –** displays the type of alert
- **Alert Details** – displays the beginning of the alert notice. Click the **Details** link to open the Alert Details window. The Alert Details window displays the information that is available for the alert, including the actual conditions at the time of the alert.

Alert Count over Time Report

The Alert Count over Time report displays the number of alerts that occurred over the specified time range, organized by severity, source, or type, for a selected profile.



Working With the Alert Count over Time Report

The Alert Count over Time report displays a quick overview of the frequency of alerts that Mercury Business Availability Center has sent. In addition, by using the view filter, you can group the data by source, severity label, or alert type. For example, you can determine how often critical alerts are being sent.

- To view a greater level of detail, drill down in the report.
- To increase the time resolution for the selected source, severity label, or alert type, click any time point in the graph.
- To focus on a source, severity label, or alert type, click any drill down link to the right of the report.
- To view a tooltip containing details about the number of alerts corresponding to that point in time, place the pointer over any small square in the graph.

- To display the alert count, select **Source**, **Severity**, or **Type** from the report view list and click **Generate**.
- To generate a modified report, make changes to the profile, view, or active filters selections, and click **Generate**.

7

Network Reports and Tools

You use network reports and tools to analyze the quality of network performance.

This chapter describes:	On page:
About Network Reports and Tools	172
WebTrace by Location Report	173
Network Analysis Report	177
Page Component Breakdown Tool	178
Instant Diagnostics	184

About Network Reports and Tools

Network reports and tools enable you to gain an in-depth view of the network health of your monitored environment.

For details on working with reports (choosing the time range, selecting the profile, saving and sharing reports, and so forth), see "Working in Reports" in *Working with Applications*.

The following reports and tools are available:

Category	Description	For Details, See...
WebTrace by Location	Displays reports that enable you to analyze network performance by providing traceroute information to specified destinations.	page 173
Network Analysis	Displays reports that enable you to analyze network performance between configured host locations and specified destinations.	page 177
Page Component Breakdown	Displays an on-demand breakdown of download time, by component, for each element of a specified Web page.	page 178
Instant Diagnostics	(For Mercury Managed Services customers only) Provides tools that enable gathering of additional information on network and server performance.	page 184

WebTrace by Location Report

The WebTrace by Location report enables you to analyze network performance by providing typical traceroute information from configured host locations to specified destinations. You drill down to view routing details and hop time over time.

You can correlate WebTrace data with transaction performance problems, such as slow transaction response times and failed transactions, to analyze whether the problems are network related.

You can view the WebTrace by Location report for both Business Process Monitor and Client Monitor profiles. Note that Business Process Monitor uses WebTrace data and Client Monitor uses traceroute data. For details on the difference between WebTrace and traceroute, see "Differences Between WebTrace and Traceroute" on page 173. For details on configuring WebTrace and traceroute monitors, see "Defining Traceroute Monitors and Editing WebTrace Monitors" in *End User Management Data Collector Configuration.*

This section includes the following topics:

- "Differences Between WebTrace and Traceroute" on page 173
- "Understanding the WebTrace by Location Report" on page 174
- "Analyzing the WebTrace by Location Report" on page 175

Differences Between WebTrace and Traceroute

WebTrace records the route through the Internet from your host machines to the destination Web server(s) specified in the Business Process profile. Unlike standard traceroute programs, WebTrace uses a unique technology that enables it to cross firewalls.

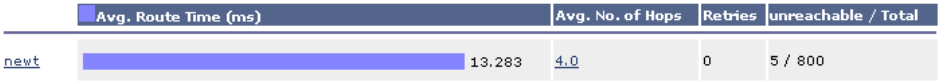
For Client Monitor profiles, Mercury Business Availability Center displays traceroute data. Traceroute records the route through the Internet from the Client Monitor machine to the destination Web server specified in the profile, using standard traceroute technology.

Note: In this chapter, the term **WebTrace** is used to represent both WebTrace (for Business Process profiles) and traceroute (for Client Monitor profiles).

Understanding the WebTrace by Location Report

For each server destination defined in the profile, the WebTrace by Location report displays a traceroute analysis, grouped by host name, for the specified time frame.

When you configure a WebTrace monitor, you select the host machines or locations to run WebTrace. Mercury Business Availability Center runs WebTrace according to the schedule set in the profile for running transaction monitors. When you generate the WebTrace by Location report, it displays an average of all the WebTrace runs that took place during the specified time period.



For each destination, the WebTrace by Location report breaks down route time from host machine to destination machine as follows:

- **Avg. Route Time** (ms) – the average time it takes for a packet of data to be sent from the host machine to the destination Web site
- **Avg. No. of Hops** – the average number of intermediate servers the data packet encounters before it reaches its destination
- **Retries** – the number of times a data packet tries, but fails, to reach its destination due to timeout, network difficulty, and so forth
- **Unreachable/Total** – the number of times the destination was unreachable out of the total number of measurements

Analyzing the WebTrace by Location Report

The WebTrace by Location report helps you identify problems related to network response time for hosts at various host locations. By correlating transaction response time and service availability information with the WebTrace by Location report data, you can determine whether slow response times or failed transactions are being caused by poor network performance from a specific host location.

For example, using the Performance Matrix report, you might determine that average transaction response times from a particular location are in the critical range, as determined by your transaction threshold settings. By analyzing WebTrace data for the same location over the same time period, you could determine whether network performance was also critical. If so, this could lead you to conclude that the Internet was slow from a particular location during that time period. Alternatively, if network performance for the location and time period seems normal, you could conclude that the problem is server-related, for example, excessive load on your Web server.

The report also displays the average number of hops from the sample, and the total number of retries and unreachables. You can cross-reference this data with transaction response time and service availability information to determine whether poor or failed application performance was caused by specific network errors or network latency for a particular location or time period.

Further Analyzing WebTrace Data

You can further analyze WebTrace data by drilling down in the WebTrace by Location report to get additional route time and hop information. Drilling down helps you determine at exactly which point along the network path bottlenecks are occurring.

To drill down for additional route time information:

1 Click a host name link to view the WebTrace Over Time report, which displays two charts:

- the host's average route time data with increased time granularity. Place your cursor over a colored bar to see a tooltip with average route time and number of errors.
- the number of errors that occurred over the defined time range. Place your cursor over a point on the bar to see a tooltip with the number of errors.

2 Click any bar or point in either of the WebTrace over Time charts to view the WebTrace Measurements chart, which displays the WebTrace data with increased time granularity. Place your cursor over a colored bar to see a tooltip with route time statistics.

3 Click a specific time measurement in the WebTrace Measurements chart to open the Routing Details window, which displays a detailed breakdown of the specific traceroute run. Mercury Business Availability Center displays the following routing details:

- hop number – the order in which the hops occur
- hop name – the name of the intermediate server
- hop IP – the IP address of the intermediate server
- errors – the number of errors associated with a specific hop IP
- hop time – the time, in milliseconds, from the source to the specific hop

Click the Next or Previous links to move to the next or previous set of time measurements (if available).

To drill down for additional hop information:

Click a link in the Avg. No. of Hops column to open the Hop Time over Time report in a new window. The report displays average hop time, for each hop, over the selected time frame. You can view this report in either graph or table format.

Network Analysis Report

The Network Analysis report provides an in-depth picture of network performance for a Business Process profile, if you defined a WebTrace monitor for the profile. The report enables you to understand, for the selected profile and defined time frame:

- average route time over time between configured host locations and specified destinations
- errors over time
- hop time over time between configured host locations and specified destinations

Generating the Network Analysis Report

When you generate the Network Analysis report initially, the WebTrace by Location report is displayed. To analyze data for a specific location, click the location name link. The sub-reports are generated.

The Network Analysis report consists of the following components:

Report Category	Report Name	Description
Main report	WebTrace by Location	Displays a traceroute analysis from configured locations to specified destinations.
Sub-reports	WebTrace over Time	Displays average route time across the network over the selected time frame.
	Errors over Time	Displays the number of errors that occurred over the selected time frame.
	Hop Time over Time	Displays average hop time over the selected time frame.

Page Component Breakdown Tool

The Page Component Breakdown tool provides an on-demand component breakdown of any Web page. You use the Page Component Breakdown report to analyze network, server, and client health in real time. You correlate this data with transaction performance problems, such as slow transaction response times and failed transactions, to analyze whether they are network-, server-, or client-related.

When generating a Page Component Breakdown report, you select the location from which you want the HTTP requests to originate. By default, the Page Component Breakdown report can be generated from all configured Business Process Monitor locations running Business Process Monitor version 4.5.2 or later.

Note: Page Component Breakdown does not function for streaming objects, such as Java applets, sounds, and movies. This is because the engine that runs Page Component Breakdown uses technology that handles only those components that can be parsed directly from the HTML code (for example, images).

Note to Mercury Managed Services customers: The available locations for Page Component Breakdown depend on the locations defined in your Mercury Managed Services package.

This section includes the following topics:

- "Generating the Page Component Breakdown Report" on page 179
- "Working With the Page Component Breakdown Report" on page 180
- "Understanding the Page Component Breakdown Report" on page 180
- "Analyzing the Page Component Breakdown Report" on page 182
- "Viewing Page Component Breakdown Data in other Contexts" on page 183

Generating the Page Component Breakdown Report

You generate a Page Component Breakdown report by specifying a URL and a location from which to run the breakdown.

To generate the page component breakdown report:

1 In the **URL** box, enter an address for the target Web page. This can be:

- the name of a server on the local network
- a Web address
- the full URL for a page, for example:

```
http://www.mercury.com/
```

In general, you enter the URLs of specific pages on your Web site, for example, those that are included in the transactions defined in your Business Process Monitor profiles.

2 From the **Location** list, select the location from which you want the report to be generated. Each listed location represents a specific Business Process Monitor instance, displayed using the syntax: location_name (host_name).

Note: The system administrator can hide the host name values in the list in the Infrastructure Settings Manager.

Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **End User/System Availability Management** and locate the **Display Host Name in Page Component Breakdown Report** entry in the **End User/System Availability Management - Display** table. Change the setting to **false**.

---

3 If you are accessing a secure site, click **Authentication**, and type the user name and password required to access the site.

4 Click **Generate** to generate the report.

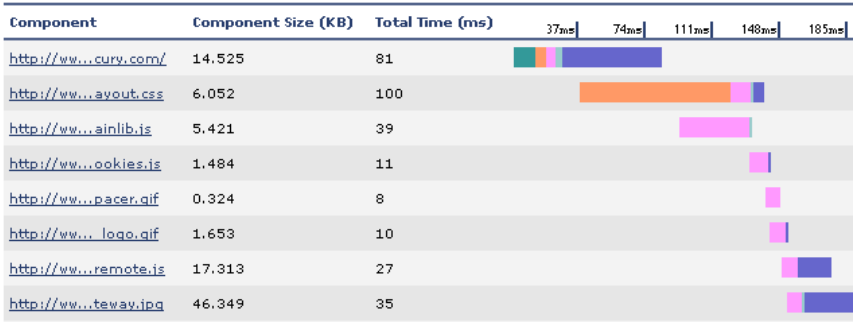
Working With the Page Component Breakdown Report

- Place the pointer over any link in the Component column to view a tooltip displaying the component's URL. If the component is an image, the image is also displayed. Click the link to view or open the component.
- Place the pointer over a color-coded portion of any bar in the graph view to get statistics relevant to that portion of the bar.
- Click the **View as Table** link to view the data in table format. The table displays the size of each component, its total download time (in milliseconds), a breakdown of the total download time, and error information if relevant.

Understanding the Page Component Breakdown Report

The Page Component Breakdown report enables you to assess whether transaction response times and service availability are being affected by page content. The report displays the size (in KB) of each page element, the total time it takes for each component of a specified Web page to download, and the offset time for each component. The offset time for a specific component is the time that passes from the start time of the first component on the page until the start time of the specific component. In the graph view, holding the cursor over the white space to the left of a component's colored bar will show a tooltip with the offset time for that component. In the table view, the time is specified in a separate column in the table.

The report further breaks down each component by retry time, DNS resolution time, connection time, network time to first buffer, server time to first buffer, and download time. If your site uses SSL authentication, SSL handshaking time appears in the chart after connection time.



For information on the breakdown categories used in the Page Component Breakdown report, see "Understanding the Transaction Breakdown Reports" on page 52.

Note:

Gaps in time between elements, in the Breakdown section of the report, represent processing time—client-side delays caused by browser think time, CPU think time, HTML page processing time, time needed to open sockets or threads, and so forth.

In certain circumstances, for example, when the Business Process Monitor is using a proxy server, the transaction breakdown mechanism cannot differentiate between server time to first buffer and network time to first buffer. In these cases, the report displays the time between initial HTTP request and receipt of first buffer as Time to First Buffer.

Analyzing the Page Component Breakdown Report

The Page Component Breakdown report helps you identify problematic elements of a Web page, for example, images that download slowly, or broken links. Furthermore, by breaking down an element's download time, the report can help you identify where problems are occurring along the network (for example, during DNS Resolution, or during Network Time to First Buffer).

By correlating transaction response time and service availability information with Page Component Breakdown report data, you can determine whether slow response times or failed transactions are being caused by specific problematic elements on a Web page that is accessed during the transaction, or by network errors during Web page download.

For example, using the Response Time over Time report, you might determine that the average response times for a particular transaction are suddenly significantly higher than in the past. By running a page component breakdown on the same Web page that is accessed in the transaction, you may discover that a particular image, recently added to the Web page, is downloading very slowly due to its size. This would account for the sudden increase in transaction response times.

The Page Component Breakdown report's color-coded bars enable you to differentiate between retry time, DNS resolution time, connection time, SSL handshaking time (if relevant), network time to first buffer, server time to first buffer, and download time. By analyzing the structure of the page download—for example, how many elements download simultaneously as compared to sequentially—you can pinpoint download bottlenecks.

You can also cross-reference this data with transaction response time and service availability information to determine whether poor or failed application performance is being caused by specific network errors or network latency. For example, if DNS lookup time is slow or returning errors, there may be a problem with your DNS server, which could explain why transactions are failing.

Viewing Page Component Breakdown Data in other Contexts

In addition to generating the Page Component Breakdown report from the Network and Tools tab in the End User Management application, you can generate page component breakdown data in the following contexts:

- if page component breakdown data collection is enabled for a specific transaction monitor, Mercury Business Availability Center collects and saves page component breakdown data for a sampling of transaction instances over a given time period. You can view this data via the Breakdown Summary report. For details on enabling page component breakdown data collection, see "Enable/Disable Page Component Breakdown (Business Process Profiles Only)" in *End User Management Data Collector Configuration*. For details on viewing page component breakdown data in the Breakdown Summary report, see "Breakdown Summary Report" on page 59.
- a Page Component Breakdown report can be generated on demand from the Business Process Monitor page within the Business Process Monitor Admin. For details, see "Running an On-Demand Page Component Breakdown" in *Business Process Monitor Administration*.
- if page component breakdown data collection is enabled for a specific transaction monitor, a Page Component Breakdown report is generated when invoking a task from the transaction monitor Task page within the Business Process Monitor Admin. For details, see "Running Script Tasks" in *Business Process Monitor Administration*.

Instant Diagnostics

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

You use Instant Diagnostics tools to obtain additional information on network and server performance.

To access the tools, you select the location from which you want the tools to run. The available locations depend on the locations defined in your Mercury Managed Services package.

There are two categories of tools:

➤ "Application Diagnostics Tools" on page 184

➤ "Advanced Tools" on page 185

Application Diagnostics Tools

The following application diagnostics tools are available:

DNS Lookup – Checks whether the specified DNS server can resolve the specified domain name to an IP address.

Check FTP Server – Checks whether a specified FTP file can be retrieved by sending a file retrieval request to the specified FTP server from the selected location. You also provide FTP server connection parameters.

Ping – Checks whether the specified domain or IP address is available by pinging it from the selected location.

WebTrace – Performs a WebTrace from the selected location to the specified domain or IP address. For details on WebTrace, see

Traceroute – Performs a standard traceroute from the selected location to the specified domain or IP address.

Advanced Tools

The following advanced diagnostic tools are available. Note that they may require additional setup:

LDAP Authentication – Performs a user authentication on an LDAP server. You provide LDAP server connection parameters and a LDAP query.

Check News Server – Checks whether a News Server is operational by sending informational requests to the server. You provide the server name and other optional parameters.

8

User Reports

User reports is a feature common to the Service Level Management, End User Management, and System Availability Management applications. You configure and view user reports from the User Reports tab.

For complete details on creating, viewing, and administering user reports, see “Configuring and Viewing User Reports” in *Working with Applications*.

Index

A

Active Filters
    in Real User Monitor 79
active filters
    Real User Monitor 79
advanced diagnostics tools 185
aggregation
    Real User Monitor data 84
Alert Count Over Time report 169
    working with 169
Alert Log 167
alerts
    Alert Count Over Time 169
    Alert Log 167
application diagnostics tools 184
Availability Over Time report 38
    working with 39
Availability tab 98, 116

B

Breakdown Over Time report 57
    correlating data with other Mercury Business Availability Center reports 61
    drilling down to Diagnostics application 57
Breakdown Summary report 59
    drilling down to Diagnostics application 59
    further data analysis 64
    working with data 60
Business Process Distribution report 74, 155
    analyzing 157
Business Process reports
    Availability Over Time 38
    Breakdown Over Time 57
    Breakdown Summary 59
    Desktop Analysis 67
    Error Summary 43
    Failed Transactions 46
    Location Analysis 51
    Min./Max. Response Time 65
    Response Time Over Time 40
    Transaction Analysis 42
    transaction breakdown reports, understanding 52

C

client time, transaction breakdown 56
connection time
    transaction breakdown 55
customizing reports, Real User Monitor 77

D

data aggregation 2
    Real User Monitor 84
Desktop Analysis report 67
Desktop Performance report
    choosing criteria 67
    further data analysis 68
    understanding 68
Diagnostics
    drilling down from Breakdown Over Time report 57
    drilling down from Breakdown Summary report 59
DNS resolution
    transaction breakdown 55
download time
    transaction breakdown 56

drilling down to Mercury Diagnostics reports
Real User Monitor 78
drilling down within reports
Real User Monitor 77

E

enabling summary rows
Real User Monitor 76
End User Management reports 3
introduction 1
overview 1
Status Snapshot 5
End User Over Time report 131
End User Summary report 129
error and TBD raw data links
using 61
Error Summary report 43
modifying tables 49
outlier transactions 45
working with 45
Event Count Over Time 74
Event Count Over Time report 150
Event Log 154
Event Summary 74
Event Summary report 152

F

Failed Transactions report 46
filter 47
snapshot on error 48

G

General tab 95, 114
Global Statistics report 86
graphs
Transaction Response Time Over Time 157
Transaction Runs Over Time 156

H

HTTP denial codes 162
HTTP error codes 162

I

Infrastructure Settings Manager
changing Triage report settings 28, 29
editing Status Snapshot settings 6
hiding host name values 179

L

links
broken 93
Location Analysis report 51
generating 51
generating sub-reports 51

M

maximum number of rows displayed
modifying 76
maximum number of rows displayed in a table, Real User Monitor 76
maximum number of rows returned
modifying for 76
maximum number of rows returned for Session Analyzer report and Event Log 76
Mercury Diagnostics Server Requests View 113
Page Summary report 113
Min./Max. Response Time report 65
analyzing 65
further data analysis 66
most active end users 88
most popular pages 86
Multi-Profile Summary report
alert summary 13
limitations 14
location performance 12
profile performance 11
working with 11

N

Net Performance tab 119
Network Latency report 74, 160

network reports and tools
advanced diagnostics tools 185
application diagnostics tools 184
Instant Diagnostics 184
Network Analysis 177
Page Component Breakdown 178
Page Component Breakdown report, authenticated logon 179
Routing Details 176
WebTrace by Location 173
WebTrace by Location, hops 174
WebTrace by Location, retries 174
WebTrace by Location, route time 174
WebTrace by Location, unreachables 174
WebTrace Measurements 176
WebTrace Over Time 176
network time to first buffer
transaction breakdown 55

P

Page Broken Down by End Users report 104
Page Broken Down by End-Users report 104
Page Component Breakdown data
viewing in other contexts 183
Page Component Breakdown report
analyzing 182
authenticated logon 179
generating 179
understanding 180
working with 180
Page Over Time report 105
Page Summary report 73, 94
Viewing Mercury Diagnostics data 113
pages with slowest server time 90, 92
Performance Matrix report 18
analyzing 22
reducing time frames 21
working with 19
Performance tab 100

R

Real User Monitor
active filters 79
Business Process Distribution report 155
customizing reports 77
data aggregation 84
drilling down to Mercury Diagnostics reports 78
drilling down within reports 77
enabling summary rows 76
End User Over Time report 131
End User Summary report 129
Event Count Over Time report 150
Event Summary report 152
Global Statistics report 86
maximum number of rows returned for Session Analyzer report and Event Log 76
Network Latency report 160
Page Summary report 94
Server Summary report 133
Session Analyzer report 139
Transaction Summary report 113
using Active Filters 79
Real User Monitor Active Filters
using 79
Real User Monitor reports 71
Business Process Distribution report 74
customizing 77
drilling down 77
End User Summary report 73
Event Count Over Time report 74
Event Summary report 74
global statistics 72
Network Latency report 74
overview 72
Page Summary report 73
Performance tab 100
Server Performance tab 102, 121
Server Summary report 73
Session Analyzer report 73
Total Performance tab 118
Transaction Summary report 73
working with 75
Real User Monitor, maximum number of rows displayed in a table 76

replaying a session 159
reports
access and permissions 2
Alert Count Over Time 169
Alert Log 167
Alert, *See* alert reports
Availability Over Time 38
Breakdown Over Time 57
Breakdown Summary 59
Business Process, *See* Business Process reports
Desktop Analysis 67
End User Management 3
End User Management Status Snapshot 5
Error Summary 43
Failed Transactions 46
Instant Diagnostics 184
Location Analysis 51
Min./Max. Response Time 65
Network Analysis 177
network, *See* network reports and tools
Page Component Breakdown 178
Page Component Breakdown, authenticated logon 179
Performance Matrix 18
Real User Monitor 71
Response Time by Percentile 69
Response Time Over Time 40
Routing Details 176
Single Profile Summary 16
summary, *See* summary reports
Transaction Analysis 42
WebTrace by Location 173
WebTrace by Location, hops 174
WebTrace by Location, retries 174
WebTrace by Location, route time 174
WebTrace by Location, unreachables 174
WebTrace Measurements 176
WebTrace Over Time 176
Response Time by Percentile report 69
Response Time Over Time report 40
working with 41
retry time
transaction breakdown 55

S

Server Over Time report 135
Server Performance tab 102, 121
Server Summary report 133
server time to first buffer
transaction breakdown 56
Servers by Page Summary report 111, 137
Session Analyzer report 139
Session Detail report 141, 155
Session Details report
page 159
session replay 159
sessions
replaying 159
Sessions page 158
Single Profile Summary report
Alert Summary 14, 16
Overall Quality of Service 14, 16
Performance of Locations 14, 17
Performance of Transactions 14, 17
working with 15
slowest end users 89
snapshot on error 48
SSL
handshaking, transaction breakdown 55
Status Snapshot
calculated by End User Management 6
End User Management reports 5
overview 5
working with 7
summary reports 9
Alert Summary 10
Location Performance 10
Multi-Profile Summary 10
Performance Matrix 18
Profile Performance 10
Single Profile Summary 14

T

time to first buffer
transaction breakdown 57

Total Performance tab 118
Transaction Analysis report 42
    generating 42
    generating sub-reports 42
transaction breakdown
    categories 54
    client time 56
    connection time 55
    DNS resolution 55
    download time 56
    download time, understanding 57
    network time to first buffer 55
    retry time 55
    server time to first buffer 56
    SSL handshaking 55
    time to first buffer 57
    understanding 52
Transaction Breakdown report
    understanding breakdown 53
Transaction Broken Down by End Users report 122
Transaction Over Time report 123
Transaction Response Time Over Time graph 157
Transaction Runs Over Time graph 156
Transaction Summary report 73, 113
Triage report 23, 34
    changing maximum number of transactions and locations 28
    incorporating in custom report 30, 37
    working with 24, 34

U

user reports 187

W

WebTrace by Location report
    analyzing 175
    differences between WebTrace and traceroute 173
    further data analysis 175
    hops 174
    retries 174
    route time 174
    unreachables 174