

HP Real User Monitor

Software Version: 9.25

Real User Monitor Administration Guide

Document Release Date: June 2015
Software Release Date: January 2015



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2005-2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

iPod is a trademark of Apple Computer, Inc.

Java is a registered trademark of Oracle and/or its affiliates.

Microsoft®, Windows®, Windows NT®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=>.

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

Support

Visit the HP Software Support web site at: <https://softwaresupport.hp.com>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software Support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests

- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to <https://softwaresupport.hp.com> and click **Register**.

To find more information about access levels, go to: <https://softwaresupport.hp.com/web/softwaresupport/access-levels>

HP Software Solutions & Integrations and Best Practices

Visit HP Software Solutions Now at <https://h20230.www2.hp.com/sc/solutions/index.jsp> to explore how the products in the HP Software catalog work together, exchange information, and solve business needs.

Visit the Cross Portfolio Best Practices Library at <https://hpln.hp.com/group/best-practices-hpsw> to access a wide variety of best practice documents and materials.

Contents

- Real User Monitor Administration Overview 10
- Part 1: RUM Introduction and Compatibility 11
 - Chapter 1: Introducing RUM Administration 12
 - Overview of RUM 12
 - How RUM Works 12
 - Ports Used by RUM 14
 - Overview of RUM Performance Measurements 15
 - Introduction to Performance Measurements 15
 - TCP Request-Response Measurements 16
 - HTTP Measurements 17
 - Page Performance Measurements 17
 - Component Measurements 18
 - Page Measurements 19
 - Transaction Measurements 20
 - End User Measurements 21
 - Installing and Administering RUM 23
 - Chapter 2: RUM Compatibility Matrixes 24
 - RUM–BSM Compatibility Matrix 24
 - RUM Probe–RUM Engine Compatibility 25

- Part 2: Data Collection Methods 26
- Chapter 3: RUM Data Collection Methods 27
- Chapter 4: Data Collection Using a Network Tap or Switch Configuration 29
- Chapter 5: Sniffing Using the RUM Server Collector 30
 - Configuring the RUM Server Collector 31
 - Configuring the RUM Sniffer Probe 32
 - Administering the RUM Server Collector Service 33
 - RUM Server Collector Log File 34
- Chapter 6: RUM Client Monitor Probe 35
 - Using the RUM Client Monitor Solution to Monitor Web Applications 36
 - Using the RUM Mobile Solution to Monitor Mobile Applications 39
- Part 3: Configuring and Administering Real User Monitor 42

Chapter 7: Administering the RUM Engine	43
Administering RUM Monitor	43
RUM Logs	44
Chapter 8: Using the RUM Web Console	47
Accessing the RUM Engine Web Console	47
Logging In	48
Logging Out	48
Changing Login Parameters	49
Changing the Language of the RUM Web Console User Interface	50
Changing Timeout Parameters	51
Monitoring the Health of RUM Components	51
System Health	52
Configuration Retrieval From BSM Server	53
Database	54
RUM Sniffer Probe	56
RUM Client Monitor Probe	78
RUM Engine	84
Samples to BSM Server	107
ATT	108
Data Access Layer	109
Partition Manager	110
Topology Engine	111
Missing Mirrored Data	118
Capture Log Files	118
RUM Configuration and Settings	118
BSM Connection Settings	119
Probe Management	122
Action Buttons	123
Probe Configuration Dialog Box	124
Probe Traffic Discovery	127
Common Elements	127
Summary View Tab	128
Domain View/Server View Tabs	129
SSL Keystore Management	130
Interface Configurations	134
Server Filter Settings	136
Probe Traffic Capture	137
Session ID Detection	138
Configuring Applications in End User Management Administration Using Traffic Discovery and Session ID Detection	139

Session ID Detection Page	139
Session ID Detection Report	140
TransactionVision Connection Settings	143
Advanced Settings	145
Data Flow Probe Connection Settings	145
System Info	147
RUM Diagnostics Tools	147
Monitoring Configuration Information	148
Applications	148
End Users	149
Events	149
Pages	150
Probes	151
Transactions	151
Engine Settings	152
Transaction Snapshot Mode	153
JMX Console	154
IP Translator	154
Time Converter	154
Page Name Cache	154
Mobile Application Instrumentation	156
Signing an APK using Java's jarsigner.exe Tool	159
Chapter 9: Using the JMX Console to Configure the RUM Engine	161
Using the RUM JMX Console	161
Accessing the JMX Console	161
Setting URL Correlation Parameters	162
Configuring RUM Aggregation	162
Configuring the Samples Rate	164
Configuring the Amount of Unsent Sample Data to Store in RUM	165
Configuring the Classification Type	165
URL Correlation Parameters	167
Setting URL Correlation Parameters Via the JMX Console	168
Correlating Session ID Parameters	169
Chapter 10: RUM Transaction Flow Monitoring	171
RUM Transaction Flow Monitoring Overview	171
RUM Transaction Flow Monitoring User Interface	172
Enterprise Components Pane	172
Components Properties/Graph Overview Pane	173
Topology View Pane	174

Topology Map - Statistical Graph	174
Topology Map - Pattern Tree	177
Select Server Dialog Box	177
Action Description Statistics Dialog Box	178
Add Transaction Pattern Element Dialog Box	178
Chapter 11: RUM Engine File Configuration	179
Configuring Meaningful Page Names	179
About Discovered Page Names	179
Formatting Tags	180
URL Decoder	181
Rename	181
Substring	182
ExtractStrToStr	182
ExtractIndexToStr	183
ExtractStrToCount	184
Insert	185
ChangeCase	186
Remove	187
RemoveNonAlpha	187
Replace	187
Alias	188
RegExExtract	188
RegExMatch	189
Rule Tags	189
Sample XML File	192
Validating Meaningful Name XML Files	198
Adding and Deleting Meaningful Name XML Files	199
Changing Meaningful Name XML Files	199
Viewing Discovered Page Statistics	200
Unifying Frames	201
Configuring User Name Translation	203
Chapter 12: Configuring the RUM Sniffer Probe	205
Changing the Protocol for Accessing the RUM Probe	205
Configuring the RUM Probe for I18N	205
Changing the Header in Which to Locate Client IP Addresses	206
Creating Default Configuration and Properties Files for a Specific Probe	206
Configuring the RUM Probe to Support Multiprotocol Label Switching (MPLS)	207
Chapter 13: Administering the MySQL Database	208
Overview of the MySQL Database	208

Creating and Connecting to the MySQL Database	208
Starting and Stopping the MySQL Database	209
Maintaining the MySQL Database	209
Chapter 14: Hardening RUM	211
Hardening the RUM Sniffer Probe	211
Changing the Probe's User and Password	211
Limiting Access to the Probe	212
Limiting the SSH Version	212
Securing the HTTP Connection to the Probe	213
Securing Connections to the RUM Engine	215
Using Authentication	216
Using HTTPS	216
Chapter 15: Deploying RUM in a SiteMinder Environment	218
Overview	218
Prerequisites	219
System Flow	219
Configuring the SiteMinder Policy Server	220
Create an Agent	220
Create the Agent Conf Object	221
Create the Authentication Scheme	221
Configure the Domain	222
Installing and Configuring the SiteMinder Web Agent	224
Configuring the Web Server	226
Configuring IIS to Work with RUM	226
Configuring IIS to Work with the SiteMinder Web Agent	230
Configuring the RUM Engine	232
Changing the Configuration of the TCP Port	233
Testing and Troubleshooting	233
RUM Engine	233
SiteMinder Web Agent	234
Mirror Servlet	235
Chapter 16: RUM Data Export	237
Enable Data Export	237
How Data is Exported	237
Data Export XML File	238
Valid Channel Types and Fields	242
Page	242
Transaction	246
Session	248

Action	251
Part 4: Supporting Specific Protocols	255
Chapter 17: Parsing Supported Protocols	256
Chapter 18: Customizing Error Codes for SAPGUI	258
Chapter 19: Monitoring Citrix with RUM	260
Overview of Citrix Monitoring with RUM	260
Overview of the RUM VDI Agent	262
Configurations for Working with the RUM VDI Agent for HTTP Traffic	263
Advanced Configuration for HTTP Traffic	265
Using the RUM VDI Agent with Terminal Services for HTTP Traffic	267
Chapter 19: Supporting ISO8583 Based Protocols	267
Send Documentation Feedback	269

Real User Monitor Administration Overview

This guide provides detailed instructions on how to configure and administer the HP Real User Monitor (RUM) data collector.

For details on installing and upgrading RUM, see the Real User Monitor Installation and Upgrade Guide.

Note: If you are an HP Software-as-a-Service customer, you must contact an HP Software Support representative to receive connection information that enables you to work with RUM.

This guide contains the following parts:

- ["RUM Introduction and Compatibility" on page 11](#)

Introduces RUM and explains how it works.

- ["Data Collection Methods" on page 26](#)

Describes the different methods by which the RUM Probe can obtain monitored data.

- ["Configuring and Administering Real User Monitor" on page 42](#)

Explains how to configure a RUM Probe by changing the default settings, as well as how to configure and administer the RUM Engine and how to administer RUM's MySQL database. Also provides guidelines for hardening RUM, deploying RUM in a SiteMinder environment, and publishing RUM data.

- ["Supporting Specific Protocols" on page 255](#)

Explains how to configure and work with RUM for monitoring specific protocols.

Part 1: RUM Introduction and Compatibility

Chapter 1: Introducing RUM Administration

This chapter introduces HP Real User Monitor (RUM) and explains how it works.

This chapter includes the following topics:

- ["Overview of RUM" below](#)
- ["How RUM Works" below](#)
- ["Ports Used by RUM" on page 14](#)
- ["Overview of RUM Performance Measurements" on page 15](#)
- ["Installing and Administering RUM" on page 23](#)

Overview of RUM

RUM monitors both user and system initiated network traffic between client machines and servers and between servers, collecting network and server performance and availability data in real time. This enables administrators to pinpoint the cause of delays and quantify the business impact of detected performance issues related to end users. When performance and availability exceed specified thresholds, HP Business Service Management (BSM) proactively alerts application managers who, using the End User Management (EUM) reports, analyze the collected data to isolate the root cause of detected problems.

Tip: For a description of the process required to set up and use RUM to monitor applications, see "How to Set up Real User Monitors" in the BSM Application Administration Guide.

How RUM Works

RUM consists of three major components: the probe, the engine, and the MySQL database.

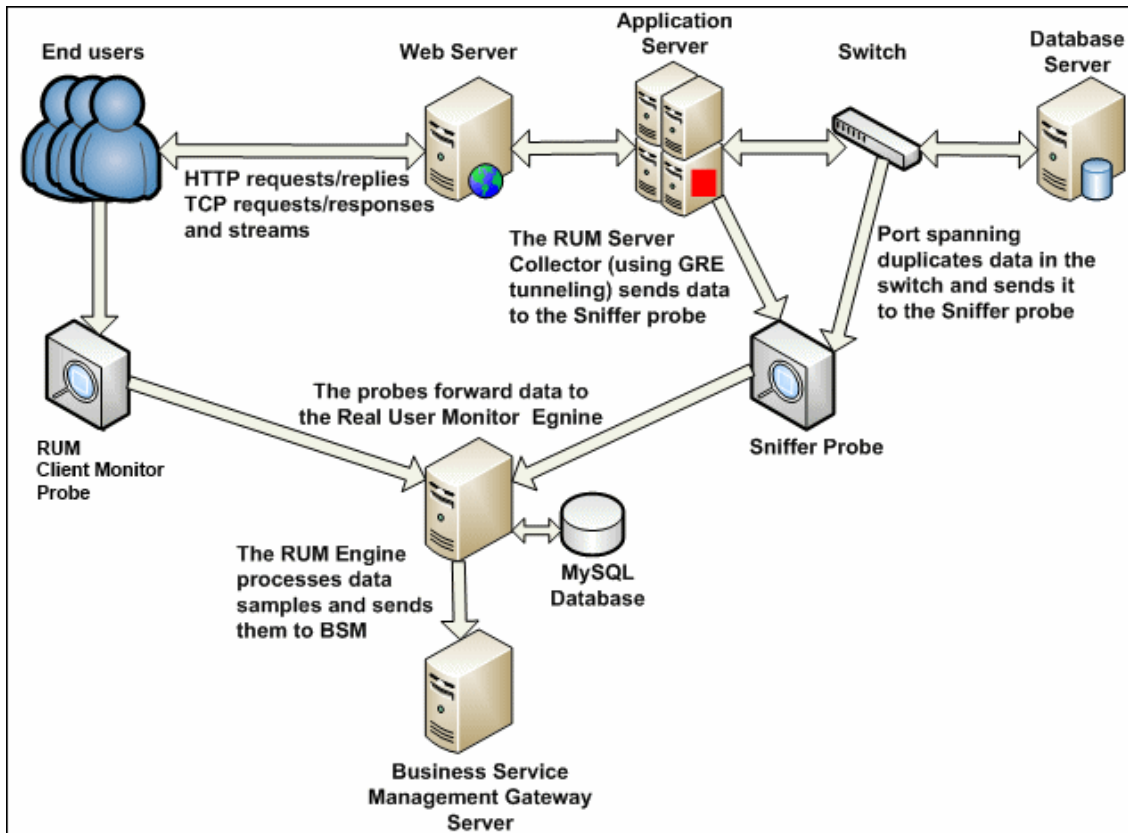
- The **probe** receives data on end-user experience and/or applications, carries out initial processing on this data, and sends it to the RUM Engine. There are two types of probe:
 - **Sniffer Probe** - a non-intrusive, passive listening device that is subject to the same traffic the server receives. The traffic can be collected in a number of different ways. For details, see ["RUM Data Collection Methods" on page 27](#).
 - **RUM Client Monitor Probe** - collects user experience data directly from the client, for monitored web or mobile applications. For details, see ["RUM Client Monitor Probe" on page 35](#).

- The **engine** receives the data collected by the probe and assembles this data according to the configuration specifications it receives from HP Business Service Management (BSM), that have been configured in End User Management Administration. The engine transmits the page, transaction, end-user, and server data samples it creates to the BSM Gateway Server. The BSM Gateway Server then distributes the data to the relevant BSM components, which create RUM alerts, reports, and Service Health views.

Note: If the RUM Engine fails or is temporarily unavailable, or is unable to copy data from the RUM Probe, the RUM Probe continues to collect data. The last two hours worth of data is saved on the RUM Probe and this data is copied by the RUM Engine when it becomes available again.

- The **MySQL database** acts as RUM's repository for data that the RUM Engine does not forward to BSM immediately, or at all. The MySQL database stores the RUM Engine's configuration settings, session clickstreams (pages and snapshots included in a session), and the open sessions summary.

The following diagram shows how RUM receives user-experience and application data and passes it on to BSM.



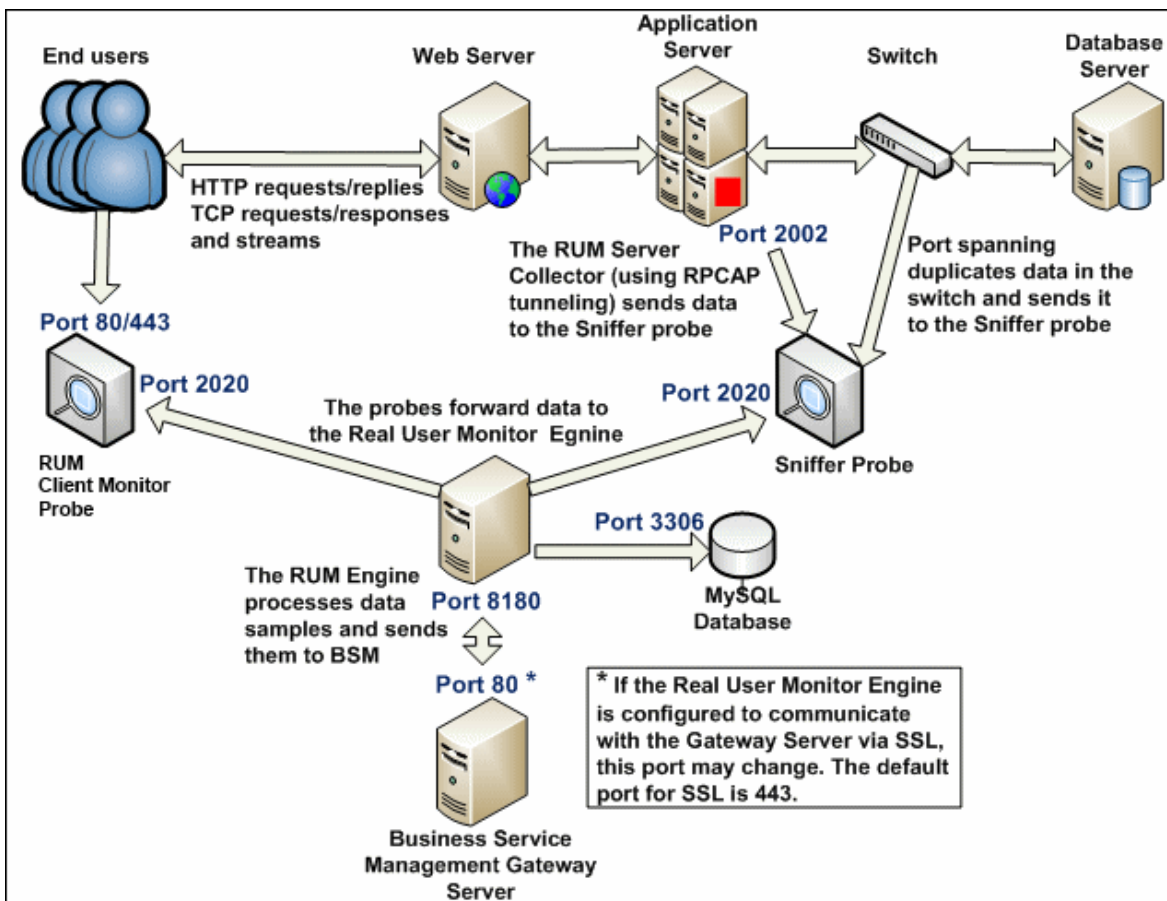
Use the EUM reports to analyze network and application performance and availability data for the servers, applications, pages, transactions, events, and end users that you configure for monitoring,

as well as general statistics that are collected and sent by the probes to the engine. When notified by an alert that a certain performance or availability threshold has been exceeded, you can examine the issue in the appropriate reports and try to pinpoint the cause of the problem and the time at which the problem occurred. For detailed information on EUM reports, see "End User Management Reports Overview" in the BSM User Guide.

In addition, RUM data is included in Service Health. For information on displaying RUM data in Service Health, see "Predefined Views for End User Management" in the BSM Application Administration Guide.

Ports Used by RUM

The following diagram shows the various ports used by RUM:



Note:

- The BSM Gateway Server initiates a connection to the RUM Engine on port 8180 for retrieving various types of data.

- The RUM Engine initiates a connection to the BSM Gateway Server on port 80 (default) for sending samples.
- The RUM Engine initiates a connection to the RUM Probe on port 2020 for https (which is the default type of communication in RUM version 7.0 and later) and http.
- The RUM Probe does not initiate a connection to any other server in the system.
- There is no direct connection from BSM to the RUM Probe.
- By default, the Snapshot Replay applet retrieves data to a user's machine via a BSM server. You can configure the applet to retrieve data directly from the RUM Engine, in which case the connection is made on port 8180. For details on configuring from where the Snapshot Replay applet retrieves data, see "Determining How the Real User Monitor Snapshot Applet Retrieves Snapshots" in the BSM User Guide.

Overview of RUM Performance Measurements

This section describes the measurements provided by RUM for the data that it monitors.

This section includes the following topics:

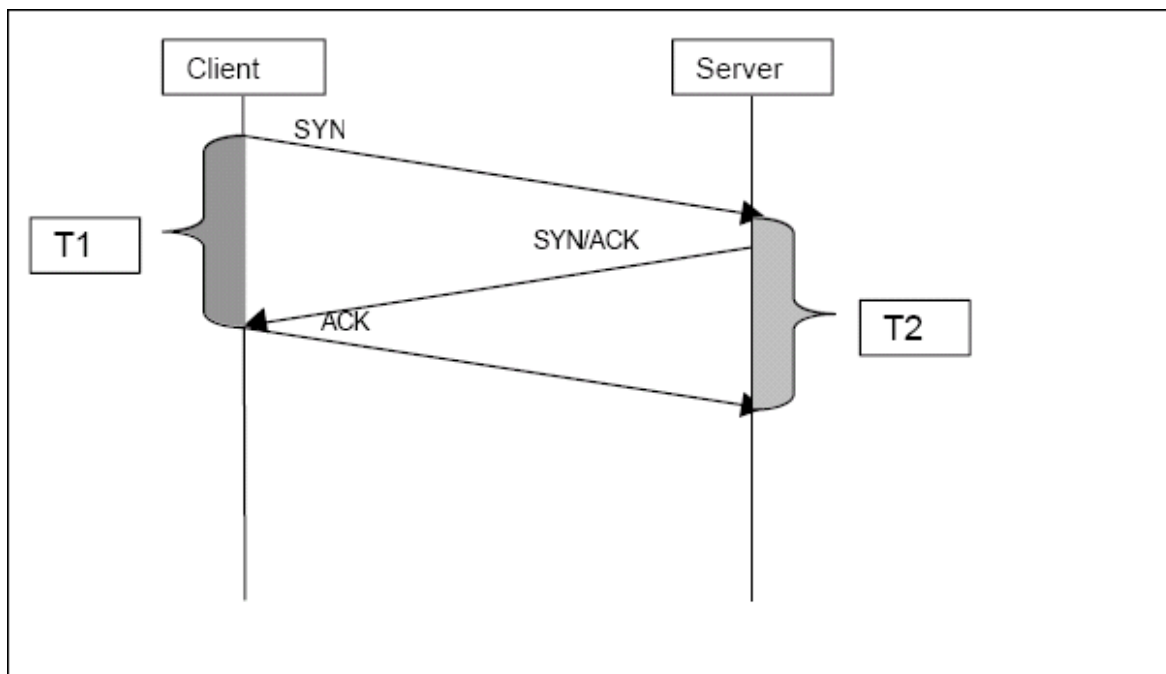
- ["Introduction to Performance Measurements" below](#)
- ["TCP Request-Response Measurements" on the next page](#)
- ["HTTP Measurements" on page 17](#)
- ["End User Measurements" on page 21](#)

Introduction to Performance Measurements

To understand RUM performance measurements, a basic knowledge of TCP/IP is beneficial. The following are some of the TCP/IP and http terms used in describing performance measurements:

- **SYN.** A request for connection
- **ACK.** An acknowledgement response
- **GET.** A request for data

Performance measurements are aimed at measuring real-user experience, that is, the end-to-end user experience. To measure both client-side and server-side measurements, the Parallel Technique is used, in which it is assumed that measuring the event on the server side is a close approximation of the event's measurement on the client side. All RUM measurements are performed on the server side, but provide end-to-end data. The following diagram shows that since the lines are parallel, it is assumed that T1 (client-side measurement)=T2 (server-side measurement).



TCP Request-Response Measurements

It is important to understand the following TCP Request-Response measurements, as they form an integral part of the TCP Request-Response data reported by RUM:

- **Response Time.** The time from the first packet of the request, until client acknowledgement of the last packet of the response. If the request opens a new connection, the time taken to establish this connection is included in the response time. Download time is the sum of server time and network time.
- **Server Time.** By understanding the TCP protocol, RUM determines which time intervals were spent on server processing (either server application processing time or server kernel processing time). These intervals are incorporated into the server time. This measurement includes server time to first buffer.
- **Server Time to First Buffer.** The time from the last packet of the request to the first packet of the response. This is the time taken by the server to process the request.
- **Network Time.** The time intervals that were spent by the server waiting for client acknowledgement to arrive are incorporated into the network time. RUM measures what part of the network time is due to network errors.

HTTP Measurements

HTTP measurements are used by RUM to report page and transaction data to BSM.

This section includes the following topics:

- ["Page Performance Measurements" below](#)
- ["Component Measurements" on the next page](#)
- ["Page Measurements" on page 19](#)
- ["Transaction Measurements" on page 20](#)

Page Performance Measurements

The following table describes the performance measurements of pages that appear in RUM reports:

Measurement	How it is Calculated	Why it Matters
Page Time	The end-to-end time it took to download the whole page.	Enables you to discover which pages are slow (exceed their threshold).
Page Server Time	The time spent on the servers to create the response.	Enables you to track server performance issues.
Page Network Time	The time spent on the network to send the response.	Enables you to isolate network delays.
Page Client Time	The time spent on the client side.	Enables you to understand the client's effect on performance.
Page Hits	There are separate counters for available and unavailable hits. Unavailable hits are defined by events and errors configured in End User Management Administration.	Help you determine the overall availability of an application.
Network Latency	Network latency (round trip) per domain.	Enables you to determine whether there is a network problem.
Server Availability	Server is up or down, and the service (application) is up or down, as a percentage of available http requests.	Enables you to determine whether there is a server availability problem.

Component Measurements

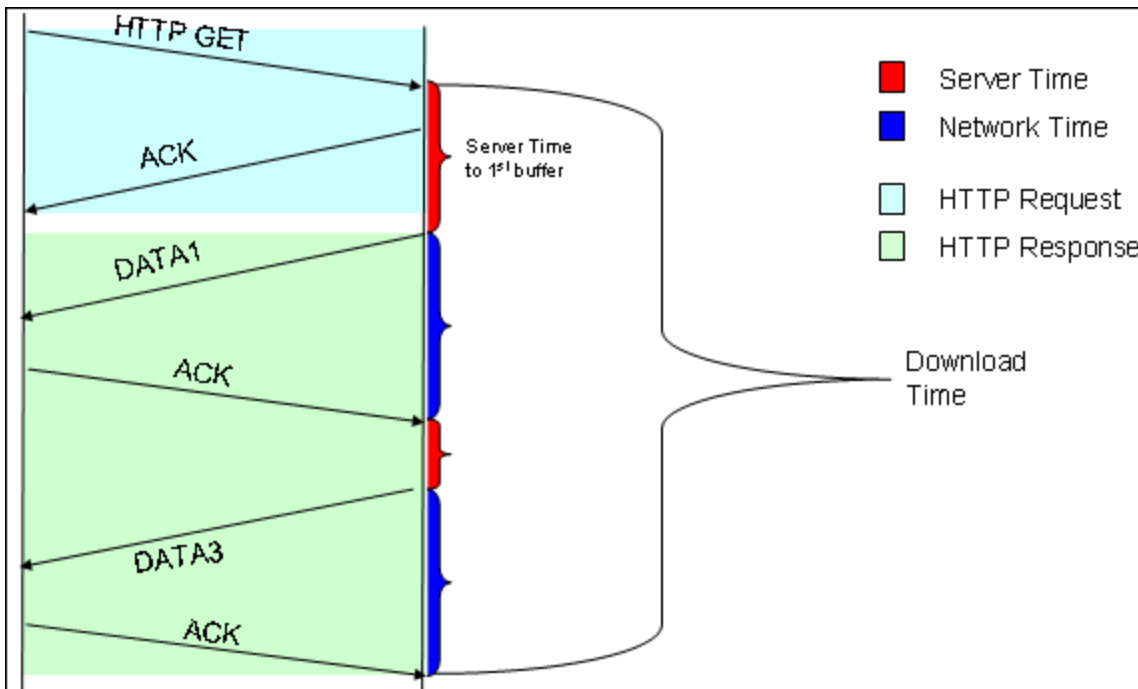
While component measurements are not reported to BSM, it is important to understand them as they form an integral part of page and transaction measurements.

An http component is a single request response couple.

The following component measurements are used in RUM:

- **Component Download Time.** The time from the first packet of the request, until client acknowledgement of the last packet of the response. Component download time is the sum of component server time and component network time. If a request opens a new connection, the time taken to establish this connection is included in the download time.
- **Component Server Time.** By understanding the TCP protocol, RUM determines which time intervals were spent on server processing (either server application processing time or server kernel processing time). These intervals are incorporated into the component server time. This measurement includes component server time to first buffer.
- **Component Server Time to First Buffer.** The time from the last packet of the request to the first packet of the response. This is the time taken by the server to process the request.
- **Component Network Time.** The time intervals that were spent by the server waiting for client acknowledgement to arrive are incorporated into the component network time. RUM measures what part of the network time is due to network errors.

The following diagram shows how component download time is calculated from the component server and network times:



Page Measurements

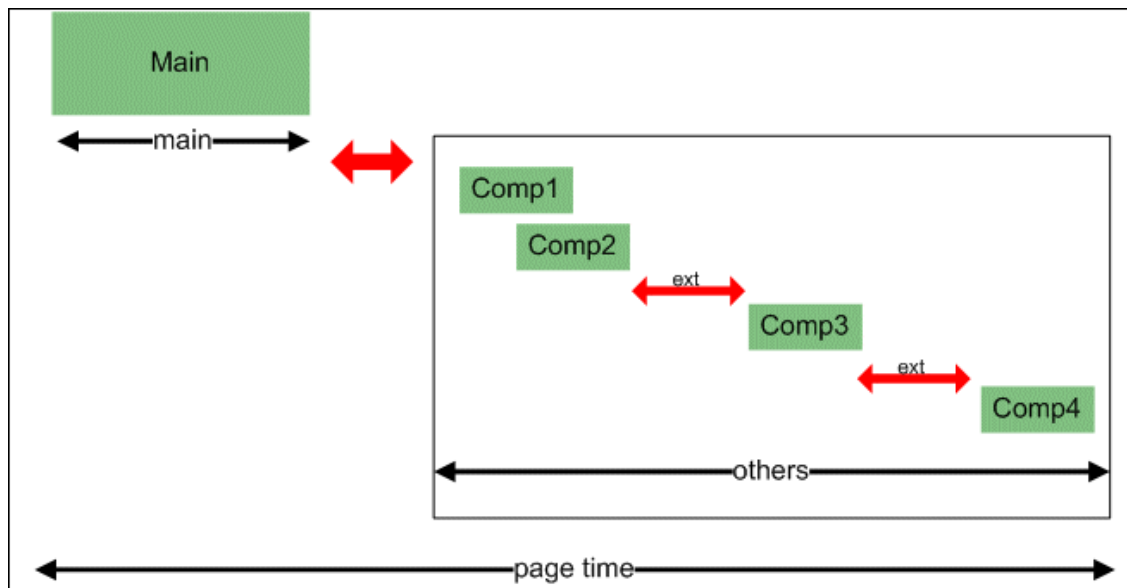
Each HTML page can contain sub-components (such as GIFs, JPGs, and so forth). RUM correlates the main component (the HTML) and the sub-components, and calculates the download time for the whole page.

The following page measurements are used in RUM:

- **Page time.** The time from the first packet of the first component's request to the client ack for the last packet of the last component's response. Page time comprises page client/external time, page network time and page server time.

Because a single page might be downloaded over several connections, which means two or more components might be downloaded simultaneously, and since there might also be time gaps in the page time in which no component is being downloaded, the total page time might not necessarily equal the sum of all the components' download time.

The following diagram shows how several components server time or network time might overlap (Comp1 and Comp2). This makes it difficult to define what portion of the page time is server time and what portion is network time. To overcome this, RUM uses relative measurements for page breakdown:



- **Page client/external time.** A collection of all the time intervals in the page time in which no component was downloaded. These gaps, which are shown in red in the above diagram, are usually caused by client application processing (such as JavaScript).
- **Page Server Time.** The relative part of the Page Time that was spent on server processing. The formula used to calculate this is:

$$\frac{\sum \text{ComponentServerTime}}{\sum \text{ComponentDownloadTime}} \bullet (\text{PageTime} - \text{PageExternalTime})$$

- **Page network time.** The relative part of the page time that was spent on network transportation. The formula used to calculate this is:

$$\frac{\sum \text{ComponentNetworkTime}}{\sum \text{ComponentDownloadTime}} \bullet (\text{PageTime} - \text{PageExternalTime})$$

Transaction Measurements

An RUM transaction consists of a series of pages. A transaction is matched when RUM has monitored all the pages in the series in the correct order.

The following transaction measurements are used in RUM:

- **Transaction Total Time.** The time from the beginning of the download of the first page until the end of the download of the last page.
- **Transaction Net Time.** The portion of the total time that was actually spent downloading the pages. This calculation excludes gaps between the pages, which are considered as user think time. Transaction net time comprises the following measurements:
 - **Transaction Server Time.** The relative part of net time that was spent on server processing. This is calculated considering the server time of the pages. Server time is counted only once for pages that have overlapping sever time. Transaction server time = net transaction time * (total server time / total download time).
 - **Transaction Network Time.** The relative part of net time that was spent on network transportation. This is calculated considering the network time of the pages. Network time is counted only once for pages that have overlapping network time. Transaction network time = net transaction time * (total network time / total download time).
 - **Transaction Client/External Time.** The relative part of net time during which no server processing or network transportation took place (that is, the gaps between components), usually due to client processing. This is calculated considering the client time of the pages. Client time is counted only once for pages that have overlapping client time. Transaction client time = net transaction time * (total client time / total download time).

The following example shows the applicable times for a transaction comprising two pages:

	Start Time	End Time	Download Time	Server Time	Client Time	Network Time	Total Time
Page 1	0	10	10	4	4	2	
Page 2	8	18	10	2	4	4	
Net Transaction Time			18	5.4	7.2	5.4	18

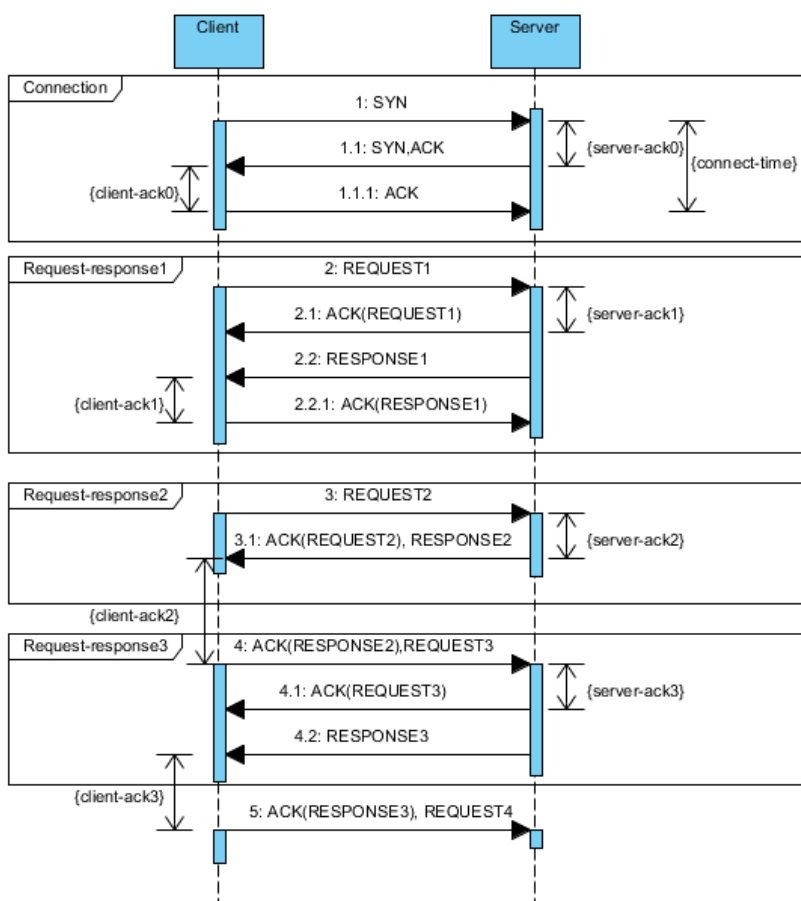
It is possible for a transaction's server, network, or client time to be less than the individual server, network, or client time of one of its included pages. This can occur when the download time of the pages included in the transaction overlap, but register different measurements for the same time period. For example, two pages may be downloading at the same time, but one registers server time while the other registers network time.

End User Measurements

End User Latency is the average RTT (round trip time) it takes for a packet to travel between the server and the client.

Within the scope of RUM, latency refers to Network Latency only. This term mainly refers to network characteristics, but not to RUM itself. The following describes how RUM uses this parameter to calculate latency.

The following diagram displays a single connection having several Actions which are shown as request-response sections:



The latency for this connection is calculated based on the delay between the data connection and corresponding ACK. Only ACK packets with no data are considered when calculating End User Latency.

In the diagram above, there is only one ACK client considered in the latency calculation: client-ack1. The server ACKs participating in the calculation are: server-ack1 and server-ack3.

The following ACK durations are not considered in the calculation:

- client-ack0 and server-ack0, because they are related to the connection stage
- client-ack2 and server-ack2, because they are related to an ACK which contains packets with data (REQUEST3 and RESPONSE2, respectively).

The latency for the connection is calculated as:

- Server-ack-average = $(\text{server-ack1} + \text{server-ack3}) / 2$
- Client-ack-average = $(\text{client-ack1}) / 1$ (we have only one considered ACK client)
- Connection-latency = $(\text{Server-ack-average} + \text{Client-ack-average}) / 2$

The *Reported Latency* for EUGs and Applications is the aggregated value calculated as the average for all included connections (sessions).

Latency constantly changes, so for End-User Subgroups in RUM, the Global Statistic refers to the average network latency in milliseconds for the period.

Installing and Administering RUM

To begin using RUM, you must perform the following steps (after you have installed BSM):

Install the RUM Engine.

For information on installing the RUM Engine and setting up the engine to connect to the Gateway Server, see "Installing the RUM Engine" in the Real User Monitor Installation and Upgrade Guide.

Create and connect to the MySQL database.

You can create and connect to the MySQL database either as part of the RUM Engine installation procedure or separately, at a later time. For details on creating the MySQL database as part of the RUM Engine installation procedure, see "Installing the RUM Engine" in the Real User Monitor Installation and Upgrade Guide. For details on creating the MySQL database at a later time, see "[Overview of the MySQL Database](#)" on page 208.

Install one or more RUM Probes.

For information on installing a RUM Probe and setting it up to report real-user activity data to the engine, see "Installing the RUM Sniffer Probe" and "Installing the RUM Client Monitor Probe" in the Real User Monitor Installation and Upgrade Guide.

If necessary, reconfigure the connection between RUM and BSM.

If connection parameters (such as SSL, proxy, and authentication) have changed since the installation of BSM, use the RUM Engine's web console to reconfigure the connection between RUM and BSM. For detailed information, see "[Using the RUM Web Console](#)" on page 47.

Configure RUM in BSM End User Management Administration.

In End User Management Administration, you configure the specific application, transactions, actions, events, and end-user groups you want to monitor. For more information, see "How to Set up Real User Monitors" in the BSM Application Administration Guide.

Note: You can create RUM alerts if you want to be notified of certain occurrences while monitoring real-user data. You can view reports of the data collected by RUM in the End User Management application. For information on configuring alerts, see "EUM Alerts Administration Overview" in the BSM Application Administration Guide. For information on viewing RUM reports, see "End User Management Reports Overview" in the BSM User Guide.

Chapter 2: RUM Compatibility Matrixes

This section includes the following information:

- "RUM–BSM Compatibility Matrix" below
- "RUM Probe–RUM Engine Compatibility" on the next page

RUM–BSM Compatibility Matrix

The following table shows the compatibility between the different versions of the RUM Engine and BSM Server:

Compatibility Matrix	HP Business Service Management										
	9.25	9.24	9.23	9.22	9.21	9.20	9.13	9.12	9.10	9.0x	8.0x
RUM 9.25	✓	✓	✓	✓	✓	✓	✓	✓	✓	x	x
RUM 9.24	x	✓	✓	✓	✓	✓	✓	✓	✓	x	x
RUM 9.23	x	x	✓	✓	✓	✓	✓	✓	✓	x	x
RUM 9.22	x	x	x	✓	✓	✓	✓	✓	✓	x	x
RUM 9.21	x	x	x	x	✓	✓	✓	✓	✓	x	x
RUM 9.20	x	x	x	x	x	✓	✓	✓	✓	x	x
RUM 9.13	x	x	x	x	x	x	✓	✓	✓	x	x
RUM 9.12	x	x	x	x	x	x	x	✓	✓	x	x
RUM 9.10	x	x	x	x	x	x	x	x	✓	x	x
RUM 9.02	x	x	x	x	x	x	x	x	x	✓	x
RUM 9.01	x	x	x	x	x	x	x	x	x	✓	x
RUM 9.00	x	x	x	x	x	x	x	x	x	✓	x
RUM 8.0x	x	x	x	x	x	x	x	x	x	x	✓

RUM Probe–RUM Engine Compatibility

- **RUM Sniffer Probe.** The RUM Sniffer Probe version must be the same as the RUM Engine version.
- **RUM Client Monitor Probe.** The RUM Client Monitor Probe version must be the same as the RUM Engine version.

Part 2: Data Collection Methods

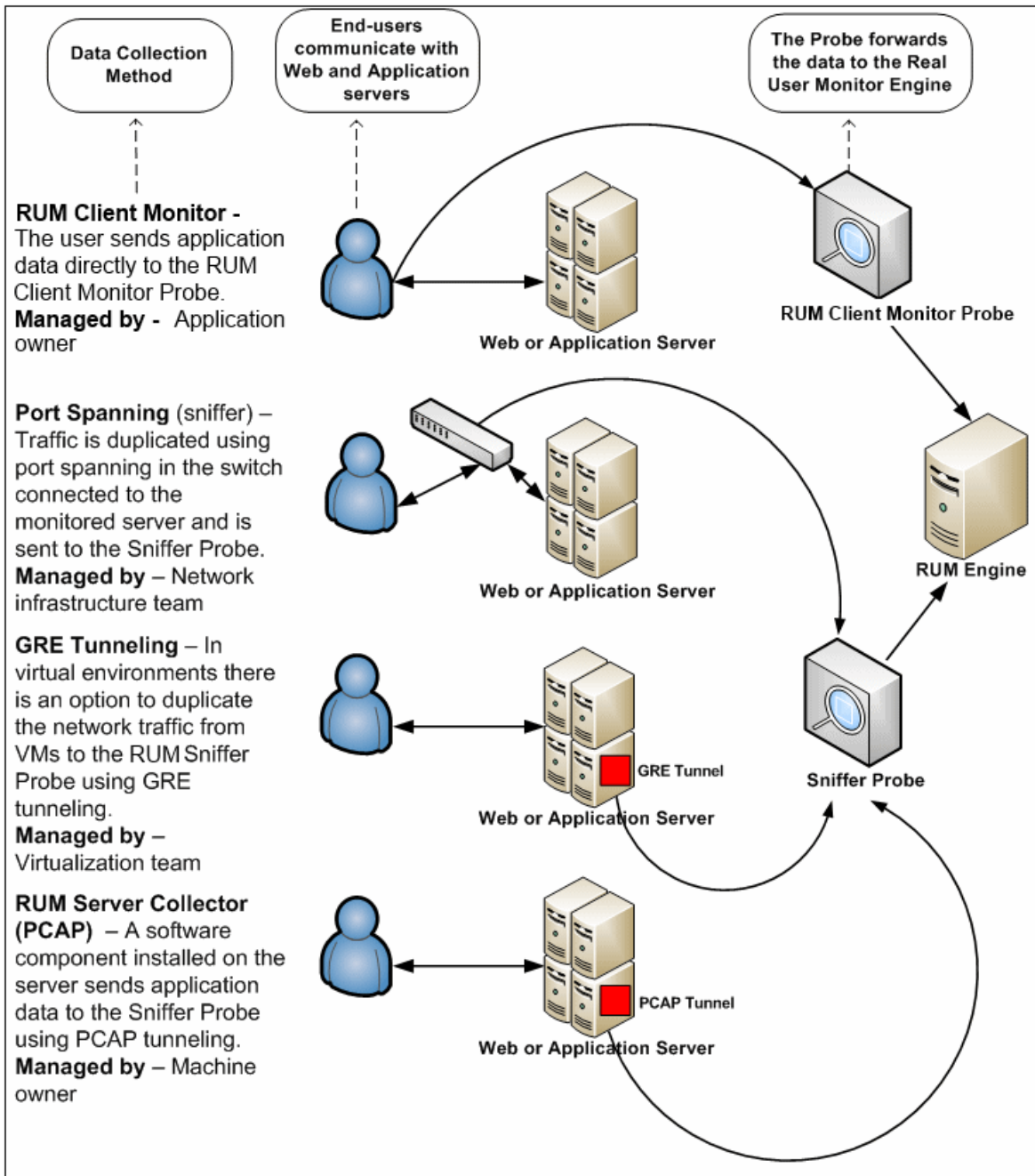
Chapter 3: RUM Data Collection Methods

There are a number of ways by which the RUM Probe can obtain data for monitored applications. The available monitoring solutions depend on the type of RUM Probe you use:

- **Sniffer Probe** data collection methods:
 - **Network tap or switch configuration.** For details, see ["Data Collection Using a Network Tap or Switch Configuration"](#) on page 29.
 - **RUM Server Collector.** For details, see ["Sniffing Using the RUM Server Collector"](#) on page 30.
 - **VMware.** For details see Duplicating Traffic for RUM with VMware in the RUM Deployment Guide.
- **RUM Client Monitor Probe.** For details, see ["RUM Client Monitor Probe"](#) on page 35.

For details on installing the RUM Probe, refer to the Real User Monitor Installation and Upgrade Guide.

The following diagram illustrates the data flow for different RUM Probes and their data collection methods:

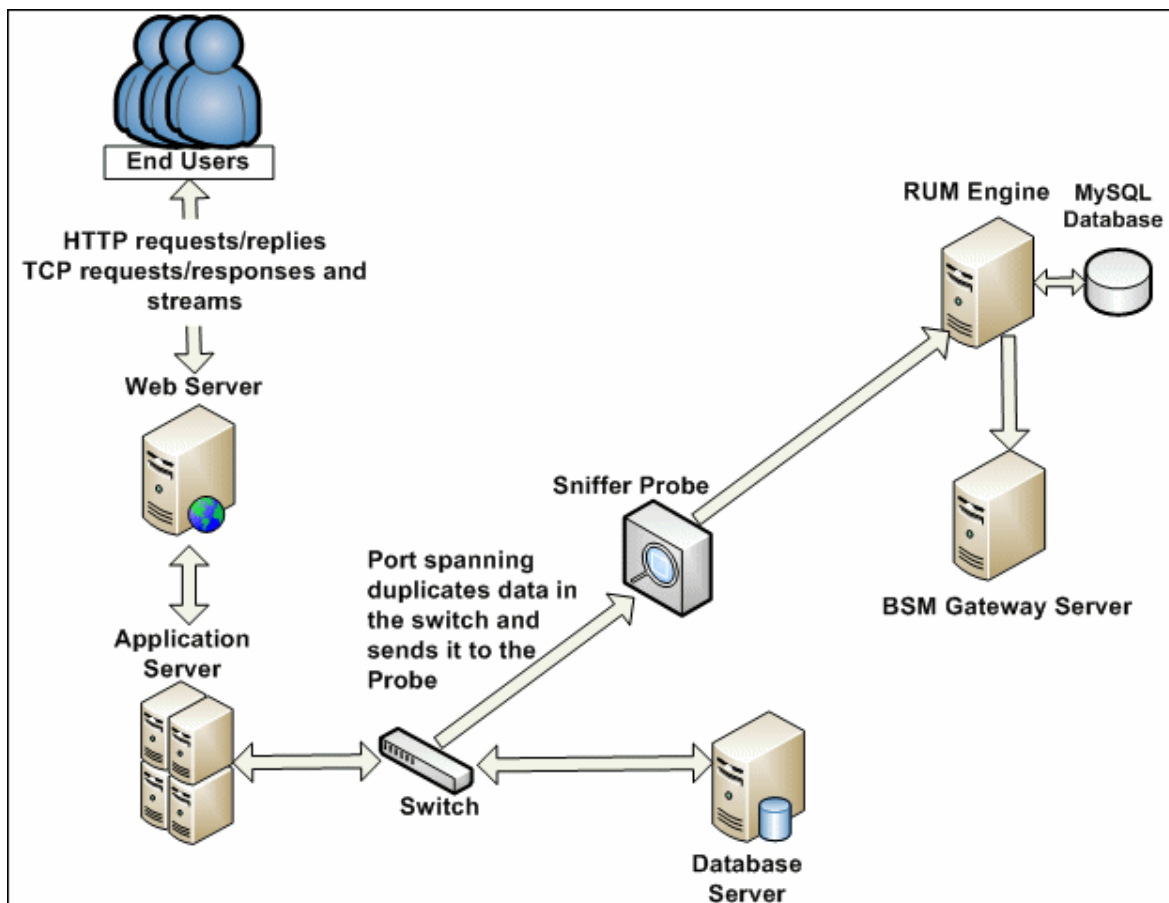


Chapter 4: Data Collection Using a Network Tap or Switch Configuration

The Sniffer Probe is a non-intrusive, passive listening device that is subject to the same traffic the server receives. It is plugged into a network tap that is connected to a monitored server. As end-user traffic passes through the tap, the probe listens to requests and responses sent to and from the server. In this way, data is tracked all the way from the end-user's IP address to the server handling the request.

Note: The configuration in a switch is usually called a mirror or span port, depending on the switch vendor.

The following diagram illustrates the flow for data collection using a network tap or switch configuration:



Chapter 5: Sniffing Using the RUM Server Collector

Note: The RUM Server Collector poses a significant impact on network performance and a slight impact on the server's CPU. Therefore, use of the RUM Server Collector is limited to networks with very low throughput and is mostly recommended for proof of concept (POC) purposes. For example, you can use the RUM Server Collector if the network traffic is not high (150 Mbps for windows and 250 Mbps for Linux) and if you are aware of the implications as noted above.

When it is not possible to use a network tap or port spanning, you can install the RUM Server Collector on a monitored server so that the server sends packets directly to the probe (that is, the probe receives packets directly from the monitored agent). The probe then processes the packets and forwards data to BSM in the regular manner.

The benefit of this is that you only have to be the machine owner of the server on which you install the RUM Server Collector, and are not dependent on the infrastructure team. However, this method does require you to install a software component on the server that runs your application, that is more than just a plug-in to the application.

Note: The recommended data collection method is to use a network tap or port spanning when possible as this eliminates the need to configure and maintain the monitored servers for data collection.

To work with the RUM Server Collector, you must:

1. Install the RUM Sniffer Probe. For details, see "Installing the RUM Sniffer Probe" in the Real User Monitor Installation and Upgrade Guide.
2. Install the RUM Server Collector on the server you want to monitor. For details, see "Installing the RUM Server Collector" in the Real User Monitor Installation and Upgrade Guide.
3. Configure the RUM Server Collector. For details, see ["Configuring the RUM Server Collector" on the next page](#).
4. Configure the RUM Sniffer Probe to retrieve data from the RUM Server Collector. For details, see ["Configuring the RUM Sniffer Probe" on page 32](#).
5. Start the RUM Server Collector service. For details, see ["Administering the RUM Server Collector Service" on page 33](#).

Configuring the RUM Server Collector

Caution: The UTC times on the RUM Sniffer Probe and RUM Server Collector machines must be identical. If they are not, the traffic captured on the RUM Server Collector may be incorrectly processed by the RUM Sniffer Probe, resulting in missing data in EUM reports in BSM.

Note: The RUM Server Collector poses a significant impact on network performance and a slight impact on the server's CPU. Therefore, use of the RUM Server Collector is limited to networks with very low throughput and is mostly recommended for proof of concept (POC) purposes. For example, you can use the RUM Server Collector if the network traffic is not high (150 Mbps for windows and 250 Mbps for Linux) and if you are aware of the implications as noted above.

The RUM Server Collector is installed with default settings, which you can change according to your needs. The configuration is stored in the **collector.conf** file that is located in:

- **Windows:** <RUM Server Collector installation directory>\etc\rum_collector\

(The default RUM Server Collector installation directory is C:\RUMSC)

- **Linux:** <RUM Server Collector installation directory>/etc/rum_collector/

(The default RUM Server Collector installation directory is /opt/HP/RUMSC)

To change the configuration, edit the file, make any of the following changes, and then save the file.

- **Port number.** The default port number used by the RUM Server Collector is **2002**. You can change this number by setting the **port** parameter in the **[general]** section of the file.
- **Allowed clients.** By default, the RUM Server Collector is configured to accept connections from any client (probe). You can limit connections to specific probes by setting a **client** parameter in the **[passive]** section of the file to a specific IP address.

Set a **client** parameter for each IP address you want to allow to connect to the RUM Server Collector.

- **Security.** By default, the RUM Server Collector is configured to enforce SSL connectivity. You can change this by setting the **use_ssl** parameter in the **[security]** section of the file to **false**.

The default security keys and certificates used by the RUM Server Collector for SSL connections are predefined. If you want to use different keys and certificates, you must update the following parameters in the **[security]** section of the file:

- **ssl_ca_file.** The full path to the certificate file used to validate the client certificate sent by the probe.
- **ssl_key.** The full path to the private key file used for accepting server SSL connections from the

probe.

- **ssl_cert.** The full path to the certificate file used for accepting server SLL connections from the probe.

Note: When you make changes to the collector.conf file, you must restart the RUM Server Collector service for the changes to take effect. For details, see ["Administering the RUM Server Collector Service" on the next page.](#)

Configuring the RUM Sniffer Probe

The UTC times on the RUM Sniffer Probe and RUM Server Collector machines must be identical. If they are not, the traffic captured on the RUM Server Collector may be incorrectly processed by the RUM Sniffer Probe, resulting in missing data in EUM reports in BSM.

You can configure any RUM Sniffer Probe to connect to a RUM Server Collector, provided that it has the capacity to handle all the monitored traffic (that is, both the regular sniffed traffic and the RUM Server Collector traffic). A RUM Server Collector can only be connected to one RUM Sniffer Probe, but a RUM Sniffer Probe can be connected to multiple RUM Server Collectors.

Note: The RUM Server Collector poses a significant impact on network performance and a slight impact on the server's CPU. Therefore, use of the RUM Server Collector is limited to networks with very low throughput and is mostly recommended for proof of concept (POC) purposes. For example, you can use the RUM Server Collector if the network traffic is not high (150 Mbps for windows and 250 Mbps for Linux) and if you are aware of the implications as noted above.

To configure the RUM Sniffer Probe to connect to the RUM Server Collector to retrieve data, on the RUM Engine edit the `\HPRUM\conf\configurationmanager\Beatbox_<Probe IP or Probe Host>_Const_Configuration.xml` file. (Either the Probe IP or Probe Host will used depending on the probe registration)

Note: The `Beatbox_<Probe IP or Probe Host>_Const_Configuration.xml` file will appear if you are performing a custom configuration for the probe (such as selecting a NIC). Otherwise, the following default file name appears: `Beatbox_Default_Const_Configuration.xml` file.

If you cannot find the file relevant to your probe, create a copy of the `Beatbox_Default_Const_Configuration.xml` file and rename it to `Beatbox_<Probe IP or Probe Host>_Const_Configuration.xml`.

For example:

`Beatbox_192.168.1.1_Const_Configuration.xml`
or
`Beatbox_ProbeHost_Const_Configuration.xml`

In the `[collector]` section of the file, add devices in the following format:


```
device rpcap://[<server name>]:<port number>/<device name>
```

where:

- **<server name>** = the name or IP address of the server on which the RUM Server Collector is installed. (If you use an IP address it must be enclosed in square brackets.)
- **<port number>** = the port number used to access the server on which the RUM Server Collector is installed, as configured in the RUM Server Collector (default 2002).
- **<device name>** = the Windows or Linux device name of the network card used to access the server on which the RUM Server Collector is installed. To monitor all network cards, omit the **<device name>** parameter completely.

Examples:

- **Specific Windows device using IP:** device rpcap://[172.23.61.71]:2002\Device\WPRO_41_2001_{8568244D-52DE-4CE5-97E7-6DDA2E86E16D}
- **Specific Windows device using server name:** device rpcap://myserver:2002\Device\WPRO_41_2001_{8568244D-52DE-4CE5-97E7-6DDA2E86E16D}
- **Specific Linux device:** device rpcap://[172.23.61.71]:2002/eth0
- **All devices (Windows or Linux):** device rpcap://[172.23.61.71]:2002/

Administering the RUM Server Collector Service

Note: The RUM Server Collector poses a significant impact on network performance and a slight impact on the server's CPU. Therefore, use of the RUM Server Collector is limited to networks with very low throughput and is mostly recommended for proof of concept (POC) purposes. For example, you can use the RUM Server Collector if the network traffic is not high (150 Mbps for windows and 250 Mbps for Linux) and if you are aware of the implications as noted above.

After installing the RUM Server Collector, the HP RUM Server Collector service is automatically started. You can administer the RUM Server Collector service as follows:

Windows: Start, stop, or restart the service from the **services** console.

Linux: Use the command `/etc/init.d/rum_server-collector` option

Valid options are `start`, `stop`, `restart`, or `status`.

RUM Server Collector Log File

To help troubleshoot problems, you can view the RUM Server Collector log file in the following locations:

Windows: <RUM Server Collector installation directory>\var\log\rum_collector\collector.log

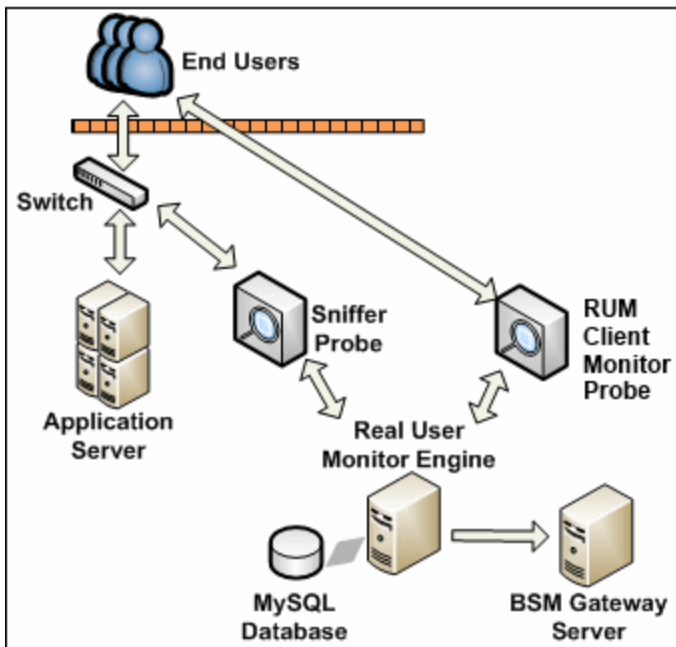
Linux: <RUM Server Collector installation directory>/var/log/rum_collector/collector.log

Note: The RUM Server Collector poses a significant impact on network performance and a slight impact on the server's CPU. Therefore, use of the RUM Server Collector is limited to networks with very low throughput and is mostly recommended for proof of concept (POC) purposes. For example, you can use the RUM Server Collector if the network traffic is not high (150 Mbps for windows and 250 Mbps for Linux) and if you are aware of the implications as noted above.

Chapter 6: RUM Client Monitor Probe

The RUM Client Monitor Probe collects user experience data for your users. Unlike the RUM Sniffer Probe that collects traffic by monitoring network packets using traffic duplication, the RUM Client Monitor Probe receives data for monitored web or mobile applications directly from the client (end user).

The following diagram shows the conceptual difference between the RUM Sniffer Probe and the RUM Client Monitor Probe:



You use different solutions for monitoring web and mobile applications with the RUM Client Monitor Probe:

- The RUM client monitor solution enables you to monitor web applications through an end user's Internet browser. For details, see ["Using the RUM Client Monitor Solution to Monitor Web Applications" on the next page](#).
- The RUM mobile solution enables you to monitor mobile applications through an app on an end user's mobile device. For details, see ["Using the RUM Mobile Solution to Monitor Mobile Applications" on page 39](#).

Note: As the RUM Client Monitor Probe monitors traffic from the client side, reported data in EUM reports is displayed for domains instead of running software elements.

When monitoring mobile applications using Client Monitor Probes, RUM Engine creates a Running Software CI. This CI is not labeled with an IP address since it is situated on the client side and RUM cannot determine the server IP address. Therefore, RUM labels the CI with the application domain.

When a crash occurs, RUM cannot retrieve the domain name so the CI is labeled as *application name_crash*. You can filter out these mobile application Running Software CIs.

Using the RUM Client Monitor Solution to Monitor Web Applications

The RUM client monitor solution enables you to monitor web applications through a user's Internet browser and sends the collected data from the browser directly to the RUM Client Monitor Probe. The advantage of monitoring traffic on the client side instead of the server side, is that the metrics are more accurate as the traffic includes data for the following:

- Proxies
- Content Delivery Networks (CDN)
- External sources (other servers than the one providing the HTML that provide external content such as images)

Note: Data about failures, however, is not included as only successful pages are reported back to the client.

You enable the RUM client monitor solution by installing a JavaScript snippet in the specific HTML pages you want to monitor. This snippet is responsible for collecting performance data on the client machine and sending the collected data to a specific RUM Client Monitor Probe machine. For details, see "Installing the JavaScript Snippet" in the Real User Monitor Installation and Upgrade Guide.

Note: When monitoring the HTML pages, time is only measured for slow components (less than 2 seconds). Size is not measured.

This section includes the following topics:

- ["Supported Browsers" below](#)
- ["Getting Started with the RUM Client Monitor Probe" on the next page](#)
- ["Configuring Applications in BSM for the RUM Client Monitor Solution" on the next page](#)

Supported Browsers

The RUM client monitor solution supports the following Internet browsers:

- Internet Explorer
- Google Chrome

- Firefox
- Safari
- Opera

Getting Started with the RUM Client Monitor Probe

To use the RUM client monitor solution with the RUM Client Monitor Probe, you must:

1. Install the RUM Client Monitor Probe. For details, see "Installing the RUM Client Monitor Probe" in the Real User Monitor Installation and Upgrade Guide.
2. Install the JavaScript snippet in the HTML pages you want to monitor. For details, see "Installing the JavaScript Snippet" in the Real User Monitor Installation and Upgrade Guide.
3. In BSM, configure the web application whose pages you want to monitor. For details, see ["Configuring Applications in BSM for the RUM Client Monitor Solution" below](#).

Configuring Applications in BSM for the RUM Client Monitor Solution

When you configure a web application in End User Management in BSM for monitoring by RUM, some of the configuration settings are not applicable, or must be configured in a certain way, if the application is monitored by a RUM Client Monitor Probe as opposed to a Sniffer Probe. The following table details the relevant configuration settings:

Configuration Setting	Configured In	Remarks
Session Properties	RUM Session Page > Session Properties Area	You must configure the following session properties, although apart from the name, the rest of the session property settings are not used: <ul style="list-style-type: none">• Operating System• Browser
User Name Detection	RUM Application General Page > User Name Detection Area	N/A. User name detection can be configured in the JavaScript snippet.
Parameter Extraction	RUM Application General Page > Parameter Extraction Area	N/A

Configuration Setting	Configured In	Remarks
TCP Settings	RUM Application General Page > TCP/Network Settings Area	N/A. TCP data is not reported for applications configured for the RUM Client Monitor Probe.
Session ID	RUM Session Page > Session Identification Area	N/A. The RUM Client Monitor Probe uses its own mechanism for user session tracking.
Exclude BPM Data	RUM Data Collection Page > General Area	N/A
Sensitive Data	RUM Data Collection Page > Sensitive Data Area	N/A
Snapshots	RUM Data Collection Page > Snapshot Collection Area	N/A
Events	RUM Application Events Page	<p>The following events are applicable to applications monitored by the RUM Client Monitor Probe:</p> <ul style="list-style-type: none"> • Error Page • Text Pattern - you configure the name of the text pattern event in EUM, but define the actual text pattern settings in the JavaScript snippet. • Session Pages • Page Size - the RUM Client Monitor Probe cannot always determine page size. • Page Time <p>All other events are not applicable to applications monitored by the RUM Client Monitor Probe.</p>

Using the RUM Mobile Solution to Monitor Mobile Applications

The RUM mobile solution enables you to monitor mobile applications through apps on a user's mobile device and sends the collected data from the app directly to the RUM Client Monitor Probe. The advantages of monitoring traffic on the client side instead of the server side are:

- The user experience is measured including the latency of the mobile network.
- Data is broken down by operating system, device, connection, and application version.

This section includes the following topics:

- ["Supported Operating Systems" below](#)
- ["Supported Libraries" below](#)
- ["Getting Started with the RUM Client Monitor Probe" on the next page](#)
- ["Configuring Applications in BSM for the RUM Mobile Solution" on the next page](#)

Supported Operating Systems

The RUM mobile solution supports the following operating systems:

- Android 2.2 and later
- iOS 5 and later

Supported Libraries

Network data includes http(s) traffic only. The RUM mobile solution monitors the following libraries:

- iOS
 - NSURLConnection (NSURLSession)
 - AFNetworking
- Android
 - HttpURLConnection
 - ApacheHttpClient

- HTML5 (in Hybrid applications)
 - Page load time - Android version 4 and up only
 - Ajax

Getting Started with the RUM Client Monitor Probe

To use the RUM mobile solution with the RUM Client Monitor Probe, you must:

1. Install the RUM Client Monitor Probe. For details, see "Installing the RUM Client Monitor Probe" in the Real User Monitor Installation and Upgrade Guide.
2. In BSM, configure the mobile application whose pages you want to monitor. For details, see ["Configuring Applications in BSM for the RUM Mobile Solution" below](#).
3. Instrument the mobile application. For details, see "Instrumenting Mobile Apps for Android" and "Instrumenting iOS Apps" in the Real User Monitor Installation and Upgrade Guide.

Note: For more information on monitoring hybrid apps, see "Monitoring Hybrid Applications" in the Real User Monitor Installation and Upgrade Guide.

4. Sign the mobile application and upload the application to the application store (for production applications). For details, see "Instrumenting Mobile Applications for Android" in the Real User Monitor Installation and Upgrade Guide.
5. Install the instrumented application on a mobile device.
6. Start and use the application.

Configuring Applications in BSM for the RUM Mobile Solution

When you configure a mobile application in End User Management in BSM for monitoring by RUM, some of the configuration settings are not applicable, or must be configured in a certain way, if the application is monitored by a RUM Client Monitor Probe as opposed to a Sniffer Probe. The following table details the relevant configuration settings:

Note: When you configure a new mobile application in End User Management, use the **Network for Mobile Application** template.

Configuration Setting	Configured In	Remarks
Application Location	RUM General Page > Application Location Area	Instead of configuring an application location using URLs or IP addresses, you generate an application key that the probe uses to link monitored data for a mobile application, to the application configured in BSM.
Session Properties	RUM Session Page > Session Properties Area	Applicable session properties are predefined in the Network for Mobile Application template and must not be changed.
User Name Detection	RUM Application General Page > User Name Detection Area	Configure user name extraction in the same way as parameter extraction (without configuring a parameter name). Instead of configuring all, or specific login actions to search, you can configure all, or specific URL patterns to search.
TCP Settings	RUM Application General Page > TCP/Network Settings Area	N/A. TCP data is not reported for applications configured for the RUM Client Monitor Probe.
Session ID	RUM Session Page > Session Identification Area	N/A. The RUM Client Monitor Probe uses its own mechanism for user session tracking.
Exclude BPM Data	RUM Data Collection Page > General Area	N/A
Sensitive Data	RUM Data Collection Page > Sensitive Data Area	N/A
Snapshots	RUM Data Collection Page > Snapshot Collection Area	N/A
Events	RUM Application Events Page	N/A

Part 3: Configuring and Administering Real User Monitor

Chapter 7: Administering the RUM Engine

You administer RUM by using the Windows Start menu and a task bar icon, and use the RUM logs for troubleshooting.

This chapter includes the following topics:

- ["Administering RUM Monitor" below](#)
- ["RUM Logs" on the next page](#)

Administering RUM Monitor

The Windows Start menu options and the task bar icon that you use to administer RUM are installed during the Windows installation of RUM.

This section includes the following topics:

- ["RUM Windows Start Menu" below](#)
- ["RUM Engine Nanny" on the next page](#)

RUM Windows Start Menu

To access the RUM Start menu that is added to the Windows machine on which the RUM Engine is installed, select **Start > Programs > RUM**. The menu includes the following options:

Administration

The Administration menu option includes the following options:

Option	Description
RUM Configuration Tool	Runs the RUM Configuration Tool, which enables you to create a MySQL database schema, and to connect RUM to a MySQL database. For details, see "Creating and Connecting to the MySQL Database" on page 208 .
Database (only if the MySQL database has been installed)	Opens a submenu with options for starting and stopping the MySQL database on the machine on which it is installed.
Disable RUM	Stops RUM on the specific machine, and disables it from being run automatically whenever the machine is started.
Enable RUM	Starts RUM on the specific machine, and sets it to run automatically whenever the machine is started.

Open RUM Web Console

Selecting this option opens the HP RUM web console used for administering HP RUM. For details, see ["Using the RUM Web Console" on page 47](#).

RUM Engine Nanny

The RUM Engine nanny is responsible for starting and stopping RUM and managing the processes used by it. The nanny runs as a Windows service.

When you enable or disable RUM using the Windows Start menu (**Start > Programs > HP Real User Monitor > Administration**) you start or stop the nanny service, which in turn starts or stops RUM. You can see the status of RUM in the nanny JMX console.

To view the status of RUM:

1. Access the nanny JMX console using the following URL in a browser:
`http://<RUM Engine machine name or IP address>:22735`
2. When prompted for credentials, enter the same user name and password that are configured for the RUM web console.
3. In the **RUM.Nanny** section, click **RUM.Nanny:service=engine**.
4. In the **List of MBean attributes** table, view the value for the Status attribute. Valid statuses for the RUM Engine process are:
 - Starting
 - Started
 - Stopping
 - Stopped
 - Failed

RUM Logs

RUM logs store messages from RUM modules and are used to troubleshoot problems, and to provide information about the system's operations. There are three types of logs: engine logs, jboss logs, and core logs. The log files are located in the **<Real User Monitor Engine root>\log** directory.

This section includes:

- ["Engine Logs" on the next page](#)
- ["Jboss and Tomcat Logs" on the next page](#)
- ["Core Logs" on page 46](#)

Engine Logs

Engine logs contain log messages from the different processes. There are two types of engine log files:

- **RUM Engine log files.** Log files for modules within the RUM Engine.
- **Repository log files.** Log files for modules connecting the RUM Engine and its MySQL database.

There is a log for each module and the RUM Engine saves up to 20 files for each log by default. When a file reaches a maximum, default size of 3 MB, a new log file is created automatically. Each time the RUM Engine is restarted, it creates a new set of logs.

The name of the RUM Engine log file consists of the module name, log and the log file number. For example, a module called **clustermanager** would produce the following log files:

```
clustermanager.log  
clustermanager.log.1  
clustermanager.log.2  
...
```

The name of the repository log file consists of the log type (repository), the module name, log and the log file number. For example, a repository module called **dataaccesslayer** would produce the following log files:

```
repository.dataaccesslayer.log  
repository.dataaccesslayer.log.1  
repository.dataaccesslayer.log.2  
...
```

The structure of a message in the log file is as follows: <timestamp> <invoking thread> <java class name and line number> <message log level> <message content>. For example:

```
2005-08-03 14:20:32,953 [main] (NodesVerifierManager.java:185) INFO - Found  
primary installation on current machine  
2005-08-03 14:20:33,125 [main] (NodeVerifierServer.java:103) INFO - Got host  
name=paddington from repository. Hostname ID=1
```

Jboss and Tomcat Logs

Jboss and Tomcat log messages are written to the following files in the **<Real User Monitor Engine root>\log** directory:

- **jboss_boot.log.** Logs startup activities including running the jboss process, deployment, and startup status. If RUM fails to start, any problems are written to this log.
- **jboss_server.log.** Logs all jboss activities including jboss messages, deployment and startup

status.

- **jboss_tomcat.log**. Logs the Tomcat messages.

Core Logs

Core log messages are written to log files in the **<Real User Monitor Engine root>\log\core** directory.

The core log files contain messages about the general status of the application server on which the RUM Engine is installed, and its services.

Chapter 8: Using the RUM Web Console

After the RUM Engine has been installed and started, you can use the RUM Engine web console to view and configure the connection between RUM and BSM, view other RUM Engine settings, monitor the health of RUM components, and use RUM diagnostic tools.

This chapter includes the following topics:

- ["Accessing the RUM Engine Web Console" below](#)
- ["Monitoring the Health of RUM Components" on page 51](#)
- ["RUM Configuration and Settings" on page 118](#)
- ["BSM Connection Settings" on page 119](#)
- ["Probe Management" on page 122](#)
- ["TransactionVision Connection Settings" on page 143](#)
- ["Advanced Settings" on page 145](#)
- ["Data Flow Probe Connection Settings" on page 145](#)
- ["System Info" on page 147](#)
- ["RUM Diagnostics Tools" on page 147](#)

Accessing the RUM Engine Web Console

Use the RUM Engine web console to monitor the health of RUM components. You can also use a number of configuration tools to configure the RUM Engine, as well as view and configure the connection parameters between RUM and BSM. In addition, the RUM web console includes diagnostic tools that you can use in resolving RUM problems.

When you start the RUM Engine after installation, you can access the RUM Engine web console by launching a web browser and entering the following URL: `http://<RUM Engine machine name or IP>:8180`.

When prompted, enter the JMX console authentication credentials (if you do not have these credentials, contact your system administrator).

Note: On a Windows machine on which the RUM Engine is installed, you can also access the RUM Engine web console by selecting **Start > Programs > HP Real User Monitor > Open Real User Monitor Web Console**.

This section includes the following topics:

- ["Logging In" below](#)
- ["Logging Out" below](#)
- ["Changing Login Parameters" on the next page](#)
- ["Changing the Language of the RUM Web Console User Interface" on page 50](#)

For information on supporting smart card authentication see *Supporting Smart Card Authentication* in the Real User Monitor Hardening Guide.

Logging In

When you access the RUM Engine web console, the login page opens.

Enter the login parameters (login name and password) of a user defined in RUM, and click **Log In**. After logging in, the user name appears at the top right, in the title bar.

Initial access can be gained using the default superuser login parameters: Login Name=**admin**, Password=**admin**. We recommend that the system superuser change this password immediately to prevent unauthorized entry. For details on changing the password, see ["Changing Login Parameters" on the next page](#).

The RUM Engine web console opens, displaying the top menu bar that enables navigation to the configuration, health, tools, and help pages, as well as the **Logout** button.

Note: After three, consecutive, bad log in attempts, you are locked out of the system for a period of time set by your system superuser. Consult your system superuser for details.

Tip for system superusers: You set the lock out time in the **usersLockoutTime** parameter in the **<RUM root directory>\conf\rumwebconsole\rumwebconsole.xml** file. We recommended that you limit access to this file.

Logging Out

When you complete your session, we recommend that you log out of the web site to prevent unauthorized entry, by clicking **Logout** at the top of the page.

Note: You are automatically logged out of the RUM web console after 20 minutes of inactivity.

Changing Login Parameters

You can add, change, and delete RUM users by editing the **<RUM root directory>\conf\rumwebconsole\users.xml** file. In this file, there is a line for each user in the following format:

```
<user login="admin" name="Administrator" password="encryptedPassword"  
passwordEncrypted="true"/>
```

Note:

- We recommend that the system superuser limits access to the **<RUM root directory>\conf\rumwebconsole\users.xml** file.
- Changes to the **<RUM root directory>\conf\rumwebconsole\users.xml** file only take effect when the RUM Engine is restarted. When the RUM Engine is started, RUM encrypts the password, and sets the **passwordEncrypted** parameter to **true**.

To add a RUM user:

1. Open the **<RUM root directory>\conf\rumwebconsole\users.xml** file in a text editor.
2. Duplicate the entry for one of the existing users.
3. In the duplicate line, enter the **user name**, **login**, and **password** parameters for the new user. Ensure that the **passwordEncrypted** parameter is **false**.
4. Save the file.

To change a RUM user:

1. Open the **<RUM root directory>\conf\rumwebconsole\users.xml** file in a text editor.
2. In the appropriate line, change the **user name** and **login** parameters as required.
3. To change a user's password, enter the new password in the **password** parameter and ensure that the **passwordEncrypted** parameter is **false**.
4. Save the file.

To delete a RUM user:

1. Open the **<RUM root directory>\conf\rumwebconsole\users.xml** file in a text editor.
2. Delete the appropriate line.

3. Save the file.

Note: When deleting users, ensure that there is at least one user configured in the users file, or you are unable to access the RUM web console.

Changing the Language of the RUM Web Console User Interface

The RUM web console user interface can be viewed in the following languages in your web browser:

Language	Language Preference in Web Browser
Chinese	Chinese (China) [zh-cn]
English	English (United States) [en-us]
French	French (France) [fr]
German	German (Germany) [de]
Japanese	Japanese [ja]
Korean	Korean [ko]
Russian	Russian (Russia) [ru]
Spanish	Spanish (Spain) [es]

Use the language preference option in your browser to select how to view the RUM web console. The language preference chosen affects only the user's local machine and not the RUM machines or any other user accessing the same RUM web console. The language is determined when you log in to the RUM web console; changing the language preference in your browser once you have logged in has no effect until you log out and log back in.

To view the RUM web console in a specific language using Internet Explorer:

1. Select **Tools > Internet Options** and click **Languages**. The Language Preference dialog box opens.
2. Select the language in which you want to view the RUM web console.
3. If the language you want is not listed in the dialog box, click **Add** to display the list of languages. Select the language you want to add and click **OK**.
4. Click **Move Up** to move the selected language to the first row.
5. Click **OK** to save the settings.
6. Refresh the page: the RUM web console user interface is displayed in the selected language.

Note:

- Starting from RUM version 7.0, there is no language pack installation. All translated languages are integrated into the RUM Multilingual User Interface.
- Data stays in the language in which it was entered, even if the language of the web browser changes. Changing the language of the web browser on your local machine does not change the language of RUM definitions and configurations.
- If a user selects a language not supported by the RUM Multilingual User Interface, the RUM web console user interface appears in English.

Changing Timeout Parameters

You can enable a RUM Web Console user session to time out after a defined period of inactivity. When this feature is enabled, a RUM Web Console user is logged out after the defined period of inactivity. Only active user actions like browsing, clicking, or refreshing pages are considered to be user activities.

To enable the RUM Web Console user session to time out:

1. Open the **<RUM root directory>\conf\common\common.properties** file.
2. Locate the parameter **EnableWebConsoleUserSessionTimeout** and set it to **true**.
3. The default period of inactivity is 1200 seconds (20 minutes). To change the period of inactivity, locate the parameter **WebConsoleUserSessionTimeout** and set a new timeout value in seconds.

Note: You must restart RUM for the changes to take effect.

Monitoring the Health of RUM Components



The **Health** drop-down menu on the RUM Engine web console menu bar includes options for displaying the status of the main RUM components and for creating a zip file of the RUM resource and log files for use by HP Software Support.

This section includes:

- ["System Health" on the next page](#)
- ["Capture Log Files" on page 118](#)

System Health

You use the **System Health** menu option to display the status of the main RUM components. When you select this option, the System Health page opens. For each component displayed on the System Health page, there are four possible statuses:

	OK
	Minor
	Critical
	No status

You can drill down to see the status of the entities that comprise the RUM component by clicking the component name.

For each entity displayed, apart from the columns included in the tables below, there is a column called **Value (Value Since Startup)**. If an entity is configured to display a value, it is displayed in this column either as an absolute value (for example, the number of pages published), or as a ratio showing a value for a given time period (for example, the number of session events per second). An additional absolute value may be displayed in brackets, which is the accumulated value of the entity since the RUM Engine was last started.

Note: Entities using ratios have no status until the System Health page has been automatically updated twice by the RUM Engine. This can take several moments (by default, up to six minutes).

The following components are displayed in the System Health page and the table for each lists the included entities and describes the meaning of the different statuses:

- ["Configuration Retrieval From BSM Server" on the next page](#)
- ["Database" on page 54](#)
- ["RUM Sniffer Probe" on page 56](#)
- ["RUM Client Monitor Probe" on page 78](#)
- ["RUM Engine" on page 84](#)
- ["Samples to BSM Server" on page 107](#)
- ["ATT" on page 108](#)
- ["Data Access Layer" on page 109](#)
- ["Partition Manager" on page 110](#)

- ["Topology Engine" on page 111](#)
- ["Missing Mirrored Data" on page 118](#)

Configuration Retrieval From BSM Server

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Connection to BSM server	Status of the connection to the BSM Gateway Server for retrieving RUM Engine and Probe configurations	Connection to BSM server is operational	N/A	Connection to BSM server is not operational	Check the <HPRUM>/log/config.manager.log file
Data type <type name> retrieval	Status of the last attempt to retrieve data type <type name> configuration from the BSM Gateway Server	Configuration of data type <type name> successfully retrieved from BSM server	N/A	Errors while trying to retrieve configuration on data type <type name> from BSM server	<ul style="list-style-type: none"> • Check the <HPRUM>/log/config.manager.log file • Files in the <HPRUM>/log/configuration/dataType folder describe the configuration retrieved for each data type

Database

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Database connectivity	Status of the connectivity between the RUM Engine and the MySQL database	Connection to database OK	N/A	Connection to database not working	<ul style="list-style-type: none"> • Check that the MySQL service is running. • Check the following files: <ul style="list-style-type: none"> ■ <HPRUM_DATA>\<hostname>.err ■ <HPRUM>\log\repository.dataaccesslayer.log
Database free space	Percentage of free space (including free space in the tablespace) on the disk on which the MySQL database is installed	More than 4% is free.	3–4% is free.	Less than 3% is free.	<ul style="list-style-type: none"> • Increase disk space • Remove heavy configuration items (such as snapshots, clickstream, and extracted parameters)
Database Response Time	Status of the response time between the RUM Engine and the MySQL database	Database response time is normal	Database response time is below normal	Database response time is slow	<ul style="list-style-type: none"> • Remove database files from anti-virus software configurations • If the database is installed on a virtual system (VMware) and the disk is loaded, relocate the database machine to another ESX.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Database Session Purging Time	The length of time taken to purge old sessions from the database	Purging time is normal	Purging time is slow	N/A	
Number of stale queries	The number of database queries aborted because they were stale (running for too long a period)	N/A	N/A	N/A	<ul style="list-style-type: none"> Remove database files from anti-virus software configurations If the database is installed on a virtual system (VMware) and the disk is loaded, relocate the database machine to another ESX.

RUM Sniffer Probe

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
100 Continue Hits	Opens a page that displays for each monitored web application, the number of 100 Continue Hit messages received by the web servers from clients	N/A	N/A	N/A	
Active Connections	The number of active TCP connections currently monitored by the RUM Probe	The number of active TCP connections is below the internal permitted number	The number of active TCP connections is close to the internal permitted number	The number of active TCP connections has exceeded the internal permitted number	<ul style="list-style-type: none"> • Disable traffic discovery, if it is running. • Verify that monitored traffic does not exceed sizing recommendations.
Active Sessions	The number of sessions currently monitored by the RUM Probe	The number of active sessions is below the internal permitted number	The number of active sessions is close to the internal permitted number	The number of active sessions has exceeded the internal permitted number	Check session configuration. In the RUM web console, Use Probe Management > Session ID Detection.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Bytes received for protocol <type>	The number of bytes received by the servers from clients for the protocol <type>	N/A	N/A	N/A	
Bytes sent for protocol <type>	The number of bytes sent by the servers to clients for the protocol <type>	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Channel "connections" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	Possible causes: <ul style="list-style-type: none"> • Connectivity problem • Configuration problem • Two engines connected to the same probe (in such a case there will be an error message in the probe capture log file - C:\HPRumProbe\output\log\capture.log)
Channel "missing components" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	
Channel "pages" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Channel "poorRequests" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	
Channel "sessions" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	
Configuration to Probe	Status of the last attempt to send the configuration to the RUM Probe	Probe was configured successfully	N/A	Errors during probe configuration process	
Connection to Probe	Status of the http connection from the RUM Engine to the RUM Probe	The connection is successful	N/A	There is no connection	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Disk Utilization for	The RUM Probe disk utilization on a specific partition	Free disk space is sufficient	Free disk space is nearing its limit	Free disk space is insufficient	You can reduce disk size utilized by the Probe by disabling snapshot collection in EUM Administration.
Incomplete Transactions	The percentage of incomplete packets (that is, requests without responses). A high number can indicate a problem with a switch, or with a probe's network configuration.	N/A	N/A	N/A	<ul style="list-style-type: none"> • If the Probe gives a response code 202 and the server time is 0, see troubleshooting for Missing Mirrored Data. • If you are using a switch, ensure that both TX and RX are configured. You can trace this using a sniffer. • If the time to first buffer (the time between the request and the beginning of the response) is greater than two minutes, increase the following processor configuration values in the Probe's Beatbox_Default_Const_Configuration.xml file: <ul style="list-style-type: none"> ■ encrypted_request_timeout (seconds) ■ unencrypted_request_timeout (seconds) <p>Create a pcap and open it with a tcp.analysis.lost_segment filter. Validate that there are no such packets.</p>

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
IPv6 address parsing	The ability of the probe to code and decode IPv6 addresses	No IPv6 application is defined, or an IPv6 application is defined and an IPv6 interface is present on the probe machine	N/A	An IPv6 application is defined, but no IPv6 interface is present on the probe machine	Probable cause is that the RUM Probe has an IPv6 application, but no IPv6 network driver is activated and the Probe may not be able to parse IPv6 data correctly.
Lost SSL Requests	The percentage of SSL requests for which the decryption failed.	N/A	N/A	N/A	View the failure reason in the RUM web console > SSL Keystore management.
Missing Mirrored Data	Click Missing Mirrored Data to see the entities that comprise the Missing Mirrored Data component.				High rates of lost mirror packets result in incomplete data in RUM reports, especially for SSL applications. Contact your network administrator to check the network mirroring configuration. When using a switch, consider using a network tap.
Network Captures Retriever Queue Size	The queue size of the probe's network capture files.	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Orphan Application Hits	Opens a page that displays for each monitored application, the percentage of page components that could not be correlated to a specific page	N/A	N/A	N/A	Check session configuration. In the RUM web console, Use Probe Management > Session ID Detection.
Packet Queue Work	The current number of packets that have been collected from the network devices, but have not yet been processed	The packet rate is normal	The packet rate is nearing the limit for normal processing	The packet rate is too high	Verify that monitored traffic does not exceed sizing recommendations.
Packets filtered IPv4	The number of IPv4 packets that were filtered (that is, that reached the probe, but were not processed)	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Packets filtered IPv6	The number of IPv6 packets that were filtered (that is, that reached the probe, but were not processed)	N/A	N/A	N/A	
Packets filtered sum	The total number of packets (IPv4 and IPv6) that were filtered (that is, that reached the probe, but were not processed)	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Packets lost IPv4	The percentage of IPv4 packets that the RUM Probe has recognized as missing	< 1%	>= 1% < 3%	>= 3%	High rates of lost mirror packets result in incomplete data in RUM reports, especially for SSL applications. Contact your network administrator to check the network mirroring configuration. When using a switch, consider using a network tap.
Packets lost IPv6	The percentage of IPv6 packets that the RUM Probe has recognized as missing	< 1%	>= 1% < 3%	>= 3%	
Packets lost sum	The percentage of total packets (IPv4 and IPv6) that the RUM Probe has recognized as missing	< 1%	>= 1% < 3%	>= 3%	
Packets processed IPv4	The number of IPv4 packets that were processed	N/A	N/A	N/A	
Packets processed IPv6	The number of IPv6 packets that were processed	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Packets processed sum	The total number of packets (IPv4 and IPv6) that were processed	N/A	N/A	N/A	
Packets with bad checksum	The percentage of packets with bad checksums	N/A	N/A	N/A	If the RUM Probe is on a client/server machine, edit the <HPRUM>\conf\configurationmanager\Beatbox_Default_Const_Configuration.xml file and in the <static_global_params> section change the global_skip_checksum value to true. The checksum is calculated only after passing the network card.
Pages Cached	The number of page views currently being cached to the RUM Probe's memory	The page rate is stable	The page rate is nearing the limit for normal caching	The page rate is too high	Verify that monitored traffic does not exceed sizing recommendations.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Pages Channel Processing Delay	Displays the difference between the time a page hit was received by the probe to when it was reported to the RUM Engine	N/A	N/A	N/A	<ul style="list-style-type: none"> • Check that the number of pages/sec is within Engine sizing guidelines. • The connection between the Engine and the Probe is slow, or the Engine needs a lot of time to connect to the Probe using SSH: <ul style="list-style-type: none"> ■ Check the bandwidth between the Engine and the Probe. ■ Check the <HPRUM>\log\bbretriever.log file.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Plain Bytes Received	The total number of non SSL bytes received by the servers from clients	The current load of http received traffic is normal	N/A	The current load of http received traffic is too high for a single RUM Probe	The Probe may be processing too much traffic. Check the sizing guidelines.
Plain Bytes Sent	The total number of non SSL bytes sent by the servers to clients	The current load of http sent traffic is normal	N/A	The current load of http sent traffic is too high for a single RUM Probe	
Plain Packets	The total number of non SSL packets processed by the RUM Probe	The http packet rate is normal	N/A	The http packet rate is too high for a single RUM Probe	
Probe and Engine Time Difference	Displays the status of the time synchronization between the RUM Engine and Probe	The RUM Engine and Probe are in sync	The RUM Engine and Probe are slightly out of sync	The RUM Engine and Probe are grossly out of sync	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Channel rum-components Guarantee Delivery Files Total Size	The total size of component channel files on the RUM Probe	N/A	N/A	N/A	
Probe Channel rum-components Total Guarantee Delivery Files	The number of guaranteed delivery files for the components channel waiting to be read by the RUM Engine	The number of component channel files is normal	The number of component channel files is high, indicating that the RUM Engine might be processing less data than the RUM Probe is producing	N/A	The Probe is handling traffic faster than the Engine can read and process data from the Probe. Check sizing guidelines.
Probe Channel rum-connections Guarantee Delivery Files Total Size	The total size of connection channel files on the RUM Probe	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Channel rum-connections Total Guarantee Delivery Files	The number of guaranteed delivery files for the connections channel waiting to be read by the RUM Engine	The number of connection channel files is normal	The number of connection channel files is high, indicating that the RUM Engine might be processing less data than the RUM Probe is producing	N/A	The Probe is handling traffic faster than the Engine can read and process data from the Probe. Check sizing guidelines.
Probe Channel rum-pages Guarantee Delivery Files Total Size	The total size of page channel files on the RUM Probe	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Channel rum-pages Total Guarantee Delivery Files	The number of guaranteed delivery files for the pages channel waiting to be read by the RUM Engine	The number of page channel files is normal	The number of page channel files is high, indicating that the RUM Engine might be processing less data than the RUM Probe is producing	N/A	The Probe is handling traffic faster than the Engine can read and process data from the Probe. Check sizing guidelines.
Probe Channel rum-poor-requests Guarantee Delivery Files Total Size	The total size of poor-request channel files on the RUM Probe	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Channel rum-poor-requests Total Guarantee Delivery Files	The number of guaranteed delivery files for the poor-requests channel waiting to be read by the RUM Engine	The number of poor-request channel files is normal	The number of poor-request channel files is high, indicating that the RUM Engine might be processing less data than the RUM Probe is producing	N/A	The Probe is handling traffic faster than the Engine can read and process data from the Probe. Check sizing guidelines.
Probe Channel rum-sessions Guarantee Delivery Files Total Size	The total size of session channel files on the RUM Probe	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Channel rum-sessions Total Guarantee Delivery Files	The number of guaranteed delivery files for the sessions channel waiting to be read by the RUM Engine	The number of session channel files is normal	The number of session channel files is high, indicating that the RUM Engine might be processing less data than the RUM Probe is producing	N/A	The Probe is handling traffic faster than the Engine can read and process data from the Probe. Check sizing guidelines.
Probe Channels Data Flow	Status of retrieving data from the RUM Probe	Data from the probe successfully retrieved	Probe has not produced new data for some time	N/A	Problem with the connection between the RUM Engine and the RUM Probe, or problems with one or more channels on the Probe side: <ul style="list-style-type: none"> • Check the <HPRUM>\log\bbretriever.log file • Try to restart the RUM Probe
Probe Connections Published	The number of connections recorded by the RUM Probe	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Connections Processed by Engine	The number of connections that the RUM Engine has started to process	N/A	N/A	N/A	
Probe has been Restarted	"1" indicates that the RUM Probe was restarted in the last measured interval (5 minutes by default).	Always green	N/A	N/A	
Probe Page Hits	The number of page hits recorded by the RUM Probe	N/A	N/A	N/A	
Probe Page Hits Processed by Engine	The number of page hits that the RUM Engine has started to process	N/A	N/A	N/A	
Probe Process CPU Utilization	The current percentage of probe utilization of the probe process	Probe utilization is normal	Probe utilization is nearing the limit for a single RUM Probe	N/A	The Probe may be processing too much traffic. Check the sizing guidelines.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Process Memory	The total amount of non-swapped, physical memory used by the RUM Probe, in kilobytes	Always	N/A	N/A	
Probe Process Memory Utilization	The total amount of non-swapped physical memory used by the probe process, out of the total amount of physical system memory, in kilobytes	Memory utilization is normal	Memory utilization is high	Memory utilization is nearing the maximum permissible value	The Probe may be processing too much traffic. Check the sizing guidelines.
Probe Storage ccomps Number of Errors	The number of non critical errors for components that occurred when working with the database	N/A	N/A	N/A	
Probe Storage ccomps Number of Total Records	The total number of records for components in the database	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Storage ccomps Status	The current status of the database for components	Database status is normal	N/A	Database status is bad	
Probe Storage mainpagedb Number of Errors	The number of non critical errors for main pages that occurred when working with the database	N/A	N/A	N/A	
Probe Storage mainpagedb Number of Total Records	The total number of records for main pages in the database	N/A	N/A	N/A	
Probe Storage mainpagedb Status	The current status of the database for main pages	Database status is normal	N/A	Database status is bad	
Probe Storage pcapnetwork Number of Errors	The number of non critical errors for network captures that occurred when working with the database	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Storage pcapnetwork Number of Total Records	The total number of records for network captures in the database	N/A	N/A	N/A	
Probe Storage pcapnetwork Status	The current status of the database for network captures	Database status is normal	N/A	Database status is bad	
Received Bytes on Network Device	The total number of bytes received per specific NIC, in bits per second	Network device load is normal	Network device load is nearing the probe's limit	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
SSL Bytes Received	The total number of ssl bytes received by the servers from clients	The current load of https received traffic is normal	N/A	The current load of https received traffic is too high for a single RUM Probe	The Probe may be processing too much traffic. Check the sizing guidelines.
SSL Bytes Sent	The total number of ssl bytes sent by the servers to clients	The current load of https sent traffic is normal	N/A	The current load of https sent traffic is too high for a single RUM Probe	
SSL Packets	The total number of ssl packets processed by the RUM Probe	The https packet rate is normal	N/A	The https packet rate is too high for a single RUM Probe	
Total Memory	The total amount of physical system memory, in kilobytes	Always	N/A	N/A	
SSL Transactions Dropped	The percentage of SSL transactions that could be decrypted	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
XFF over NAT	Value can be 0 or 1. If 1, the value of “x-forwarder-for” http header has different values within the same connection. Can indicate differences between http and TCP reports on the same application.	N/A	N/A	N/A	

RUM Client Monitor Probe

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Active Sessions	The number of sessions currently monitored by the RUM Probe	The number of active sessions is below the internal permitted number	The number of active sessions is close to the internal permitted number	The number of active sessions has exceeded the internal permitted number	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Active Sessions per Application	The number of sessions for a specific application currently monitored by the RUM Probe	The number of active sessions is below the internal permitted number	The number of active sessions is close to the internal permitted number	The number of active sessions has exceeded the internal permitted number	Check session configuration. In the RUM web console, Use Probe Management > Session ID Detection.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Channel "cbd" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	Possible causes: <ul style="list-style-type: none"> • Connectivity problem • Configuration problem • Two engines connected to the same probe (in such a case there will be an error message in the probe capture log file - C:\HPRumProbe\output\log\capture.log)
Channel "connections" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	
Channel "missing components" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Channel "pages" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	
Channel "poorRequests" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	
Channel "sessions" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Configuration to Probe	Status of the last attempt to send the configuration to the RUM Probe	Probe was configured successfully	N/A	Errors during probe configuration process	<ul style="list-style-type: none"> • Check the connection to the probe • Check the connection to the probe
Connection to Probe	Status of the http connection from the RUM Engine to the RUM Probe	The connection is successful	N/A	There is no connection	
Pages Cached	The number of page views currently being cached to the RUM Probe's memory	The page rate is stable	The page rate is nearing the limit for normal caching	The page rate is too high	Verify that monitored traffic does not exceed sizing recommendations.
Probe and Engine Time Difference	Displays the status of the time synchronization between the RUM Engine and Probe	The RUM Engine and Probe are in sync	The RUM Engine and Probe are slightly out of sync	The RUM Engine and Probe are grossly out of sync	
Probe Client Monitor Page Hits	The number of hits from a client browser on a mobile device	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Channel Delay	The delay between the read time from the probe and the current time	N/A	N/A	N/A	
Probe Channels Data Flow	Status of retrieving data from the RUM Probe	Data from the probe successfully retrieved	Probe has not produced new data for some time	N/A	Problem with the connection between the RUM Engine and the RUM Probe, or problems with one or more channels on the Probe side: <ul style="list-style-type: none"> • Check the <HPRUM>\log\bbretriever.log file • Try to restart the RUM Probe
Probe Dropped Page Hits Due Other Reasons	The number of pages dropped due to other reasons	N/A	N/A	N/A	
Probe Dropped Page Hits Due Traffic	The number of pages dropped due to traffic issues	N/A	N/A	N/A	
Probe Dropped Page Hits Due Unresolved Host	The number of pages dropped due to an unresolved host	N/A	N/A	N/A	
Probe Dropped Page Hits of Undefined Application	The number of pages dropped as they do not belong to a defined application	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe License Status	The license status according to the license configured in BSM	The license status is OK	N/A	Check license status and details in BSM	In BSM > End User Management Administration, check license status for current Probe
Probe Mobile Page Hits	The number of hits from a mobile device to a remote server	N/A	N/A	N/A	
Probe Session Hits	The number of closed sessions monitored by the RUM Probe	N/A	N/A	N/A	

RUM Engine

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Application Transaction Count	The total number of open application transactions	Always	N/A	N/A	
ATT	Click ATT to see the entities that comprise the ATT (Automatic Transaction Tracking) component.				

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
BBRetriever hold time due to load on Entry Topic	The time (in milliseconds) that the BBRetriever was stopped due to JMS load on the Entry topic	N/A	N/A	N/A	
BBRetriever hold time due load on RawEntry Topic	The time (in milliseconds) that the BBRetriever was stopped due to JMS load on the RawEntry topic	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
BBRetriever hold time due to load on TCP Entry Topic	The time (in milliseconds) that the BBRetriever was stopped due to JMS load on the TCP Entry topic	N/A	N/A	N/A	
BBRetriever hold time due to load on TCP RawEntry Topic	The time (in milliseconds) that the BBRetriever was stopped due to JMS load on the TCP RawEntry topic	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
BBRetriever Thrown Objects	The total number of objects thrown by the BBRetriever	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
BBRetriever Total Actions Published	The number of actions being published by the BBRetriever in the RUM Engine	The number of actions being published is normal	The number of actions being published is above average	The number of actions being published is high	There is more traffic (actions/connections/pages) than the Engine can handle. Check sizing guidelines.
BBRetriever Total Connections Published	The number of connections being published by the BBRetriever in the RUM Engine	The number of connections being published is normal	The number of connections being published is above average	The number of connections being published is high	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
BBRetriever Total Pages Published	The number of pages being published by the BBRetriever in the RUM Engine	The number of pages being published is normal	The number of pages being published is above average	The number of pages being published is high	
BBRetriever Total Poor Requests Published	The number of Poor requests published by the BBRetriever in the RUM Engine	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Classification total application tiers with classification disabled	The number of applications whose actions will no longer be classified	0	> 0	N/A	<p>A specific application is not supported by the RUM classification algorithm.</p> <p>You can view application statistics in the RUM JMX console:</p> <p><code>http://<Engine_host>:8180/jmx-console/HtmlAdaptor?action=inspectMBean&name=RUM.modules%3Aservice%3DResolverClassification >viewStatistics</code></p> <p>If the application has more than 200 clusters, we recommend disabling classification for the application (in BSM, select EUM Admin > <application> > Data Collection and clear the Enable automatic page classification check box).</p>
Classification total clusters number	The total number of classification clusters	The number is below the threshold	N/A	The number exceeds the threshold	
Classification total nodes number	The total number of classification nodes	The number is below the threshold	N/A	The number exceeds the threshold	
Data Access Layer	Click Data Access Layer to see the entities that comprise the Data Access Layer component.				

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Data Publisher Channel Configuration Status	The status of building the last published Data Publisher configuration	Always	N/A	The latest published configuration failed to build	
Data Publisher Records failed to be published due to cache overflow	The total number of records which were not successfully published due to cache overflow	0	N/A	>0	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Data Publisher Records failed to be written	The total number of records which were not successfully published	0	N/A	>0	
Free Memory	The free memory available for the RUM Engine	The free memory is sufficient for the RUM Engine to run under the current load	The free memory is nearing the limit for the RUM Engine to run under the current load	The free memory is not sufficient for the RUM Engine to run under the current load	This value shows the total free amount of memory in the Java virtual machine. Try Restarting the RUM Engine.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
JMS Entry topic size	The number of messages in the <entity> queue	The number of messages in the queue is normal	The number of messages in the queue is above normal	The number of messages in the queue is abnormal	<ul style="list-style-type: none"> Performance issue – check sizing guidelines. Configuration issue causes specific module to stop working.
JMS Integration Entry topic size					
JMS Publisher topic size					
JMS Raw Entry topic size					
JMS Samples topic size					
JMS TCP Entry topic size					
JMS TCP Raw Entry topic size					

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
JMS Topology Topic size					

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Location Configuration Validity	Displays the correctness of location configurations	Location configuration is OK	Overlap of IP addresses. One of the overlapping locations is automatically deleted. Check resolver.log for details. Manually reconfigure the locations so that there is no overlap. (You can delete all	Location configuration is problematic. All data is discarded. Check resolver.log for details.	The location configuration received from BSM is invalid. Check locations in the Location manager in BSM. Ensure that there are no overlapping IP ranges.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
			manually created locations; default locations are automatically recreated.)		
Login Maps Size per Name	The total number of login names mapped to sessions	Always	N/A	N/A	
Login Maps Size per Session	The total number of sessions mapped to login names	Always	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Partition Manager	Click Partition Manager to see the entities that comprise the Partition Manager component.				
Publish configuration to module <module name> on host <IP address>	Status of the last attempt to publish the configuration to the RUM Engine internal modules	Configuration to module <module name> on host <IP address> successfully published	N/A	Error while trying to publish configuration to module <module name> on host <IP address>	
Publish Chunks in Memory	The number of sample chunks (not yet sent to BSM) stored in memory	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Poor Request Network Captures Retrieved	The number of Poor request captures retrieved by the RUM Engine	N/A	N/A	N/A	
Poor Request Network Captures Thrown	The number of Poor request captures thrown by the RUM Engine	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Poor Requests with Network Captures	The number of Poor requests that have a network capture file	N/A	N/A	N/A	
Publisher Chunks in Queue	The total number of sample chunks waiting to be sent to BSM	N/A	N/A	N/A	
Resolver Active End Users	The status of received end-user configuration from BSM	Valid end-user configuration received	N/A	Valid end-user configuration not received	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Resolver End User DNS Cache size	The size of the end user DNS cache	N/A	N/A	N/A	
Resolver Ignored Sessions Cache Size	The size of the ignored sessions cache	Cache size is normal	N/A	Cache size has exceeded the permissible limit	
Resolver Server DNS Cache size	The size of the server DNS cache	N/A	N/A	N/A	
Resolver Thrown Actions Because Empty Descriptor	The number of actions for which the template (generic) descriptor is empty or null	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
SessionManager Application Session Count	The total number of open application sessions	Always	N/A	N/A	
SessionManager BB Session Count	The total number of open BB sessions	Always	N/A	N/A	
SessionManager Opened Session Count	The total number of open sessions	Always	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Snapshot Jobs Alive Count	The total number of open snapshot jobs waiting to be processed	RUM can process all the open snapshots	The number of open snapshots waiting to be processed is nearing the limit for RUM under the current load	RUM might not be able to process all the snapshots	In BSM, check the snapshot configuration (EUM Admin > End User Management > Data Collection > Snapshot collection) and ensure that a reasonable number of pages back are configured for snapshots.
Snapshot Jobs Submit Denials	The total number of submit requests for snapshot failures	Always	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Snapshot of Relevant Events	The total number of events that should trigger snapshot creation	Always	N/A	N/A	
Snapshot of Sessions Map Size	The total number of open sessions for which at least one snapshot was created	The number of current sessions is normal	The number of current sessions is nearing the permissible limit	The number of current sessions has exceeded the permissible limit	<ul style="list-style-type: none"> • Check resource connectivity. • Check the application session count (which may be a root cause for this indication). Try to reduce the number of snapshots per application.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Statistics Total Aggregation Size	The number of aggregation buckets in memory	The number of aggregation buckets is normal	The number of aggregation buckets is nearing the permissible limit	The number of aggregation buckets has exceeded the permissible limit	<ul style="list-style-type: none"> Try restarting the Engine. There may be a problem with the aggregation manager module. Look for a problematic type (such as pages, transactions, and so forth) in the RUM Engine JMX console: <a href="http://<Engine_host>:8180/jmx-console/HtmlAdaptor?action=inspectMBean&name=RUM.modules%3Aservice%3DStatisticsMgrConf%3EviewStatus">http://<Engine_host>:8180/jmx-console/HtmlAdaptor?action=inspectMBean&name=RUM.modules%3Aservice%3DStatisticsMgrConf%3EviewStatus
Statistics Total Messages Ignored	The number of entities filtered out by the statistics manager	Always	N/A	N/A	
Topology Engine	Click Topology Engine to see the entities that comprise the Topology Engine component.				

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Total application tiers with number of page names above threshold	The number of applications for which the total number of page names was exceeded and no more page names will be given	0	N/A	N/A	
Total number of page names	The total number of pages (for all applications) that have been given names	< 50000	= 50000	> 50000	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Trie Classification Within Thresholds	The Trie Classification module is functioning and has not exceeded its defined thresholds	1 - within thresholds	0 - exceeds thresholds	N/A	
Trie Classification Total Descriptors Number	The current number of page descriptors in the Trie Classification module	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Trie Classification Total Nodes Number	The current number of internal nodes in the Trie Classification module	N/A	N/A	N/A	

Samples to BSM Server

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Connection to BSM server	Status of the connection between the RUM Engine and the BSM Gateway Server for publishing samples	RUM is successfully sending samples to BSM	N/A	RUM has failed in sending data to BSM	
Publisher burst state	Indication if any samples were delayed during the last attempt to publish data to BSM	All RUM samples are being sent to BSM. No samples are delayed	N/A	RUM is delaying samples so as not to overload BSM	This means that there is more traffic (actions) than the Engine can handle. Check sizing guidelines.
Publisher Samples Created for <entity>	The number of <entity> samples created since the last RUM Engine restart	Always	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Publisher Samples Thrown	The total number of samples thrown	Always	N/A	N/A	
Publisher Total Samples Created	The total number of samples created (for all <entities>) since the last RUM Engine restart	Always	N/A	N/A	
Publisher Total Samples Sent	The total number of samples sent from the Publisher module of the RUM Engine to BSM since the last RUM Engine restart	Always	N/A	N/A	

ATT

To access, click ATT in RUM Engine monitors.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Number of times the interlacing events data exceeded its limit	The number of times that the interlacing events data structure exceeded the internal, default size	OK (the data structure never exceeded the internal, default size)	N/A	The data structure exceeded the internal default size
Number of times the open events data exceeded its limit	The number of times that the open events data structure exceeded the internal, default size	OK (the data structure never exceeded the internal, default size)	N/A	The data structure exceeded the internal default size
Size of event statistics data size	The size of the event statistics data structure	OK (less than the internal, default size)	N/A	Greater than the internal, default size
Size of interlacing events data size	The size of the interlacing events data structure	OK (less than the internal, default size)	N/A	Greater than the internal, default size

Data Access Layer

To access, click Data Access Layer in RUM Engine monitors.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Average response time for <entity>	The amount of time taken to write the <entity> objects to the database	Response time of database is normal	Response time of database is high, which might indicate a database problem	Response time of database is very high, which might indicate a database problem
DAL Active	Whether the Data Access Layer is active or not. In some instances, when free disk space on the database server is running low, the Data Access Layer stops sending data to the database.	The Data Access Layer is active	N/A	The Data Access Layer is not active
Number of cache misses in <entity> lookup table cache	The number of queries to the <entity>'s cache for which data was not available, but should have been	N/A	N/A	N/A
Number of files in <entity> cache	The size of the cache for each <entity> type	There is no backlog	A backlog of objects to be sent to the database exists, which could indicate a database problem or a temporary load peak	A large backlog of objects to be sent to the database exists, which could indicate a database problem or a temporary load peak
Number of futile queries to <entity> lookup table cache	The number of queries to the <entity>'s cache for which data was not available	N/A	N/A	N/A

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Number of <entity> objects sent	The number of <entity> objects sent to the database since startup	N/A	N/A	N/A
Number of queries to <entity> lookup table cache	The total number of queries to the <entity>'s cache	N/A	N/A	N/A
Size of <entity> lookup table cache	The size of the <entity> table in the memory cache	Within the cache limit	N/A	Cache limit breached

Partition Manager

To access, click **Partition Manager** in RUM Engine monitors.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Average Task Execution Time	The average execution time of the scheduled task	Partition Manager average performance is normal	Partition Manager average task performance has exceeded the warning threshold	Partition Manager average performance has exceeded the error threshold and might cause locks in the database during execution
Last Task Execution Status	The status of the last executed task	Partition Manager is running normally	N/A	Partition Manager task failed during last execution
Max Task Execution Time	The maximum execution time of the scheduled task	N/A	N/A	N/A

Topology Engine

To access, click Topology Engine in RUM Engine monitors.

Entity	Description	OK Status (Green)	Min or Status (Yellow)	Critical Status (Red)	Troubleshooting
Auto discovered pages accumulator size	The number of pages created by RUM, waiting to be sent to BSM	<= 500	N/A	> 500	Consider reconfiguring, or disabling the meaningful page mechanism in BSM (EUM Admin).
Auto discovered pages sent set size	The number of create pages sent to BSM since the last RUM Engine restart	<= 1000	N/A	> 1000	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Connection status to CMDB	Status of the connection to the Runtime Service Model (RTSM)	Connection OK	N/A	No connection	<p>Check the RTSM password in the RUM Engine web console (Configuration > BSM Connection Settings > RTSM-RUM integration user password field) and test it using the Test RTSM password button. This password may have been changed from the default one in this specific BSM installation and was not changed in the RUM Engine. You can change the password in BPM using JMX:</p> <p>http://<BSM Data Processing Server machine>:21212/jmx-console/HtmlAdaptor?action=inspectMBean&name=UCMDB:service=SecurityServices#changeIntegrationUserPassword</p> <p>where:</p> <ul style="list-style-type: none"> • customerId = 1 • userName = rum_integration_user
Discovery data is pending report	Tier discovery data is waiting to be delivered to BSM as it was not successfully delivered previously	No data pending	N/A	Data pending	This may be critical (red) during peak traffic periods.

Entity	Description	OK Status (Green)	Min or Status (Yellow)	Critical Status (Red)	Troubleshooting
IP accumulator permanently unresolved set size	The number of IP ranges sent to BSM, that the Location Manager could not resolve to a specific location	< 10,000	N/A	>= 10,000	
IPs accumulator size	The number of IP ranges waiting to be sent to BSM for location matching	<= 5,000	N/A	> 5,000	
Location accumulator permanently unresolved set size	The size of cached unresolved locations to be published to BSM	Within the permitted cache size	N/A	Greater than the permitted cache size	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Locations accumulator size	The size of cached locations to be published to BSM	Within the permitted cache size	N/A	Greater than the permitted cache size	
Number of accumulated IP ranges	The accumulated data structure size of discovered IP ranges	N/A	N/A	N/A	This may be critical (red) during peak traffic periods.
Number of accumulated tiers	The accumulated data structure size of discovered tiers	N/A	N/A	N/A	
Number of new accumulated IP ranges	The accumulated data structure size of new IP ranges	N/A	N/A	N/A	This may be critical (red) during peak traffic periods.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Reports connection to BSM status	The status of the connection to BSM	Connection OK	N/A	No connection	<p>Check the RTSM password in the RUM Engine web console (Configuration > BSM Connection Settings > RTSM-RUM integration user password field) and test it using the Test RTSM password button. This password may have been changed from the default one in this specific BSM installation and was not changed in the RUM Engine. You can change the password in BPM using JMX:</p> <p>http://<BSM Data Processing Server machine>:21212/jmx-console/HtmlAdaptor?action=inspectMBean&name=UCMDB:service=SecurityServices#changeIntegrationUserPassword</p> <p>where:</p> <ul style="list-style-type: none"> customerid = 1 userName = rum_integration_user
Resolved Hosts cache size	The number of hosts to be reported to BSM for CI creation	<= 10,000	N/A	> 10,000	<p>Check in the RTSM that your topology is really this big. If so, consider increasing the maximum value in the xml file for the monitor (c:\<HPRUM>\conf\monitoringmanager\RumEngine\TopologyEngine\<monitor name>.xml).</p>
Resolved Software Elements - Application links cache size	The number of application and software element links reported to BSM	<= 10,000	N/A	> 10,000	

Entity	Description	OK Status (Green)	Min or Status (Yellow)	Critical Status (Red)	Troubleshooting
Resolved Software Elements cache size	The number of software elements reported to BSM	<= 10,000	N/A	> 10,000	
Resolved Subgroups cache size	The number of end-user subgroups reported to BSM	<= 30,000	N/A	> 30,000	
Unresolved Hosts cache size	The number of hosts waiting to be reported to BSM	<= 1,000	N/A	> 1,000	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Unresolved Software Elements - Application links cache size	The number of application and software element links waiting to be reported to BSM	<= 500	N/A	> 500	Check in the RTSM that your topology is really this big. If so, consider increasing the max value in the xml file located in: c:\<HPRUM>\conf\monitoringmanager\RumEngine\TopologyEngine\.
Unresolved Software Elements cache size	The number of software element s waiting to be reported to BSM	<= 1,000	N/A	> 1,000	
Unresolved Subgroups cache size	The number of end-user subgroups waiting to be reported to BSM	<= 1,000	N/A	> 1,000	

Missing Mirrored Data

To access, click Missing Mirrored Data in RUM Probe monitors.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
<Application> Lost Requests	The number of lost requests to web servers per monitored application	N/A	N/A	N/A
<Application> Lost Responses	The number of lost responses from web servers per monitored application	N/A	N/A	N/A

Capture Log Files

You use this option to create a **.ZIP** file of the current status of RUM for support purposes.

Click **Capture** and specify the name and location of the file.

RUM Configuration and Settings

The **Configuration** drop-down menu on the RUM Engine web console menu bar includes the following options:

- **BSM Connection Settings.** Used to view and configure the connection parameters between RUM and BSM. For details, see ["BSM Connection Settings" on the next page.](#)
- **Probe Management.** Used to configure communication settings with the RUM Probe. For details, see ["Probe Management" on page 122.](#)
- **Transaction Management Configuration.** Used to discover the paths through both hardware and software elements, including specific request content, of the pages included in a configured transaction. For details, see ["RUM Transaction Flow Monitoring" on page 171.](#)
- **TV Connection Settings.** Used to view and configure the connection parameters between RUM and TransactionVision. For details, see ["TransactionVision Connection Settings" on page 143.](#)
- **Advanced Settings.** Provides links to specific areas of the HP Real User Monitor JMX console for configuring parameters and settings for individual RUM modules. For details, see ["Advanced Settings" on page 145.](#)
- **Data Flow Probe Connection Settings.** Used to view and configure the connection parameters between RUM and HP Universal Discovery. For details, see ["Data Flow Probe Connection Settings" on page 145.](#)

- **System Info.** Provides general system information about RUM. For details, see ["System Info" on page 147](#).

BSM Connection Settings

This page displays the current connection settings for the communication channel between RUM and BSM, which you can update.

If you change the configuration, click the **Save Configuration** button to save the configuration and update the RUM Engine.

The page contains the following panes:

- ["RUM General Settings Pane" below](#)
- ["Connection to BSM Pane" on the next page](#)
- ["Authentication Pane" on the next page](#)
- ["Proxy Pane" on the next page](#)
- ["SSL Pane" on page 121](#)

RUM General Settings Pane

Field	Description
RUM Engine name	Configure a name for the RUM Engine. This name is registered in BSM and is used to identify the engine in RUM Administration.
RTSM-RUM integration user password	<p>Set the password for the default RTSM-RUM integration user.</p> <p>The RUM Engine sends created CIs to the Run-time Service Model (RTSM), via the BSM Gateway Server. To enable the connection to the RTSM, a default user name (rum_integration_user) and password is used. If you change the default integration user's password in BSM, you must also change it in the RUM Engine. For details on changing the password in BSM, see "Create an Integration User" in the RTSM Developer Reference Guide.</p> <p>Note: If the correct password is not configured (that is, the password configured in the RUM Engine is different to the password configured in BSM), RUM-related topology is not updated in the RTSM and you will not see all RUM data in End User Management reports.</p>

Connection to BSM Pane

Field	Description
BSM Gateway Server host name	The IP address or host name of the machine on which the BSM Gateway Server is installed.
Port	The port number used to connect to the host machine on which the BSM Gateway Server is installed.
Protocol	The protocol used to connect to the host machine on which the BSM Gateway Server is installed. Select either http or https.

Note: If you are an HP Software-as-a-Service user, contact an HP Software Support representative to receive the host name or URL to enter.

Authentication Pane

Field	Description
Use authentication	Select the check box if authentication is required when connecting to the host machine on which the BSM Gateway Server is installed.
Authentication user name	If authentication is required, enter the user name to use.
Authentication password	If authentication is required, enter the password to use.
Authentication domain	If authentication is required, enter the applicable domain for the user.

For more information on using basic authentication in BSM, see "Using Basic Authentication in BSM" in the BSM Hardening Guide.

Proxy Pane

Field	Description
Use proxy	Select the check box if the RUM Engine connects to the BSM Gateway Server machine via a proxy server.
Proxy host	If the RUM Engine connects to the BSM Gateway Server machine via a proxy server, enter the IP address or host name of the proxy server.

Field	Description
Proxy port	If you connect to the BSM Gateway Server machine via a proxy server, enter the port number used to connect to the proxy server.
Use proxy authentication	Select the check box if authentication is required when connecting to the proxy server.
Proxy user name	If authentication is required when connecting to the proxy server, enter the user name to use.
Proxy password	If authentication is required when connecting to the proxy server, enter the password to use.
Proxy domain	If authentication is required when connecting to the proxy server, enter the applicable domain for the user.

For information on using a reverse proxy server with BSM, see "Using a Reverse Proxy in BSM" in the BSM Hardening Guide.

SSL Pane

Field	Description
Truststore path	<p>The full path and file name of the keystore file containing the trusted root certificates. The keystore file must be either a java keystore file (JKS) or PKCS#12 type file.</p> <p>Note:</p> <ul style="list-style-type: none"> • Configure this field only if do not want to use the default JRE truststore (containing well known CA certificates). • We recommend that you locate the truststore file outside of the <Real User Monitor Engine root directory> to avoid possible upgrade issues.
Truststore type	The type of truststore file—JKS or PKCS#12.
Truststore password	The password for the truststore file.

Field	Description
Keystore path	The full path and file name of the keystore file containing the private keys and client certificate. The keystore file must be either a java keystore file (JKS) or PKCS#12 type file. Note: <ul style="list-style-type: none"> • Configure this field only if you want to use client certificates. • We recommend that you locate the keystore file outside of the <Real User Monitor Engine root directory> to avoid possible upgrade issues.
Keystore type	The type of keystore file—JKS or PKCS#12.
Keystore password	The password for the keystore file.
Private key password	The password for the private key located in the keystore file.
Validate host names on server certificates	Select this check box to validate that the configured BSM Gateway Server host name matches the name in the server certificate.
Validate that the server certificates are trusted	Select this check box to validate that at least one of the certificates in the server certificate chain exists in the truststore (either in the configured truststore path, or in the default truststore).
Validate that the server certificates are not expired	Select this check box to validate that the certificate is current.

For information on configuring RUM and BSM to work with SSL, see "Using SSL in BSM" in the BSM Hardening Guide.

Probe Management

You use the Probe Management configuration option to create and administer the RUM Probes that are connected to the engine.








When you select the Probe Management option from the Configuration drop-down menu, the Probe Management page opens and displays a table with the following information for each probe:







Column	Description
Enabled	This value denotes whether the probe is enabled or not. A probe that is not enabled does not monitor RUM traffic. Note: Not all the configuration options are enabled for disabled probes.

Column	Description
Name	The name you configured for the probe.
Host Name	The host name of the machine on which the probe is installed.
Description	A free text description you configured for the probe.



Action Buttons

You use the actions buttons displayed above the table to configure a selected probe and to manage the table. You select a probe by clicking a row in the table. The following table lists and describes the available action buttons:

Icon	Description	For details, see ...
	New Probe Configuration. Opens the New Probe Configuration dialog box, where you configure a new probe for the engine.	"Probe Configuration Dialog Box" on the next page
	Edit Probe Configuration. Opens the Edit Probe Configuration dialog box, where you configure an existing probe for the engine.	"Probe Configuration Dialog Box" on the next page
	Delete Probe Configuration. Deletes a selected probe from the engine.	N/A
	Probe Traffic Discovery. Opens the Probe Traffic Discovery page, where you enable the probe to automatically discover the servers and domains being accessed by the traffic to which it is listening. Note: This button is not enabled for disabled probes.	"Probe Traffic Discovery" on page 127
	Probe Information. Displays general information about the selected probe in a new window. The information displayed shows the status of the probe, the operating system and version running on the probe, the last configuration time of the probe, and the last successful configuration time.	N/A
	SSL Keystore Management. Opens the SSL Keystore Management page, where you manage the keys used by the probe to monitor SSL encrypted traffic. Note: This button is not enabled for disabled probes.	"SSL Keystore Management" on page 130
	Interfaces Configuration. Opens the Interfaces Configuration page, where you list and select a probe's Ethernet devices used to monitor server traffic. Note: This button is not enabled for disabled probes.	"Interface Configurations" on page 134

Icon	Description	For details, see ...
	Server Filter Settings. Opens the Server Filter Settings page, where you list and configure the filters to be used for monitoring server traffic. Note: This button is not enabled for disabled probes.	"Server Filter Settings" on page 136
	Probe Traffic Capture. Opens the Probe Traffic Capture page where you instruct a RUM Probe to save the traffic it monitors to a file.	"Probe Traffic Capture" on page 137
	Session ID Detection. Opens the Session ID Detection page, where you instruct a RUM Probe to detect Session IDs in the traffic it monitors.	"Session ID Detection" on page 138
	Refresh. Refreshes the list of probes in the table.	N/A
	Reset columns width. Resets the columns in the table to their default width.	N/A
	Select Columns. Selects the columns displayed in the table.	N/A

Probe Configuration Dialog Box

You use the Probe Configuration dialog box to configure a new probe for a RUM Engine, or to edit the settings of an existing probe. To access the Probe Configuration dialog box, click the **New Probe Configuration** button  or the **Edit Probe Configuration** button  on the Probe Management page. The Probe Configuration dialog box includes the following fields that you configure for a probe:

Probe Details Pane

Field	Description
Enabled	Select the check box to enable the probe, or clear the check box to disable the probe. Note: A probe that is not enabled does not monitor RUM traffic.
Name	The probe name. Note: This field is mandatory. Syntax exceptions: Cannot exceed 255 characters.
Description	A free text description of the probe. Cannot exceed 255 characters.

Connection to Probe Pane

Field	Description
Host	The IP address or host name of the machine on which the probe is installed. Note: This field is mandatory. Syntax exceptions: <ul style="list-style-type: none">• Cannot exceed 255 characters.• Allowed characters are a-z, A-Z, 0-9, and - \ .] *.
Port	The port number used to connect to the host machine on which the probe is installed. Default value: 2020 Syntax exceptions: Cannot exceed 100 characters.
Protocol	The protocol used to connect to the host machine on which the probe is installed. Select either http or https.

Authentication Pane

Field	Description
Use authentication	Select the check box if authentication is required when connecting to the host machine on which the probe is installed.
Authentication user name	If authentication is required, enter the user name to use.
Authentication password	If authentication is required, enter the password to use.
Authentication domain	If authentication is required, enter the applicable domain for the user.

Proxy Pane

Field	Description
Use proxy	Select the check box if the RUM Engine connects to the probe machine via a proxy server.
Proxy host	If the RUM Engine connects to the probe machine via a proxy server, enter the IP address or host name of the proxy server.

Field	Description
Proxy port	If you connect to the probe machine via a proxy server, enter the port number used to connect to the proxy server.
Use proxy authentication	Select the check box if authentication is required when connecting to the proxy server.
Proxy user name	If authentication is required when connecting to the proxy server, enter the user name to use.
Proxy password	If authentication is required when connecting to the proxy server, enter the password to use.
Proxy domain	If authentication is required when connecting to the proxy server, enter the applicable domain for the user.

SSL Pane


Field	Description
Truststore path	The full path and file name of the keystore file containing the trusted root certificates. The keystore file must be either a java keystore file (JKS) or PKCS#12 type file. Note: Configure this field only if do not want to use the default JRE truststore (containing well known CA certificates).
Truststore type	The type of truststore file—JKS or PKCS#12.
Truststore password	The password for the truststore file.
Keystore path	The full path and file name of the keystore file containing the private keys and client certificate. The keystore file must be either a java keystore file (JKS) or PKCS#12 type file. Note: Configure this field only if you want to use client certificates.
Keystore type	The type of keystore file—JKS or PKCS#12.
Keystore password	The password for the keystore file.
Private key password	The password for the private key located in the keystore file.
Validate host names on server certificates	Select this check box to validate that the configured Probe host name matches the name in the server certificate.

Field	Description
Validate that the server certificates are trusted	Select this check box to validate that at least one of the certificates in the server certificate chain exists in the truststore (either in the configured truststore path, or in the default truststore).
Validate that the server certificates are not expired	Select this check box to validate that the certificate is current.

Probe Traffic Discovery

You use the Probe Traffic Discovery tool to instruct the RUM Probe to automatically detect and report the domains and servers that are accessed by the traffic to which it is listening. You can use the information obtained from the Probe Traffic Discovery tool to help you:

- Configure servers and applications to be monitored by RUM, in End User Management Administration. For task details, see "Getting Started with Real User Monitor" in the BSM Application Administration Guide.
- Determine the protocol types that are used in the system.
- Determine sizing and load balancing needs for RUM. For example, discover throughput for configured applications and ports.
- Troubleshoot RUM Probe issues by checking if and what the probe is monitoring. For example, check if traffic is discovered for a configured application.

When you click the **Probe Traffic Discovery** button  in the Probe Management page, the Probe Traffic Discovery page opens and the Summary View tab is displayed by default. If probe traffic discovery is currently running its results are displayed, otherwise previously saved data (if it exists) is displayed. When you start a new probe traffic discovery, the new statistics are displayed and they are automatically saved, overwriting previously saved data, when you stop the discovery.



Note: It is possible to run the Probe Traffic Discovery tool concurrently with regular probe monitoring.

This section includes the following topics:

- ["Common Elements" below](#)
- ["Summary View Tab" on the next page](#)
- ["Domain View/Server View Tabs" on page 129](#)

Common Elements

The following elements are common to all the tabs in the Probe Traffic Discovery page:

UI Element	Description
	<p>Reset Discovery Statistics. Resets and initializes probe traffic discovery statistics.</p> <p>Note: This button is available only when probe traffic discovery is running.</p>
	<p>Refresh. Refreshes the data displayed on the Probe Traffic Discovery page with the most up to date statistics.</p> <p>Note: This button is available only when probe traffic discovery is running.</p>
<p>Server Type</p>	<p>You can filter the data displayed according to the type of servers. Select Servers on Private IPs, Servers on Non-Private IPs, or Both from the drop-down list in the Server Type filter. The data is redisplayed according to the records matching the search criteria.</p> <p>Default value: Both</p>
<p><General statistics></p>	<p>Discovery start time. The start time of a currently running traffic discovery.</p>
	<p>Sample period. The date and time that the displayed statistics were retrieved are displayed. For statistics loaded from a saved file, Saved Results is displayed next to the date and time.</p>
	<p>Peak total traffic. The peak amount of traffic transmitted to and from all the domains or servers included in the page, for all the discovered protocols.</p>
	<p>Peak pages/sec. The peak number of pages per second for all the domains or servers included in the page, for the http protocol.</p>
<p>Start Discovery</p>	<p>Click the Start Discovery button to start probe traffic discovery for the probe. Starting discovery automatically deletes any previously saved data.</p> <p>Note: The Start Discovery and Stop Discovery buttons are not enabled simultaneously. When one is enabled, the other is disabled.</p>
<p>Stop Discovery</p>	<p>Click the Stop Discovery button to stop probe traffic discovery for the probe and save the current data.</p> <p>Note:</p> <ul style="list-style-type: none"> • The Start Discovery and Stop Discovery buttons are not enabled simultaneously. When one is enabled, the other is disabled. • When you click Stop Discovery, you are prompted to save the current statistics. Saving the statistics overwrites any previously saved data.

Summary View Tab

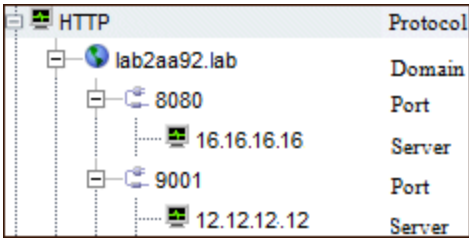
The Summary View tab displays a pie chart in which each slice represents a different, discovered protocol and the slice size is determined by the percentage of protocol throughput out of the total throughput for all the protocols. Click the slice representing the http protocol to display the Domain


View tab, or click on any other slice to display the Server View tab. The Domain View or Server View tab opens with the selected protocol expanded in the hierarchical tree.

Note: The pie chart includes a maximum of 20 slices for the protocols with the highest throughput. If there are more than 20 protocols to be displayed, the protocols with lower throughput are included in the **Others** slice, which also includes protocols and servers that have not yet been recognized.

Domain View/Server View Tabs


The Domain View and Server View tabs display the following information for each discovered protocol:

UI Element	Description
<p>Search</p>	<p>You can filter the data displayed by searching for domains or servers that match a specific pattern or IP address. Enter the search pattern in the Search filter located at the top left of the page, and click Search Domain or Search Server. The data is redisplayed according to the records matching the search criteria.</p> <p>Note:</p> <ul style="list-style-type: none"> • When using the search feature in the Domain View tab, you can enter alphanumeric characters, the asterisk (*) wild card character, and use partial strings for matching. The search filters domain names that include the search string. • In the Server View tab, you can enter only valid IP addresses in the search field. The search filters server IP addresses that exactly match the search string.
<p><Domain View protocol tree></p>	<p>For each discovered protocol, the statistics are grouped by domain names (for http), or IP addresses (for other protocols). For each port in the domain, the IP address of each server that connected to the domain is listed. For example:</p>  <p>Note: This is the default view when you drill down from the Summary View pie chart for the http protocol.</p>

UI Element	Description
<Server View protocol tree>	<p>For each discovered protocol, the statistics are grouped by server IP addresses and for each server, by port. For example:</p>  <p>Note: This is the default view when you drill down from the Summary View pie chart for protocols other than http.</p>
% Throughput	The percentage of throughput for a specific protocol out of the total throughput for all protocols.
Throughput	The total throughput to and from the domain or server, for a specific protocol.
Peak Traffic	The peak amount of traffic transmitted to and from the domain or server, for a specific protocol. Peak traffic is determined based on 30 second intervals.
Peak Pages/sec	The peak number of pages per second for the domain or server for http. Note: This is applicable for http only.
Compressed	Ticked if any of the traffic sent and received by the domain or server was compressed.
Encrypted	Ticked if any of the traffic sent and received by the domain or server was encrypted.
Server Info	The name of the server, if available.
More Details	Reserved for future use.

SSL Keystore Management

You use the SSL Keystore Management page to manage the keys used by a selected RUM Probe to monitor SSL encrypted traffic. To access the SSL Keystore Management page, click the **SSL**

Keystore Management button  on the Probe Management page. The Keystore Management page contains three panes – **SSL Keystore Administration**, **SSL Application Decryption Statistics**, and **SSL Server Decryption Statistics**. To refresh the information on this page, click the **Refresh** button



Note:

- The RUM web console keystore import tool supports PEM, DER, PKCS8, and PKCS12 private key types, as well as Java Keystore. Other key types can be imported if they are converted to one of the supported types.
- The RUM Probe cannot decrypt traffic that uses Diffie Helman keys. If there is a high

percentage of such traffic (which you can see in the **Decryption Failed (unsupported algorithm)** column in the ["SSL Application Decryption Statistics Pane" on page 133](#)) it is recommended that you configure the web server of the monitored server not to support the Diffie Helman protocol.

- The following is a list of ciphers that can be decrypted while monitoring:

SSL v3.0 cipher suites

SSL_RSA_WITH_NULL_MD5	NULL-MD5
SSL_RSA_WITH_NULL_SHA	NULL-SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	EXP-RC4-MD5
SSL_RSA_WITH_RC4_128_MD5	RC4-MD5
SSL_RSA_WITH_RC4_128_SHA	RC4-SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5	EXP-RC2-CBC-MD5
SSL_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA
SSL_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA

TLS v1.0 cipher suites

TLS_RSA_WITH_NULL_MD5	NULL-MD5
TLS_RSA_WITH_NULL_SHA	NULL-SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5	EXP-RC4-MD5
TLS_RSA_WITH_RC4_128_MD5	RC4-MD5
TLS_RSA_WITH_RC4_128_SHA	RC4-SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	EXP-RC2-CBC-MD5
TLS_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA
TLS_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	CAMELLIA128-SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	CAMELLIA256-SHA
TLS_RSA_WITH_SEED_CBC_SHA	SEED-SHA
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	EXP1024-DES-CBC-SHA
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	EXP1024-RC4-SHA

TLS v1.2 cipher suites

TLS_RSA_WITH_NULL_SHA256	NULL-SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384

This section includes:

- ["SSL Keystore Administration Pane" below](#)
- ["SSL Application Decryption Statistics Pane" on the next page](#)
- ["SSL Server Decryption Statistics Pane" on page 134](#)

SSL Keystore Administration Pane

The SSL Keystore Administration pane displays a list of all the configured keys for the selected probe, and for each key shows the number of servers on which it was used to decipher traffic.

To add a key:


1. Click **Add Key**. The Keystore Management page opens.
2. Enter a logical name for the key you are adding.
3. Select the type of file from which to import the key you are adding (a key file or a keystore) and configure the applicable settings:

Key Type	Setting	Description
Import from Key File	File	The path and name of the file containing the private key. You can click Browse to navigate to the relevant file.
	Password	The password with which the key is encrypted, or null if the key is not encrypted.

Key Type	Setting	Description
Import from Keystore	Keystore file	The path and name of the keystore file. You can click Browse to navigate to the relevant file.
	Keystore password	The keystore password. Note: This field is mandatory.
	Private key alias	The alias of the specific key in the keystore. If no alias is configured, the first key in the keystore is used.
	Private key password	The password of the specific key in the keystore.

4. Click **Submit** to save the key and exit, or **Cancel** to exit without saving.

To delete a key:

1. Select the check box to the left of the keys you want to delete.
2. Click the **Delete** button  at the bottom of the pane, or at the end of the row of the selected key.

You can select all, clear all, or invert your selection using the **Select** buttons .

SSL Application Decryption Statistics Pane

The SSL Application Decryption Statistics pane displays the following information for each application for which encrypted traffic was monitored:

Column	Description
Application Name	The name of the application.
Decryption Successful	The percentage of successfully decrypted traffic for the application.
Decryption Failed (in parsing)	The percentage of unsuccessfully decrypted traffic for the application due to a failure in parsing, possibly due to packet loss. If you determine that packet loss is occurring, check your network settings and consider using a tap instead of port spanning for the RUM Probe.
Decryption Failed (no handshake)	The percentage of unsuccessfully decrypted traffic for the application due to an SSL handshake not being found. Possible causes are a non SSL connection, or the RUM Probe being stopped/started during an SSL handshake.

Column	Description
Decryption Failed (unsupported algorithm)	The percentage of unsuccessfully decrypted traffic for the application due to an unsupported algorithm. The SSL handshake algorithm used unsupported, temporary private keys (such as D-H, or RSA with Export restrictions on the key length). If you use an SSL accelerator, a possible solution is to move the RUM Probe behind it.
Decryption Failed (no matching key)	The percentage of unsuccessfully decrypted traffic for the application due to no suitable key being found for the decryption, possibly as a result of the web server key being replaced. Check the keys and if necessary, obtain and configure a new key for use.
Decryption Failed (cache timeout)	The percentage of unsuccessfully decrypted traffic for the application due to any of the above errors in connections from the same user, when decryption failed in the first connection in the session.

SSL Server Decryption Statistics Pane

The SSL Statistics pane displays the amount of encrypted traffic as a percentage of the entire traffic monitored from each server.

Interface Configurations

Use the Interfaces Configuration page to list and select a probe's Ethernet devices used to monitor server traffic.


For RUM Probes running on Linux, only devices named **ethX** (where **X** is a number – such as, eth0, eth1, etc.) can be used for sniffing. This is because the RUM Probes sniff only from an Ethernet network device and rely on **eth** as a standard Ethernet prefix.

To sniff from an Ethernet device with a different name:

1. Open the `<HPRUM>\conf\configurationmanager\Beatbox_<probe name or IP address>_Const_Configuration.xml` file.
2. Edit the **[collector]** section by adding the corresponding configuration:

```
[collector]
#device all
device <1st NIC name>
device <2nd NIC name>
...
device <nth NIC name>
```

Note: Make sure the **#device all** line is prefixed with a hash mark (#).

To access the Interfaces Configuration page, click the **Interfaces Configuration** button  on the Probe Management page. For each Ethernet device, the following information is displayed:

UI Element	Description
Sniff	Check box to select the device to monitor server traffic.
Link Up	Whether the network interface is physically connected to a cable.
Name	The logical name of the Ethernet device.
Up	Whether the device is running or not.
Sniffable	Whether the device can be used to listen to Ethernet traffic.
Hardware	The hardware details of the device.
Driver	The name of the driver used for the device.
IP	The IP address assigned to the device, if any.
Interface Details	Click the Interface Details button for a device to display link, driver, other settings, and statistics information in a new window.

Note: For RUM Probes running on Windows, only the Name element is displayed.


To select a device to be used by the probe for monitoring server traffic, use one of the following options:

- Select the **Sniff** check box to the left of the device you want to use.
- Select the **Probe Auto Select** check box to configure the RUM Probe to listen to all available devices automatically.

Note: This differs from selecting all the devices manually, as the RUM Probe only listens to available devices and not to all devices.

- Click **Restore to Current** to select the devices currently configured for monitoring.
- Click **Recommended Selection** to have the RUM Engine select the devices it considers to be the most suitable to use.

When you have made your selection, click **Save and Upload Configuration** to save the configuration and send it to the RUM Probe.

Note: You can select all, clear all, or invert your selection using the **Select** buttons .


Server Filter Settings

Note: Use server filters to manage probe clustering only. That is, when two or more probes receive the same traffic and you want to assign different parts of the traffic for each probe to monitor.

For traffic filtering, configure application location settings in End User Management Administration. For details, see "Real User Monitor Application Configuration Wizard" in the BSM Application Administration Guide.

If you have existing server filter settings that are used for regular server filtering, we recommend that you delete them and configure application location settings in End User Management Administration instead.

The RUM Probe filters the traffic that it monitors. By default, the filter is set to monitor all traffic from port 80. You can override the default filter by setting filters for specific IP addresses or ranges, and for specific ports that you want to monitor.

You use the Server Filter Settings page to list and configure the filters to be used for monitoring specific server traffic. To access the Server Filter Settings page, click the **Server Filter Settings** button  on the Probe Management page. For each server range, the following information is displayed:

UI Element	Description
Servers	The range or mask of servers to be monitored.
Ports	The ports of the servers included in the range to be monitored.
Clients	By default, a filter applies for all clients accessing the servers.

To display the current server filters data, click **Reload Current Configuration** at the bottom of the page.

You can add new filters, and delete or edit existing filters. After adding, deleting, or changing a filter, click **Save and Upload Configuration** to save the configuration and send it to the RUM Probe.

Add a new filter


1. Click **New Definition**. The Edit Server Filter Settings page opens.

2. In the Edit Server Filter Settings page, enter the following:


Field	Description
Servers	Select the type of server filter you are adding and enter the required data. The following are the available options: <ul style="list-style-type: none">■ Single IP. Enter a single IP address.■ IP Range. Enter the starting and ending IP addresses of the range.■ IP Mask. Enter the network address and applicable IP mask.
Ports	Select the type of port filter you are adding and enter the required data. The following are the available options: <ul style="list-style-type: none">■ Single Port. Enter a single port number.■ Port Range. Enter the starting and ending port numbers of the range.

3. Click **Submit** to save the filter and exit, or **Cancel** to exit without saving.


Delete a filter


Click the **Delete** button  in the row of the filter you want to delete.

Edit a filter

1. Click the **Edit** button  in the row of the filter you want to edit. The Edit Server Filter Settings page opens.
2. In the Edit Server Filter Settings page, edit the information displayed. See above for an explanation of the filter's fields.
3. Click **Save** to save the filter and exit, or **Cancel** to exit without saving.

Probe Traffic Capture

You use the Probe Traffic Capture feature to instruct a RUM Probe to save the traffic it monitors to a file. This is useful for analysis and troubleshooting. To configure and start probe traffic capturing, click the **Probe Traffic Capture** button  on the Probe Management page. The Probe Traffic Capture page opens and displays the following elements:

Element	Description
Capture file max size (MB)	<p>Enter the maximum capture file size in megabytes. You can configure a file size of up to 100 MB.</p> <p>Note: Capturing is automatically stopped when either the configured file size or the configured time is reached.</p>
Capture duration (seconds)	<p>Enter the maximum time (in seconds) for capturing to run. You can configure a time of up to 3600 seconds.</p> <p>Note: Capturing is automatically stopped when either the configured file size or the configured time is reached.</p>
Use client IP filter	<p>Select this check box if you want to capture traffic for a specific range of clients.</p>
Client IP filter from...to	<p>If you select the Use client IP filter check box, enter the IP range for the clients whose traffic you want to capture.</p>
Start Capture	<p>Click the Start Capture button to start the probe traffic capture. The following elements are displayed:</p> <ul style="list-style-type: none"> • Time left. The amount of remaining time that capturing will run. • Current file size. The current size of the capture file. • Capture file location and name. • Stop Capture. Click the Stop Capture button to stop probe traffic capturing when it is running. • Click the Refresh button  to manually refresh the displayed Time left and Current file size data. <p>Note: The Time left and Current file size data is refreshed automatically every ten seconds when capturing is running.</p>

Session ID Detection

Use session ID detection to instruct the RUM Probe to detect session IDs in the traffic it monitors, for applications configured in End User Management Administration. For information on configuring applications in End User Management Administration, see "Real User Monitor Application Configuration Wizard" in the BSM Application Administration Guide.

This section includes the following topics:

- ["Configuring Applications in End User Management Administration Using Traffic Discovery and Session ID Detection" on the next page](#)


- ["Session ID Detection Page" below](#)
- ["Session ID Detection Report" on the next page](#)

Configuring Applications in End User Management Administration Using Traffic Discovery and Session ID Detection


To configure applications in End User Management Administration, you use traffic discovery and session ID detection in the following sequence:

1. Run traffic discovery to identify applications on monitored servers.
2. Configure the discovered applications in End User Management Administration, without session ID parameters.
3. Run session ID detection to identify the relevant session IDs for the applications.
4. Configure the session ID parameters for the applications in End User Management Administration.

Session ID Detection Page

When you click the **Session ID Detection** button  on the Probe Management page, the Session ID Detection page opens. On the Session ID Detection page, the following elements are displayed, which you use to configure and run session ID detection for the selected probe:

UI Element	Description
Detection duration	The length of time, in minutes, that session ID detection should run, when started.
Detect for single IP	If you know that only a single session originates from a specific IP address, select this check box and enter the IP address in the adjacent field. This enhances session detection accuracy.
Last successful detection time	Shows the last date and time that the Session ID Detection tool was successfully run.

UI Element	Description
Status	The status of the session ID detection. Valid statuses are: <ul style="list-style-type: none"> • Idle. Session ID detection is not running. • Running. Displays the percentage of completed data collection and the remaining amount of time that session ID detection will run.
Start Detection	Click to start session ID detection.
Stop Detection	Click to stop session ID detection.
View Results	Click to view the Session ID Detection report for the probe. For user interface details, see " Session ID Detection Report " below. Note: You can only view the results of the current run, once it has stopped (that is, either it completed its full run, or you stopped it manually). If you click the View Results button while session ID detection is running, you see the results of the last completed session ID detection run.
	Refresh. Refreshes the data displayed on the Session ID Detection page.

Session ID Detection Report

For each application configured for the probe in End User Management Administration, the Session ID Analysis report shows the following information:

UI Element	Description
Application Name	The application name, as defined in End User Management Administration. For applications not been defined in End User Management Administration, the application name is Default Website . For information on configuring applications in End User Management Administration, see "RUM Application Configuration Wizard" in the BSM Application Administration Guide.
Application Components	The total number of hits in the application.
Application Pages	The total number of pages in the application.
Application Clients	The total number of clients that accessed the application.
Application Connections	The total number of connections to the application.

UI Element	Description
All Session IDs Coverage	The percentage of hits in the application that contain a discovered session ID key.
Session ID Key	The session ID key name of the session ID discovered for the application.
Type	Where the session ID key is located – cookie, query, or cookie and query.
Regular Expression	The regular expression that uniquely defines the session ID key. The same regular expression should be used in the Scan for field in session identification advanced criteria, when configuring an application in End User Management Administration. For information on configuring applications in End User Management Administration, see "RUM Application Configuration Wizard" in the BSM Application Administration Guide.
Specific Session ID Coverage	The percentage of traffic collected for the application by the data collection process, containing the specific session ID key.
Specific Session ID Correctness	The probability that RUM gives the located key of being a real session ID key.

You can display data for a specific application only, display detailed information for a specific session ID key, and view raw data for a single end-user IP address.

To display data for a specific application only:

Select the application in the **Filter By Application Name** filter, located at the top-left of the report.

To display detailed information for a specific session ID key:

Click a specific key in the Session ID Key column. The Session ID Detection Detailed report is displayed in a new window, and shows the following information for the session ID key:

UI Element	Description
Session ID Properties	Application Name. The application name, as defined in End User Management Administration.
	Session ID Key. The session ID key name.
	Type. Where the session ID key is located – cookie, query, or cookie and query.
	Regular Expression. The regular expression that uniquely defines the session ID key. The same regular expression should be used in the Scan for field in session identification advanced criteria, when configuring an application in End User Management Administration.
	Object Retrieve Phrase. The phrase representing the specific objects to be retrieved from the regular expression. The same phrase should be used in the retrieve field in session identification advanced criteria, when configuring an application in End User Management Administration.
	Specific Session ID Coverage. The percentage of traffic collected for the application by the data collection process, containing the specific session ID key.
	Specific Session ID Correctness. The probability that RUM gives the located key of being a real session ID key.
	First Page Number. The page in which the session ID first appeared. Note: The first page number is shown only if you chose to collect raw data for a specific end-user IP address when starting session ID capturing.
Examples	Displays a few examples of the session ID key and the value located in the key.
Set Cookie Params	If the session ID key is located in a cookie, or in a cookie and query, the path and domain, which are optional parameters sent from the server when setting a cookie for the client, are displayed.
Reasons For Not Locating Session ID Keys in Collected Data	Displays the percentage of traffic collected by the data collection process, not containing the specific session ID key, and for which a reason can be given.
Reasons For Incomplete Session ID Correctness	The reasons why RUM gives the located key a probability of less than 100 percent of being a real session ID key.

To display raw data for a single end-user IP address:

Click **View Raw Data**. The **Session ID Detection Raw Data** report is displayed, and shows the

following information for the end-user IP address:

UI Element	Description
#	A sequential number indicating the row number in the report.
URI	The URI of the page or component.
Page/Component	Indicates whether the data displayed in the row refers to a page or a component.
Referrer	For a page, the referrer is the calling page; for a component, the referrer is the page in which the component is included.
Client Port	The port number of the client's machine on which the data was collected.
Set Cookie	The cookie sent from the server to the client, containing the session ID key.
Cookies	The content of the cookie included in the URL POST parameters.
Query	The content of the query.

Note: The View Raw Data button is only enabled if raw data was collected for a single end-user IP address.

TransactionVision Connection Settings

This page displays the current connection settings for the communication channel between RUM and TransactionVision, which you can update. For details on viewing TransactionVision data from RUM reports, see "Viewing TransactionVision Data From End User Management Reports" in the BSM User Guide.

The TransactionVision Connection Settings page contains the following panes:

- ["Events to TransactionVision Analyzer" below](#)
- ["Connection to TransactionVision Analyzer" on the next page](#)
- ["Authentication Pane" on the next page](#)
- ["SSL Pane" on the next page](#)

Events to TransactionVision Analyzer

Select the check box in this pane to configure RUM to send RUM events data to TransactionVision.

Connection to TransactionVision Analyzer

Configure the following TransactionVision server details:

Field	Description
Host	The IP address or host name of the TransactionVision server.
Port	The port number used to connect to the TransactionVision server.
Protocol	The protocol used to connect to the TransactionVision server. Select either http or https.

Authentication Pane

Configure the following authentication details:

Field	Description
Use authentication	Select the check box if authentication is required when connecting to the TransactionVision server.
Authentication user name	If authentication is required, enter the user name to use.
Authentication password	If authentication is required, enter the password to use.
Authentication domain	If authentication is required, enter the applicable domain for the user.

SSL Pane

Configure the following SSL details:

Field	Description
Truststore path	The full path and file name of the keystore file containing the trusted root certificates. The keystore file must be either a java keystore file (JKS) or PKCS#12 type file. Note: Configure this field only if do not want to use the default JRE truststore (containing well known CA certificates).
Truststore type	The type of truststore file—JKS or PKCS#12.
Truststore password	The password for the truststore file.

Field	Description
Keystore path	The full path and file name of the keystore file containing the private keys and client certificate. The keystore file must be either a java keystore file (JKS) or PKCS#12 type file. Note: Configure this field only if you want to use client certificates.
Keystore type	The type of keystore file—JKS or PKCS#12.
Keystore password	The password for the keystore file.
Private key password	The password for the private key located in the keystore file.
Validate host names on server certificates	Select this check box to validate that the configured TransactionVision host name matches the name in the server certificate.
Validate that the server certificates are trusted	Select this check box to validate that at least one of the certificates in the server certificate chain exists in the truststore (either in the configured truststore path, or in the default truststore).
Validate that the server certificates are not expired	Select this check box to validate that the certificate is current.

Advanced Settings

This option displays RUM modules and provides direct links to specific pages in the RUM JMX console for viewing and configuring the module settings. Each module listed can have any of the following links associated with it:

- **Main Module Page.** Links to general settings for the module name and status.
- **Configuration Page.** Links to settings for the configuration of the RUM module retrieved from BSM.
- **Settings Page.** Links to settings for the configuration of the RUM module in the RUM Engine.

For details on working with the JMX console, see ["Using the JMX Console to Configure the RUM Engine" on page 161](#).

Data Flow Probe Connection Settings

This page displays the current connection settings for the communication channel between RUM and HP Universal Discovery, which you can update.

Overview

You can configure a RUM Engine to interact with Universal Discovery's Data Flow Probes. The RUM Engine gathers information from RUM Probes and passes the following information on to the Data Flow Probes:

- Discovered IPs, running software, and connection dependencies.
- Removed IPs and running software.

When a connection is established between a RUM Engine and Universal Discovery, the RUM Engine receives configuration details from Universal Discovery and passes them on to the RUM Probes. If you have configured specific filters for a probe:

- The RUM Probe monitors traffic according to its filters and from the monitored traffic, sends to Universal Discovery only data that is relevant according to the Universal Discovery configuration settings.
- The RUM Probe sends its filter settings to Universal Discovery, so that it knows what traffic the RUM Probe is monitoring.

Prerequisites

- RUM version 9.20 or later
- HP Universal CMDB version 10.00 or later

Configuration

To configure the connection between the RUM Engine and HP Universal Discovery, enter the following information:

Field	Description
Data Flow Probe host name	The IP address or host name of the Data Flow Probe to which the RUM Engine is to report.
Port	The port number through which the RUM Engine is to send data to the Data Flow Probe.
Protocol	The protocol used to connect to the Data Flow Probe.

Note:

- Leave Authentication, Proxy, and SSL settings empty.
- If you change the configuration, click the **Save Configuration** button to save the configuration and update the RUM Engine.
- For details on configuring Data Flow Probes, refer to the HP Universal CMDB documentation.

System Info

This option shows general system information about RUM, which is displayed in the following panes:

- **RUM Server - General.** Includes the host name, host IP address, total memory, and the number of available processors for the RUM server.
- **RUM Server - OS.** Includes the name and version of the operating system of the RUM server.
- **RUM Database - General.** Includes the host name and port number of the RUM database, as well as the name of the database schema.

RUM Diagnostics Tools

The **Tools** drop-down menu on the RUM Engine web console menu bar includes the following tools:

- **Monitoring Configuration Information.** Displays general configuration data of the applications, end users, pages, probes, transactions, and engine that have been configured for monitoring by RUM in End User Management Administration. For details, see "[Monitoring Configuration Information](#)" on the next page.
- **JMX Console.** Provides a link to the RUM JMX console for configuring RUM parameters, such as URL correlation parameters. For details, see "[JMX Console](#)" on page 154. (For details on URL correlation, see "Correlating Collected Data with Configured Pages" in the BSM Application Administration Guide.)
- **IP Translator.** Used to convert between the internal number used by the engine to represent an IP address and the actual IP address it represents. For details, see "[IP Translator](#)" on page 154.
- **Time Converter.** Used to convert a date and time to an internal number used by the engine machine to represent this value. You can also convert the number used by the engine machine to the date and time it represents. For details, see "[Time Converter](#)" on page 154.
- **Page Name Cache.** Used to manage the Page Name cache of discovered pages and to delete such names that are no longer relevant. For details, see "[Page Name Cache](#)" on page 154.
- **Mobile Application Instrumentation.** Used to instrument Android APKs for monitoring mobile applications. For details, see "[Mobile Application Instrumentation](#)" on page 156.

Monitoring Configuration Information

The Engine Configuration page displays general configuration data of the applications, end-users, events, pages, probes, transactions, and engine that have been configured for monitoring by RUM in End User Management Administration.

Click the **Sync All Configuration** button, located at the top of the Engine Configuration page, to force the RUM Engine to reload the RUM configuration from BSM.

You display the data type you want to see by selecting it from the drop-down menu located at the top left corner of the page and clicking **Generate**.

This section includes the following topics:

- ["Applications" below](#)
- ["End Users" on the next page](#)
- ["Events" on the next page](#)
- ["Pages" on page 150](#)
- ["Probes" on page 151](#)
- ["Transactions" on page 151](#)
- ["Engine Settings" on page 152](#)
- ["Transaction Snapshot Mode" on page 153](#)

Applications

When you select applications as the data type to be displayed, the following information about the configured applications is displayed:

Column	Description
ID	An internal ID number allocated by BSM.
Is Application enabled	True or False – as configured in End User Management Administration.
Name	The name of the application as configured in End User Management Administration.
Type	The application type as configured in End User Management Administration.
Probes which monitor the application	The IP addresses and names of the probes configured in End User Management Administration to monitor the application.

You can filter the data displayed on the **Name** column. The filter is case sensitive.

For information on configuring applications for monitoring, see "RUM Application Configuration Wizard" in the BSM Application Administration Guide.

End Users

When you select end users as the data type to be displayed, the following information about the configured end users is displayed:

Column	Description
ID	An internal ID number allocated by BSM.
Is End User enabled	True or False – as configured in End User Management Administration.
Name	The name of the end-user group as configured in End User Management Administration.
Description	The description of the end-user group as configured in End User Management Administration.
Is Monitored (for collection)	True or False – use host name resolution as configured in End User Management Administration.

You can filter the data displayed on the **Name** column. The filter is case sensitive.

For information on configuring end-user groups for monitoring, see "Add End User Group with RUM Configuration Dialog Box" in the BSM Application Administration Guide.

Events

When you select events as the data type to be displayed, the following information about the configured events is displayed:

Column	Description
ID	An internal ID number allocated by BSM.
Is Event enabled	True or False – as configured in End User Management Administration.
Name	The name of the event as configured in End User Management Administration.
Event type	The event type as configured in End User Management Administration.
Report As Error	True or False – as configured in End User Management Administration.

Column	Description
Create Snapshot	True or False – as configured in End User Management Administration.
Collection Session Snapshot	True or False – as configured in End User Management Administration.

Note: Defining events and snapshots has an effect on RUM capacity. For more information on RUM capacity, see the Real User Monitor Sizing Guide.

You can filter the data displayed on the **Name** column. The filter is case sensitive.

For information on configuring events for monitoring, see "RUM Administration User Interface" in the BSM Application Administration Guide.

Pages

When you select pages as the data type to be displayed, the following information about the configured pages is displayed:

Column	Description
Page ID	An internal ID number allocated by BSM.
Is Page Enabled	True or False – as configured in End User Management Administration.
Page Name	The name of the page as configured in End User Management Administration.
Application	The name of the application in which the page is included.
Description	The description of the page as configured in End User Management Administration.
Monitored Type	The monitoring condition as configured in End User Management Administration. The possible conditions are: 1 = Always 2 = Never 3 = Only as part of a transaction
Page Type	Currently not used
Page Time Threshold	The page time threshold, in milliseconds, as configured for the page in End User Management Administration.
Server Time Threshold	The server time threshold, in milliseconds, as configured for the page in End User Management Administration.

Column	Description
Availability Threshold	The availability threshold, in percent, configured for the page in End User Management Administration.
Timeout	The amount of time, in milliseconds, after which the page is considered to have timed out, as configured for the page in End User Management Administration.
Page URL	The URL of the page as configured in End User Management Administration.

You can filter the data displayed on the **Page Name** column. The filter is case sensitive.

For information on configuring pages for monitoring, see "Action Dialog Box" in the BSM Application Administration Guide.

Probes

When you select probes as the data type to be displayed, the following information about the configured probes is displayed:

Column	Description
ID	An internal ID number allocated by BSM.
Is probe enabled	True or False – as configured in End User Management Administration.
IP	The IP address of the probe as configured in End User Management Administration.
Login username	The user name for logging in to the probe as configured in End User Management Administration.
Name	The name of the probe as configured in End User Management Administration.
Description	The description of the probe as configured in End User Management Administration.

You can filter the data displayed on the **Name** column. The filter is case sensitive.

For information on configuring probes for monitoring, see "Installing RUM" in the Real User Monitor Installation and Upgrade Guide.

Transactions

When you select transactions as the data type to be displayed, the following information about the configured transactions is displayed:

Column	Description
Trx ID	An internal ID number allocated by BSM.
Is Trx Enabled	True or False – as configured in End User Management Administration.
Trx Name	The name of the transaction as configured in End User Management Administration.
Application	The name of the application in which the transaction is included.
Description	The description of the transaction as configured in End User Management Administration.
Transaction report page	The name of the page which, if reached, causes the transaction to be reported as unavailable, for transaction errors or timeouts within a session.
Refresh behavior	The page instance that is measured in case of a refresh, as configured in End User Management Administration. The possible instances are: 0 = First page 1 = Last page
Timeout	The amount of time, in milliseconds, of inactivity since the last page download in a transaction, that causes the transaction to time out, as configured for the transaction in End User Management Administration.
Gross Time Threshold	The total transaction time threshold (download time + think time), in milliseconds, as configured for the transaction in End User Management Administration.
Net Time Threshold	The net transaction time threshold, in milliseconds, for the pages included in the transaction, as configured in End User Management Administration.
Server Time Threshold	The server time threshold, in milliseconds, as configured for the transaction in End User Management Administration.
Availability Threshold	The availability threshold, in percent, as configured for the transaction in End User Management Administration.
Trx pages	The names of the pages included in the transaction, as configured in End User Management Administration.

You can filter the data displayed on the **Trx Name** column. The filter is case sensitive.

For information on configuring transactions for monitoring, see "Business Transaction RUM Configuration Page" in the BSM Application Administration Guide.

Engine Settings

When you select engine settings as the data type to be displayed, the following information about the configured engine is displayed:

Column	Description
Engine Name	Name of the engine as configured in End User Management Administration.
Profile ID	Internal BSM profile ID.
Profile Name	Internal BSM profile name.
Engine ID	Internal BSM engine ID.
Customer Name	Always default client.
Snapshot on Error Enabled	True or False – as configured in End User Management Administration.
Snapshot page number	Number of pages for which to collect snapshot on error, as configured in End User Management Administration.
Is monitoring default application	The applications that are monitored by the engine, as configured in End User Management Administration. 0 = configured applications only 1 = all applications
Default Application Name	Name of default application (for all applications not configured in End User Management Administration).
Default HTTP Port	Default http port of engine machine.
Default HTTPS Port	Default https port of engine machine.
Default Application ID	Internal BSM application ID.

Transaction Snapshot Mode

When you select transaction snapshot mode as the data type to be displayed, the following information about the transaction snapshot mode is displayed:

Column	Description
Name	The application name.
ID	Internal BSM application ID.
Snapshot mode on	True or False – as configured in End User Management Administration.

JMX Console

This option provides a link to the RUM JMX console, which you use to view and configure RUM parameters, for example, URL correlation parameters. For details on configuring URL correlation parameters, see "Correlating Collected Data with Configured Pages" in the BSM Application Administration Guide. For details on working with the JMX console, see ["Using the JMX Console to Configure the RUM Engine" on page 161](#).

IP Translator

You use the IP Translator tool to convert an IP address into different formats. The formats to which the IP data is translated are:

- **Host name.** The name of the machine to which the IP address is assigned.
- **Signed integer.** An internal, signed number used in RUM data samples.
- **Unsigned integer.** An internal, unsigned number used in RUM data samples.
- **Dotted-format IP address.** The standard, dotted-decimal notation for the IP address.

You select one of the formats and enter the source data you want to convert to the other formats, or you select the **Resolve Engine host** option to use the IP address of the current RUM Engine machine as the source data.

Click **Submit** to translate the source data to all the other formats.

Time Converter

You use the Time Converter tool to convert a time into different formats. The formats to which the time is converted are:

- The number of milliseconds since January 1, 1970 – an internal number used by the RUM Engine.
- Time in Greenwich Mean Time.
- Time in the time zone set for the RUM Engine machine.

You select one of the formats and enter the source data you want to convert to the other formats, or you select the **Current time** option to use the current time as the source data for conversion.

Click **Submit** to convert the source data to all the other formats.

Page Name Cache

You use the Page Name Cache tool to display applications and the page names that have been created for discovered pages included in the application. You can delete page names that are no longer relevant (for example, if you have changed the page name rules for an application so that new and different

pages are discovered) and thereby reduce the amount of data stored in the RUM database. For details on configuring names for discovered pages, see ["Configuring Meaningful Page Names" on page 179](#).



This section includes the following topics:

- ["Application Selection Page" below](#)
- ["Application Cached Page Names Page" below](#)

Application Selection Page

When you select the Page Name Cache tool, the Application Selection page opens, listing all the applications that you configured for the RUM Engine in End User Management Administration. For information on configuring applications in End User Management Administration, see "Real User Monitor Application Configuration Wizard" in the BSM Application Administration Guide.


For each application, you can perform the following actions:

- Click the **Delete** button  to delete all the discovered page names for the application.
- Click the **Drilldown** button  to display the Application Cached Page Names page (for details, see ["Application Cached Page Names Page" below](#)) on which you can see all the discovered page names for the application and delete them selectively.


Note: The buttons are disabled for applications that do not have any discovered page names assigned to them.

Application Cached Page Names Page

You access the Application Cached Page Names page by clicking the **Drilldown** button  in the Application Selection page. The Application Cached Page Names page lists all the discovered page names that have been created for an application. To delete pages, select the check box next to the pages you want to delete and click the **Delete** button .

Note: You can select all page names, clear all page names, or invert your selection using the **Select** buttons .

Click **Back** at the top of the page to return to the Application Selection page.

From either the Application Selection page or the Application Cached Page Names page, click the **Refresh** button  to redisplay the pages.

Mobile Application Instrumentation

The RUM mobile solution enables you to monitor mobile applications through apps on a user's mobile device and sends the collected data from the app directly to the RUM Client Monitor Probe. For details, see ["Using the RUM Mobile Solution to Monitor Mobile Applications" on page 39](#).

You use the Mobile Application Instrumentation page to instrument an Android APK for monitoring a mobile application. (You can also instrument an APK using a command line batch file. For details, see "Instrumenting Mobile Apps for Android" in the Real User Monitor Installation and Upgrade Guide.) The instrumentation is made to the compiled Java classes in the APK and does not modify any source code, as it is done in the post-build stage.

Note: If you select to apply content extraction configuration change at instrumentation time only, during instrumentation the RUM engine will try to update the Static Configuration File with the latest configuration changes before instrumenting the application. If the update fails, a warning message appears telling you to check the configmanager.log for details.

Note: If during instrumentation it is discovered that ACRA crash reporting is already instrumented on your application, the RUM crash reporting will be disabled, the instrumentation will succeed, but a warning message will appear on the console.

User interface elements are described below:

UI Element	Description
APK file	Enter the path and file name of the source APK file that you are instrumenting. You can click Browse to navigate to the relevant file.

UI Element	Description									
Instrument for Production	Select this option to fully sign the APK using a Java keystore file with a private key. If you select this option, configure the following:									
	<table border="1"> <tr> <td data-bbox="331 403 472 583">Application</td> <td data-bbox="472 403 1385 583"> From the drop-down list, select the application configured in BSM to which the monitored data will be associated. Note: Only applications that use the Network for Mobile Application template are displayed in the list. </td> </tr> </table>	Application	From the drop-down list, select the application configured in BSM to which the monitored data will be associated. Note: Only applications that use the Network for Mobile Application template are displayed in the list.							
	Application	From the drop-down list, select the application configured in BSM to which the monitored data will be associated. Note: Only applications that use the Network for Mobile Application template are displayed in the list.								
	<table border="1"> <tr> <td data-bbox="331 583 472 814">RUM Client Monitor Probe URL</td> <td data-bbox="472 583 1385 814"> Enter the URL for the RUM Client Monitor Probe to which monitored data is sent. The format is: https://<RUM Client Monitor Probe host name>:443/<path to the RUM Client Monitor Probe on the host> Note: If no port is specified, port 443 is used by default. </td> </tr> </table>	RUM Client Monitor Probe URL	Enter the URL for the RUM Client Monitor Probe to which monitored data is sent. The format is: https://<RUM Client Monitor Probe host name>:443/<path to the RUM Client Monitor Probe on the host> Note: If no port is specified, port 443 is used by default.							
	RUM Client Monitor Probe URL	Enter the URL for the RUM Client Monitor Probe to which monitored data is sent. The format is: https://<RUM Client Monitor Probe host name>:443/<path to the RUM Client Monitor Probe on the host> Note: If no port is specified, port 443 is used by default.								
<table border="1"> <tr> <td data-bbox="331 814 472 1514">Application Signing</td> <td data-bbox="472 814 1385 1514"> Leave the following fields blank if you want to sign the APK later. You can sign the APK later using Java's jarsigner.exe tool (see "Signing an APK using Java's jarsigner.exe Tool" on page 159). <table border="1" data-bbox="483 947 1377 1499"> <tr> <td data-bbox="483 947 740 1127">Keystore file</td> <td data-bbox="740 947 1377 1127"> The path and name of the keystore file. You can click Browse to navigate to the relevant file. If you do not configure a keystore file, the APK will not be signed. </td> </tr> <tr> <td data-bbox="483 1127 740 1220">Keystore password</td> <td data-bbox="740 1127 1377 1220"> A password for the keystore, if configured. </td> </tr> <tr> <td data-bbox="483 1220 740 1409">Key alias</td> <td data-bbox="740 1220 1377 1409"> The alias to the private key entry in the keystore. <div style="background-color: #f0f0f0; padding: 5px;">Note: This field is mandatory if you configure a keystore file.</div> </td> </tr> <tr> <td data-bbox="483 1409 740 1499">Key password</td> <td data-bbox="740 1409 1377 1499"> A password for the private key entry in the keystore, if configured. </td> </tr> </table> </td> </tr> </table>	Application Signing	Leave the following fields blank if you want to sign the APK later. You can sign the APK later using Java's jarsigner.exe tool (see " Signing an APK using Java's jarsigner.exe Tool " on page 159). <table border="1" data-bbox="483 947 1377 1499"> <tr> <td data-bbox="483 947 740 1127">Keystore file</td> <td data-bbox="740 947 1377 1127"> The path and name of the keystore file. You can click Browse to navigate to the relevant file. If you do not configure a keystore file, the APK will not be signed. </td> </tr> <tr> <td data-bbox="483 1127 740 1220">Keystore password</td> <td data-bbox="740 1127 1377 1220"> A password for the keystore, if configured. </td> </tr> <tr> <td data-bbox="483 1220 740 1409">Key alias</td> <td data-bbox="740 1220 1377 1409"> The alias to the private key entry in the keystore. <div style="background-color: #f0f0f0; padding: 5px;">Note: This field is mandatory if you configure a keystore file.</div> </td> </tr> <tr> <td data-bbox="483 1409 740 1499">Key password</td> <td data-bbox="740 1409 1377 1499"> A password for the private key entry in the keystore, if configured. </td> </tr> </table>	Keystore file	The path and name of the keystore file. You can click Browse to navigate to the relevant file. If you do not configure a keystore file, the APK will not be signed.	Keystore password	A password for the keystore, if configured.	Key alias	The alias to the private key entry in the keystore. <div style="background-color: #f0f0f0; padding: 5px;">Note: This field is mandatory if you configure a keystore file.</div>	Key password	A password for the private key entry in the keystore, if configured.
Application Signing	Leave the following fields blank if you want to sign the APK later. You can sign the APK later using Java's jarsigner.exe tool (see " Signing an APK using Java's jarsigner.exe Tool " on page 159). <table border="1" data-bbox="483 947 1377 1499"> <tr> <td data-bbox="483 947 740 1127">Keystore file</td> <td data-bbox="740 947 1377 1127"> The path and name of the keystore file. You can click Browse to navigate to the relevant file. If you do not configure a keystore file, the APK will not be signed. </td> </tr> <tr> <td data-bbox="483 1127 740 1220">Keystore password</td> <td data-bbox="740 1127 1377 1220"> A password for the keystore, if configured. </td> </tr> <tr> <td data-bbox="483 1220 740 1409">Key alias</td> <td data-bbox="740 1220 1377 1409"> The alias to the private key entry in the keystore. <div style="background-color: #f0f0f0; padding: 5px;">Note: This field is mandatory if you configure a keystore file.</div> </td> </tr> <tr> <td data-bbox="483 1409 740 1499">Key password</td> <td data-bbox="740 1409 1377 1499"> A password for the private key entry in the keystore, if configured. </td> </tr> </table>	Keystore file	The path and name of the keystore file. You can click Browse to navigate to the relevant file. If you do not configure a keystore file, the APK will not be signed.	Keystore password	A password for the keystore, if configured.	Key alias	The alias to the private key entry in the keystore. <div style="background-color: #f0f0f0; padding: 5px;">Note: This field is mandatory if you configure a keystore file.</div>	Key password	A password for the private key entry in the keystore, if configured.	
Keystore file	The path and name of the keystore file. You can click Browse to navigate to the relevant file. If you do not configure a keystore file, the APK will not be signed.									
Keystore password	A password for the keystore, if configured.									
Key alias	The alias to the private key entry in the keystore. <div style="background-color: #f0f0f0; padding: 5px;">Note: This field is mandatory if you configure a keystore file.</div>									
Key password	A password for the private key entry in the keystore, if configured.									
<table border="1"> <tr> <td data-bbox="331 1514 472 1803">Add Access Network State permission to the application</td> <td data-bbox="472 1514 1385 1803"> Select this check box to enable the APK to determine and report the type of user connection (WiFi/Cellular). </td> </tr> </table>	Add Access Network State permission to the application	Select this check box to enable the APK to determine and report the type of user connection (WiFi/Cellular).								
Add Access Network State permission to the application	Select this check box to enable the APK to determine and report the type of user connection (WiFi/Cellular).									

UI Element	Description	
Allow access to http content	Select one of the following to define when to apply mobile device configuration changes performed in BSM Admin to the mobile devices. This includes change to parameters, user name, or un hiding query parameters.	
	Apply any configuration change to the mobile device even after instrumentation	Select this option to enable the application to send any change in content extraction to the mobile device. Changes to the configuration can be performed even after the application is deployed on the mobile device.
	Apply content extraction configuration change at instrumentation time only	Select this option to enable the application to extract content configuration only when instrumenting the application. To apply a configuration change, you need to repeat the instrumentation.
	Do not allow content extraction	Select this option to disable the application from using any extracted content (parameter settings, username detection, or allowed POST parameters) configured for it in BSM, when the application runs.

UI Element	Description		
Instrument for Testing	Select this radio button to sign the APK with a self-signed debug certificate. Note: This is sufficient for testing the APK, but not for uploading it to the Google Play store. If you select this option, configure the following:		
	<table border="1"> <tr> <td data-bbox="331 478 472 653">Application</td> <td data-bbox="472 478 1385 653"> From the drop-down list, select the application configured in BSM to which the monitored data will be associated. Note: Only applications that use the Network for Mobile Application template are displayed in the list. </td> </tr> </table>	Application	From the drop-down list, select the application configured in BSM to which the monitored data will be associated. Note: Only applications that use the Network for Mobile Application template are displayed in the list.
	Application	From the drop-down list, select the application configured in BSM to which the monitored data will be associated. Note: Only applications that use the Network for Mobile Application template are displayed in the list.	
<table border="1"> <tr> <td data-bbox="331 653 472 884">RUM Client Monitor Probe URL</td> <td data-bbox="472 653 1385 884"> Enter the URL for the RUM Client Monitor Probe to which monitored data is sent. The format is: https://<RUM Client Monitor Probe host name>:443/<path to the RUM Client Monitor Probe on the host> Note: If no port is specified, port 443 is used by default. </td> </tr> </table>	RUM Client Monitor Probe URL	Enter the URL for the RUM Client Monitor Probe to which monitored data is sent. The format is: https://<RUM Client Monitor Probe host name>:443/<path to the RUM Client Monitor Probe on the host> Note: If no port is specified, port 443 is used by default.	
RUM Client Monitor Probe URL	Enter the URL for the RUM Client Monitor Probe to which monitored data is sent. The format is: https://<RUM Client Monitor Probe host name>:443/<path to the RUM Client Monitor Probe on the host> Note: If no port is specified, port 443 is used by default.		
Instrument for Offline Testing and Data Collection	Select this option not to sign the APK after instrumentation. You can test the application offline and collect data locally only. Note: The APK must be fully signed before you can upload it to the Google Play store. If you select this option, configure the following:		
	<table border="1"> <tr> <td data-bbox="331 1083 472 1358">Store monitored data locally</td> <td data-bbox="472 1083 1385 1358"> Select this check box to configure the APK not to send collected network data to the probe and to store it locally in the application folder on the mobile device. This data includes the POST content of requests, which can assist you in defining extracted parameters for the application in BSM. For details on extracted parameters, see "Parameter Extraction Area" in the Real User Monitor Application General Page in the BSM Application Administration Guide. </td> </tr> </table>	Store monitored data locally	Select this check box to configure the APK not to send collected network data to the probe and to store it locally in the application folder on the mobile device. This data includes the POST content of requests, which can assist you in defining extracted parameters for the application in BSM. For details on extracted parameters, see "Parameter Extraction Area" in the Real User Monitor Application General Page in the BSM Application Administration Guide.
Store monitored data locally	Select this check box to configure the APK not to send collected network data to the probe and to store it locally in the application folder on the mobile device. This data includes the POST content of requests, which can assist you in defining extracted parameters for the application in BSM. For details on extracted parameters, see "Parameter Extraction Area" in the Real User Monitor Application General Page in the BSM Application Administration Guide.		

Signing an APK using Java's jarsigner.exe Tool

After generating an unsigned instrumented APK, you can sign the APK using Java's jarsigner.exe tool.

1. From a cmd window, enter:

```
jarsigner.exe -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore <KEYSTORE_FILE_FULL_PATH> -storepass <KEYSTORE_PASSWORD> -keypass <KEY_PASSWORD> <APK_FILE_FULL_PATH> <ALIAS>
```

Parameter	Description
KEYSTORE_FILE_FULL_PATH	The path to the keystore file
KEYSTORE_PASSWORD	The password to the keystore
KEY_PASSWORD	The password for the private key entry in the keystore
APK_FILE_FULL_PATH	The full path for the APK file
ALIAS	The alias to the private key entry in the keystore.

Note: If you have trouble uploading your mobile application to the app store due to a signing problem, re-sign the application using the Java 6 jarsigner.exe tool.

2. (Optional) Use Java's zipalign utility for memory optimization. From a cmd window, enter:

```
zipalign.exe -f -v 4 <SOURCE_APK_FILE_FULL_PATH> <TARGET_APK_FILE_FULL_PATH>
```

Parameter	Description
SOURCE_APK_FILE_FULL_PATH	The full path to the source APK file
TARGET_APK_FILE_FULL_PATH	The full path to the target APK file

Chapter 9: Using the JMX Console to Configure the RUM Engine

You configure RUM Engine settings via the JMX console.

Note: You also use the web console to configure the engine, monitor system health, and use a number of diagnostic tools. For details, see ["Using the RUM Web Console" on page 47](#).

This chapter includes the following topics:

- ["Using the RUM JMX Console" below](#)
- ["URL Correlation Parameters" on page 167](#)

Using the RUM JMX Console

You use the RUM Engine JMX console to view and configure RUM settings.

This section includes the following topics:

- ["Accessing the JMX Console" below](#)
- ["Setting URL Correlation Parameters" on the next page](#)
- ["Configuring RUM Aggregation" on the next page](#)
- ["Configuring the Samples Rate" on page 164](#)
- ["Configuring the Amount of Unsent Sample Data to Store in RUM" on page 165](#)
- ["Configuring the Classification Type" on page 165](#)

Accessing the JMX Console

Via the JMX console, you can view and configure RUM parameters, view statistics for RUM modules and services, and view and configure JBoss components.

Once you start the RUM Engine after installation, you can access the RUM Engine JMX console by launching the RUM Engine web console and choosing **JMX Console** from the Tools drop-down menu. To access a specific area of the JMX console for an individual RUM module, select **Advanced Settings** from the **Configuration** drop-down menu in the RUM Engine web console and then click the links for the module you want to view. For details on the RUM Engine web console, see ["Using the RUM Web Console" on page 47](#).

When you access the JMX console, you are prompted for a user name and password. Enter the JMX console authentication credentials (if you do not have these credentials, contact your system administrator).

Note: You can access the RUM Engine JMX console from a different machine by launching a web browser and typing the following: `http://<HP Real User Monitor engine machine name>:8180/jmx-console`

Caution: Changing any of the JMX configuration settings can cause RUM to malfunction. We recommend that you do not change any of these settings.

Setting URL Correlation Parameters

You can configure a number of parameters used by RUM when correlating recorded URLs with URLs you have configured for monitoring. For details on URL correlation, see "Correlating Collected Data with Configured Pages" in the BSM Application Administration Guide. For details on configuring URLs for monitoring, see "Real User Monitor Application Configuration Wizard" in the BSM Application Administration Guide.

Some of the URL correlation parameters are set using the RUM JMX console. For details on changing URL correlation parameters via the RUM JMX console, see "[Setting URL Correlation Parameters Via the JMX Console](#)" on page 168.

Configuring RUM Aggregation

RUM pre-aggregates a number of the data samples it sends to BSM. For details on BSM aggregation, see "Data Aggregation" in the BSM Application Administration Guide. For details on RUM pre-aggregation, see "Aggregating Real User Monitor Data" in the BSM User Guide.

You can change the RUM default aggregation periods via the JMX console.

This section includes the following topics:

- "[Pre-aggregated Data Sample Types](#)" on the next page
- "[Changing Default Aggregation Periods](#)" on page 164

Pre-aggregated Data Sample Types

The following table shows the data sample types that are pre-aggregated by RUM, the JMX service in which they are configured, their attribute and parameter names, and the default aggregation time period:

Data Sample Type	JMX Console Rum.modules Service Name	Attribute in JMX Service	Parameter Name	Default Aggregation Period in Milliseconds
Action	StatisticsMgrConf	Properties	aggregator.actions.interval	300,000
Slow End User			aggregator.domains.interval	300,000
Missing Component			aggregator.MissingComponents.interval	300,000
Slow Action			aggregator.SlowActions.interval	300,000
Slow Location			aggregator.slowlocations.interval	300,000
Top Location			aggregator.toplocations.interval	360,000
Top End User			aggregator.TopDomains.interval	360,000
Top Action			aggregator.TopActions.interval	360,000
Most Error Action			aggregator.actionerrorevent.interval	300,000
Application Statistics			aggregator.applications.interval	300,000
Transaction			aggregator.transaction.interval	300,000
TCP Application Statistics			aggregator.tcpapplications.interval	300,000
Undefined End User (Domain)			aggregator.domains.interval	300,000

Changing Default Aggregation Periods

You can change the default aggregation periods using the JMX console.

To change the RUM default aggregation periods via the JMX console:

1. Access the JMX console by choosing JMX Console from the Tools drop-down menu in the RUM web console, or by using the following URL in your web browser:

```
http://<HP Real User Monitor engine machine name>:8180/jmx-console
```

When prompted, enter the JMX console authentication credentials (if you do not have these credentials, contact your system administrator).

2. In the JMX Agent View, scroll down to the **RUM.modules** section and click the applicable service (**service=StatisticsMgrConf**).
3. Change the aggregation period as required. To change parameter values in the **Properties** attribute, enter the parameter name and the aggregation period (in milliseconds) you want to change under the commented lines (the lines beginning with #) in the format:

```
attribute name=aggregation period
```

For example, to change the aggregation period of the Action sample type to 10 minutes, enter:

```
aggregator.actions.interval=600000
```

4. Click the **Apply Changes** button to save the change.
5. Activate the change by clicking the **Invoke** button for the **deployConfiguration** operation.

Caution: Changing the default aggregation periods can significantly affect the amount of data sent by RUM to BSM. We recommend that you do not change the default aggregation periods.

Configuring the Samples Rate

The maximum burst rate controls the number of samples per second that the RUM Engine can send to BSM. The default setting is 300. You can increase the maximum burst rate to allow more samples to be sent per second, provided that BSM is capable of handling the increased number. You can see the state of the flow of samples between RUM and BSM by looking at the **Publisher burst state** in RUM system health. For details on RUM system health, see "[Monitoring the Health of RUM Components](#)" on page 51.

To configure the maximum burst rate:

1. Access the JMX console by choosing **JMX Console** from the Tools drop-down menu in the RUM web console, or by using the following URL in your web browser:

`http://<HP Real User Monitor engine machine name>:8180/jmx-console`

When prompted, enter the JMX console authentication credentials (if you do not have these credentials, contact your system administrator).

2. In the JMX Agent View, scroll down to the **RUM.modules** section and click **service=PublisherSettings**.
3. In the **BurstControlMaxSamples** parameter, change the value to the maximum number of samples required.
4. Click the **Apply Changes** button to save the change.
5. Click the **Invoke** button for the **applyAttributeChanges** operation to activate the change.

Configuring the Amount of Unsent Sample Data to Store in RUM

By default, 1000 chunks of samples data are stored in RUM for sending to BSM. You can increase the number of chunks of data stored (providing you have sufficient disk space) to avoid data loss when BSM cannot receive data from RUM. For example, you might want to increase the amount of data stored by RUM during a planned downtime in BSM. Bear in mind that when a lot of data has been stored in RUM, it can take a long time for all of it to be sent to BSM, which might cause a delay in seeing real time data. If you increase the number of data chunks to store, you should reset it to the original number once BSM is running and all the stored data has been transmitted to it.

To increase the maximum number of data chunks stored:

1. Access the JMX console by choosing **JMX Console** from the Tools drop-down menu in the RUM web console, or by using the following URL in your web browser:

`http://<HP Real User Monitor engine machine name>:8180/jmx-console`

When prompted, enter the JMX console authentication credentials (if you do not have these credentials, contact your system administrator).

2. In the JMX Agent View, scroll down to the **RUM.modules** section and click **service=PublisherSettings**.
3. In the **MaxChunksInQueue** parameter, change the value to the maximum number of chunks required.
4. Click the **Apply Changes** button to save the change.
5. Click the **Invoke** button for the **applyAttributeChanges** operation to activate the change.

Configuring the Classification Type

The classification algorithm groups similar, unconfigured actions under one name (a generic descriptor) and aggregates their measurements to obtain values for the descriptor. The aggregated actions can be

viewed in the RUM Action Summary report in BSM. For HTTP-Web based protocols, there are two methods of classification:

- The default method groups actions based on both URLs and parameters.
- An alternative method groups actions based on URL paths only. This method is best suited for applications with changing path or parameter names.

To configure an application to use this alternative classification method, you configure the RUM template on which the application is based. RUM templates have predefined values for the most common, recommended configuration settings for a specific protocol and are used to simplify the creation of RUM applications in BSM. For details on configuring the templates to use the alternative classification method, see ["To configure the RUM templates that classify URLs based only on their paths:" on the next page.](#)

The following examples show the generic descriptor created by each classification method for a group of monitored URLs:

Example 1

Monitored URLs	Generic Descriptor Created by the Default Classification Method (using both URLs and parameters)	Generic Descriptor Created by the Alternative Classification Method (using URL paths only)
http://site/a/b/c?x=1&y=10 http://site/a/b/c?x=2&y=20 http://site/a/b/c?x=3&y=30	http://site/a/b/c?x=*&y=*	http://site/a/b/c

Example 2

Monitored URLs	Generic Descriptor Created by the Default Classification Method (using both URLs and parameters)	Generic Descriptor Created by the Alternative Classification Method (using URL paths only)
http://site/a/b/c1?x=1&y=10 http://site/a/b/c2?x=2&y=20 http://site/a/b/c3?x=3&y=30	http://site/a/b/c1?x=*&y=* http://site/a/b/c2?x=*&y=* http://site/a/b/c3?x=*&y=*	http://site/a/b/*

You can configure RUM templates based only on the HTTP-Web protocol to use the alternative classification method using URL paths only. In BSM, you can view a template's protocol in the list of protocols provided when you create a new RUM application for monitoring, or in the Real User Monitor Application General Page when viewing an existing application.

Note: The default classification method is used for applications using RUM templates based on the HTTP-Web protocol that are not configured to use the alternative classification method. However, if the default method cannot produce satisfactory results, the alternative method is then automatically used.

To configure the RUM templates that classify URLs based only on their paths:

1. Access the JMX console by choosing **JMX Console** from the Tools drop-down menu in the RUM web console, or by using the following URL in your web browser:

```
http://<HP Real User Monitor engine machine name>:8180/jmx-console
```

When prompted, enter the JMX console authentication credentials (if you do not have these credentials, contact your system administrator).

2. In the JMX Agent View, scroll down to the **RUM.modules** section and click **service=ResolverTrieClassificationSettings**.
3. In the **adminTemplatesOfTrieClassificationAlg** parameter, enter a comma separated list of the RUM template IDs for which you want classification to be made on URL paths only.

Note: To determine a template's ID, edit the xml file for the relevant template and under the **<metadata>** tag, locate the value for **template_id**. By default, template configuration files are located on the BSM Gateway Server in the **<HPBSM>\conf\rum_templates** directory.

4. Click the **Apply Changes** button to save the change.

URL Correlation Parameters

After the RUM Engine has been installed and started, you can configure a number of parameters to determine how RUM correlates recorded URLs with web pages you have configured for monitoring in End User Management Administration.

This section includes the following topics:

- ["Setting URL Correlation Parameters Via the JMX Console" on the next page](#)
- ["Correlating Session ID Parameters" on page 169](#)

Setting URL Correlation Parameters Via the JMX Console

You can change the default setting of a number of parameters used by RUM when correlating recorded URLs with URLs you have configured for monitoring. For details on URL correlation, see "Correlating Collected Data with Configured Pages" in the BSM Application Administration Guide. For details on configuring URLs for monitoring, see "Real User Monitor Application Configuration Wizard" in the BSM Application Administration Guide.

You can configure the following parameters for URL correlation in the JMX console:

- **adaptIndexurl.** By default, RUM considers URLs with a suffix of **index.html** (and other suffixes that are configured in the `urlIndexStrings` parameter) to be same as the root URL. For example, `http://www.hp.com/index.html` is considered to be the same as `http://www.hp.com/`. To instruct RUM to consider all suffixes as being different from the root URL, change this parameter to **False**.
- **urlIndexStrings.** URL suffixes configured in this parameter are considered to be the same as the root URL, if the **adaptIndexurl** parameter is set to **True**. For example, if the suffix **index.html** is configured, then `http://www.hp.com/index.html` is considered to be the same as `http://www.hp.com/`. By default, the suffix **index.html** is configured in this parameter. To add additional suffixes, add them to the string separated by a semicolon (;). The last suffix in the string must also be followed by a semicolon. For example, `;/index.html;/index.aspx;`

Note: For the **urlIndexStrings** parameter to be active, the **adaptIndexurl** parameter must be set to **True**.

The index strings in the `urlIndexStrings` parameter are considered as being identical for all URLs. For example, if `;/index.html;` is configured in the **urlIndexStrings** parameter then `http://www.hp.com/` and `http://www.hp.com/index.html` are considered as being identical, `http://www.hp-int.com/` and `http://www.hp-int.com/index.html` are considered as being identical, and so forth.

Changing the **urlIndexStrings** parameter requires the RUM Engine Resolver to be restarted. For details, see ["To restart the RUM Engine Resolver" on the next page](#).

- **adaptCaseSensitive.** By default, RUM URL correlation is case-insensitive, so that a recorded URL such as `http://www.hp.com/rumEnginePage.html` is correlated with the configured URL `http://www.hp.com/rumenginepage.html`. To instruct RUM to use case-sensitive URL correlation (for all but the host and protocol parts of a URL), you set this parameter to **False**.
- **basicAuthentication.** By default, RUM ignores basic authentication when performing URL correlation. For example, the recorded URL `http://bob:my_password@www.hp.com` is correlated with the configured URL `http://www.hp.com`. To instruct RUM to consider basic authentication when performing URL correlation, you set this parameter to **False**.

To change the default setting of a URL correlation parameter in the JMX console

1. Access the JMX console by choosing JMX Console from the Tools drop-down menu in the RUM web console, or by using the following URL in your web browser:

```
http://<HP Real User Monitor engine machine name>:8180/jmx-console
```

When prompted, enter the JMX console authentication credentials (if you do not have these credentials, contact your system administrator).

2. In the JMX Agent View, scroll down to the **RUM.modules** section and click **service=ResolverURLMConfig**.
3. In the relevant parameter, change the setting to the required value.
4. Click the **Apply Changes** button.

To restart the RUM Engine Resolver

1. Access the JMX console by choosing JMX Console from the Tools drop-down menu in the RUM web console, or by using the following URL in your web browser:

```
http://<HP Real User Monitor engine machine name>:8180/jmx-console
```

When prompted, enter the JMX console authentication credentials (if you do not have these credentials, contact your system administrator).

2. In the JMX Agent View, scroll down to the **RUM.modules** section and click **service=Resolver**.
3. Scroll down to the **restart** operation and click **Invoke**.

Correlating Session ID Parameters

You can configure specific parameters in recorded URLs to be ignored by RUM when correlating recorded URLs with URLs you have configured for monitoring in End User Management Administration. For details on URL correlation, see "Correlating Collected Data with Configured Pages" in the BSM Application Administration Guide. For details on configuring URLs for monitoring, see "RUM Application Configuration Wizard" in the BSM Application Administration Guide.

If you set a parameter to be ignored by RUM, and the parameter is included in a recorded URL, RUM replaces the contents of that parameter with an asterisk (*). For example, if you set RUM to ignore the **BV_SessionID** and **BV_EngineID** parameters in the following URL:

```
http://www.hp.com/~anand/Ticket_Confirm.jsp?BV_
SessionID=@@@@1812057630.1043567934@@@@&BV_
EngineID=cccdadchgldfmlmcefecehidfhdfdfk.0&value=0000144976
```

The URL is translated as follows:

http://www.hp.com/~anand/Ticket_Confirm.jsp?BV_SessionID=*&BV_EngineID=*&value=0000144976

The parameters to be ignored are defined per application server.

To configure session ID parameters to be ignored

1. Open the **<HP Real User Monitor root directory>\conf\configurationmanager\Application_Server_Types_configuration.xml** file in a text editor.
2. Locate the application server type for which you are configuring the parameters to be ignored. This appears in the format **<AppServer name="app_server_name">**, where `app_server_name` is the name of the application server type. For example, for a Broadvision application server, the entry is:

```
<AppServer name="BroadVision">
```

3. Under the application server name, in the section beginning with the **<DiscardParameters>** tag, is a list of the most common session ID parameters for that application server. You can add and delete parameters to create a list of all the parameters you want RUM to ignore during correlation. Parameters are entered in the format **<parameter>parameter_name</parameter>**, where `parameter_name` is the name of the parameter. For example, for a parameter called `BV_EngineID`, the entry is.

```
<parameter>BV_EngineID</parameter>
```

4. If you want RUM to consider the parameters you enter as a regular expression instead of a string (which is the default), you add **type="regEx"** to the **<DiscardParameters>** tag. For example, **<DiscardParameters type="regEx">**

5. Under the application server name, in the line:

```
<attribute name="enabled">>false</attribute>
```

change **false** to **true**.

6. Save the file and exit the editor.

Chapter 10: RUM Transaction Flow Monitoring

You use RUM transaction flow monitoring to discover the paths through both hardware and software elements, including specific request content, of the pages included in a configured transaction.

This chapter includes the following topics:

- ["RUM Transaction Flow Monitoring Overview" below](#)
- ["RUM Transaction Flow Monitoring User Interface" on the next page](#)

RUM Transaction Flow Monitoring Overview

RUM transaction flow monitoring enables you to run an algorithm for a specific RUM transaction that you configured in End User Management Administration, that tracks and records the progress of the transaction's configured pages through servers, the specific software elements running on the servers, and the specific requests sent to the running software elements.

Using the discovered data, RUM transaction flow monitoring creates a topology flow map of the transaction showing the different hardware and software elements, and also determines action descriptions of commonly repeated patterns in the transaction pages' requests (for example, the same SQL query in which only a specific parameter value may vary in each page request). The discovered data enables you to better understand transactions and helps highlight potential problem areas. For user interface details on configuring RUM transactions, see "Business Transaction RUM Configuration Page" in the BSM Application Administration Guide.

Note: Intermediate pages in a transaction are not tracked by RUM transaction flow monitoring.

In the RUM transaction flow monitoring user interface you can view transaction topology flow maps and can also view and edit the discovered action descriptions. For user interface details, see ["RUM Transaction Flow Monitoring User Interface" on the next page](#). To access RUM transaction flow monitoring, in the RUM web console, select **Configuration > Transaction Management Configuration**. For details on accessing the RUM web console, see ["Accessing the RUM Engine Web Console" on page 47](#).

The data discovered by RUM transaction flow monitoring is sent to BSM, where it is used by Transaction Management as one of multiple data sources for the Aggregated Topology page. The Aggregated Topology is a flow map for a particular BusinessTransaction CI, as well as its associated performance data, from point to point in the flow. RUM transaction flow monitoring contributes to the performance data by supplying metrics based on end user response times. For details, see "Transaction Topology" in the BSM User Guide.

RUM Transaction Flow Monitoring User Interface

To access RUM transaction flow monitoring, in the RUM web console, select **Configuration > Transaction Management Configuration**. For details on accessing the RUM web console, see ["Accessing the RUM Engine Web Console" on page 47](#).

The RUM transaction flow monitoring user interface consists of the following three panes:

- **Enterprise Components.** Includes a tree of the business applications and their transactions that you configured in End User Management Administration, a time frame selector for filtering the data displayed in the Main View pane, and control buttons for starting and stopping the tracking algorithm. For user interface details, see ["Enterprise Components Pane" below](#).
- **Component Properties/Graph Overview.** Includes the following two tabs:
 - **Component Properties.** Displays details of a specific object selected in the topology flow map in the Main View pane.
 - **Graph Overview.** Displays a condensed version of the topology flow map displayed in the Main View pane.




For user interface details, see ["Components Properties/Graph Overview Pane" on the next page](#).

- **Topology View.** Displays the topology flow map or table for a selected transaction. For user interface details, see ["Topology View Pane" on page 174](#).

Enterprise Components Pane

The Enterprise Components pane includes a tree of the business applications and their transactions that you configured in EUM Administration, as well as a time frame filter for selecting the data displayed in the Main View pane and control buttons for starting and stopping the tracking algorithm.

User interface elements are described below:

UI Element	Description
	Refresh. Refreshes the display in the Main View pane.
	Start Algorithm. Starts the RUM transaction flow monitoring discovery algorithm for the selected transaction in the tree.
	Stop Algorithm. Stops the RUM transaction flow monitoring discovery algorithm for the selected transaction in the tree.
<Time frame>	Select the type of time period for which to display data in the Main View pane—variable or fixed. Configure the actual time frame settings in the Time Frame element.

UI Element	Description
Component Tree	A hierarchical tree of the applications to which the RUM Engine is assigned, and their configured transactions.
Time Frame	<p>The time frame settings for which data is displayed in the Main View pane. Configure the following settings:</p> <ul style="list-style-type: none"> • Fixed time frame: <ul style="list-style-type: none"> ■ From. Select the starting date and time ■ To. Select the ending date and time • Variable time frame: <ul style="list-style-type: none"> ■ Last. Select the number of <Time units> prior to the current date and time from which to start displaying data. ■ <Time units>. Select seconds, minutes, hours, or days. <p>Note: The starting and ending dates and times are updated and displayed according to the selections you make.</p>


Components Properties/Graph Overview Pane

This pane displays details of a specific object (server or communication channel) selected in the Topology View pane, or a condensed version of the topology flow map displayed in the Topology View pane, according to the selected tab. The name of the pane changes according to both the selected tab and the object selected in the topology flow map in the Main View pane. The valid names are:

- **Server Component Properties.** When the Component Properties tab is selected and a server in the topology flow map is selected.
- **Communication Channel Properties.** When the Component Properties tab is selected and a communication channel in the topology flow map is selected.
- **Graph Overview.** When the Graph Overview tab is selected.

Component Properties Tab

User interface elements are described below:

UI Element	Description
	Refresh. Refreshes the data displayed in the table.

UI Element	Description
Attribute	The name of the attributes of the selected object in the topology flow map.
Value	The value of the attributes of the selected object in the topology flow map.

Graph Overview Tab

This tab displays a condensed version of the topology flow map in the Main View pane.

Topology View Pane

This pane displays the topology flow map for a selected transaction, which you can view either as a graph or as a table (pattern tree).




This section includes the following topics:





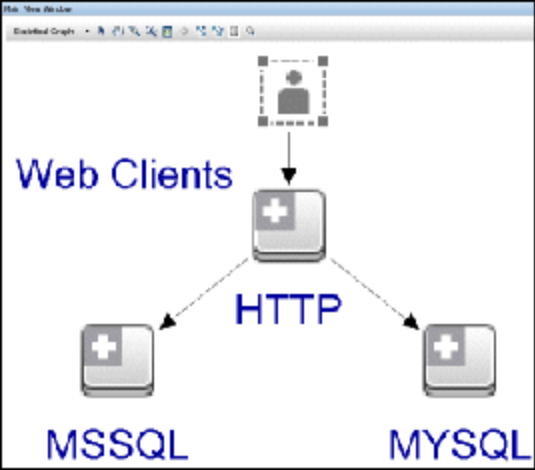
- ["Topology Map - Statistical Graph" below](#)
- ["Topology Map - Pattern Tree" on page 177](#)
- ["Select Server Dialog Box" on page 177](#)
- ["Action Description Statistics Dialog Box" on page 178](#)
- ["Add Transaction Pattern Element Dialog Box" on page 178](#)


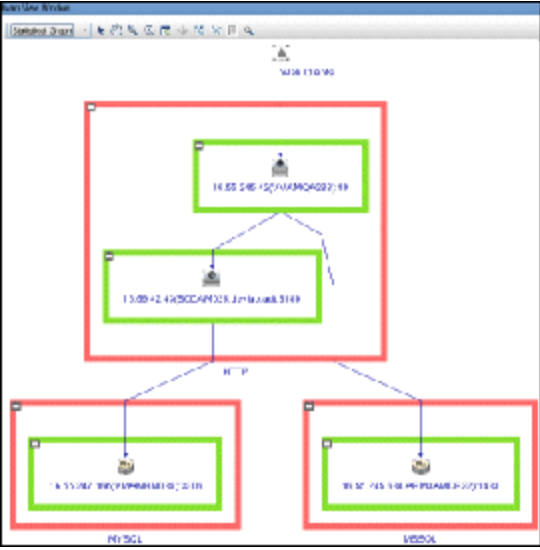

Topology Map - Statistical Graph

This tab displays a selected transaction's topology flow map as a graph.

User interface elements are described below:

UI Element	Description
	Select. Enables selecting a component in the topology flow map. Note: This button is selected by default on entering the topology flow map.
	Pan. Pans the topology flow map. You pan by holding down the left click button on your pointer. Drag the pointer in the required direction.
	Interactive Zoom. Zooms on a specific area of the topology flow map. Click in the topology flow map and drag the cursor to the top or left to decrease the zoom level, or drag to the bottom or right to increase the zoom level.



UI Element	Description
	<p>Marquee Zoom. Zooms on a selected area of the topology flow map.</p> <p>You select an area by moving your pointer while holding down the left click button. When the area is selected, you release the left click button to zoom on that area.</p>
	<p>Fit Screen. Fits all the flow map components into the visible area.</p>
	<p>Navigate Communication Channel. Enables navigating between components of the topology flow map.</p> <p>You click the Navigation Communication Channel button and then click a line connecting two components or subcomponents. The cursor navigates to the endpoint component.</p>
	<p>Collapse All. Collapses the nodes of the topology flow map. When collapsed, each object in the topology flow map represents a different type of entity such as web clients, a running software element, a protocol type, and so forth.</p> <p>Note: This is the default setting when you enter the topology flow map.</p> <p>Example:</p> 

UI Element	Description
	<p>Expand All. Expands the objects of the topology flow map. When expanded, each entity object opens to display its included objects such as servers, client machines, requests, and so forth.</p> <p>Example:</p> 
	<p>Properties Dialog Box. Opens the Graph Properties dialog box, where you can configure the default layout properties for the graph.</p>
<p><Display mode></p>	<p>Select a display mode from the following options:</p> <ul style="list-style-type: none"> • Statistical Graph. Displays the topology flow map as a graph. <p>Note: This is the default display mode.</p> <ul style="list-style-type: none"> • Pattern Tree. Displays the topology flow map as a table. For user interface details, see "Topology Map - Pattern Tree" on the next page.
<p><Topology flow map></p>	<p>In the topology flow map, you can do the following:</p> <ul style="list-style-type: none"> • Click an object to select it. The selected object's attributes and values are displayed in the Component Properties tab of the Properties/Graph View pane. For user interface details, see "Component Properties Tab" on page 173. • Double-click a communication channel line to open the Action Description Statistics dialog box, where you can view the discovered action descriptions. For user interface details, see "Action Description Statistics Dialog Box" on page 178. • Hold the cursor over an object to display a tooltip with additional information.


Topology Map - Pattern Tree

This pane displays the topology flow map as a table.

User interface elements are described below:

UI Element	Description
	Add Transaction Pattern Element. Opens the Add Transaction Pattern Element dialog box, where you can manually add a pattern rule to the selected topology. For user interface details, see "Add Transaction Pattern Element Dialog Box" on the next page.
	Remove Transaction Pattern Element. Deletes a selected pattern rule from the selected topology.
<Display mode>	Select a display mode from the following options: <ul style="list-style-type: none"> • Statistical Graph. Displays the topology flow map as a graph. For user interface details, see "Topology Map - Statistical Graph" on page 174. • Pattern Tree. Displays the topology flow map as a table. <p>Note: This is the default display mode.</p>
Name	A hierarchical tree of the servers included in the topology flow map. The hierarchy of servers is in the order in which they are accessed and each server contains as its children in the tree, the servers it accesses.
Component Type	The communication protocol by which the server is accessed.
Action	The type of action detected in the request. For example, an SQL query, a service, or a URL.

Select Server Dialog Box

The Select Server dialog box displays a table of all the servers included in the topology flow map in the Topology View pane. To access the Select Server dialog box, click the **ellipsis** button  for **Action Description** in the **Add Transaction Pattern Element** dialog box.

User interface elements are described below:

UI Element	Description
Host	The host name of the server and the port number used to access it.
IP	The IP address of the server.
Type	The type of software element running on the server.

Action Description Statistics Dialog Box

The Action Description Statistics dialog box displays a table of action descriptions discovered for a selected communications channel. To access the Action Description Statistics dialog box, click a connecting point in a communications channel in the topology flow map.

User interface elements are described below:



UI Element	Description
Name	The action description name.
Pattern	The action description pattern. That is, the common shared pattern. For example, if the same SQL query was discovered in different page requests, but for each request a specific parameter value was different, the discovered pattern is the SQL query including the parameter name, but without a parameter value.
# Hits	The number of pattern hits (for example, page hits, SQL query hits, and so forth).
Hits/Sec	The number of pattern hits per second.
Load	The total amount of traffic generated by the pattern hits.
Avg. Time	The average time of the pattern hits (that is, the total time divided by the total number of hits).

Add Transaction Pattern Element Dialog Box

The Add Transaction Pattern Element dialog box enables you to manually add a transaction pattern to a selected topology flow. To access the Add Transaction Pattern Element dialog box, click the **Add**

Transaction Element button  in the **Pattern Tree** display mode of a topology flow map.

User interface elements are described below:

UI Element	Description
Source Server	The source server for which you are adding the transaction pattern. This is the server you selected in the pattern tree.
Destination Server	The destination server for which you are adding the transaction pattern. Click the ellipsis button  to select the source element from the Select Server dialog box. For user interface details, see " Select Server Dialog Box " on the previous page.
Action Description	The action description you are adding to the transaction pattern rule. Click the ellipsis button  to select the transaction pattern from the Action Descriptions dialog box.

Chapter 11: RUM Engine File Configuration

Some of the settings used by the RUM Engine are made in various files that you can edit.

This chapter includes the following topics:

- ["Configuring Meaningful Page Names" below](#)
- ["Unifying Frames" on page 201](#)
- ["Configuring User Name Translation" on page 203](#)

Configuring Meaningful Page Names

You can configure RUM to change the URLs of discovered pages that are not configured in End User Management Administration to more meaningful names for use in RUM reports. For information on configuring pages for monitoring, see "Action Dialog Box" in the BSM Application Administration Guide. For information on RUM reports, see "End User Management Reports Overview" in the BSM User Guide.

This section includes the following topics:

- ["About Discovered Page Names" below](#)
- ["Formatting Tags" on the next page](#)
- ["Rule Tags" on page 189](#)
- ["Sample XML File" on page 192](#)
- ["Validating Meaningful Name XML Files" on page 198](#)
- ["Adding and Deleting Meaningful Name XML Files" on page 199](#)
- ["Changing Meaningful Name XML Files" on page 199](#)
- ["Viewing Discovered Page Statistics" on page 200](#)

About Discovered Page Names

For each application configured in End User Management Administration, you can create an XML file to be used to give meaningful names to pages that are discovered as part of the application, but that are not configured as pages in End User Management Administration. For information on configuring applications for monitoring, see "RUM Application Configuration Wizard" in the BSM Application Administration Guide. For information on configuring pages for monitoring, see "Action Dialog Box" in the BSM Application Administration Guide.

If an XML file has been created and an application linked to it, when a page that is not configured in End User Management Administration is discovered as part of the application, the page's URL is compared to the rules in the XML file. If matches are found, the page is given a new name for use in RUM reports. (A page's URL must be matched at least three times before this occurs.) If no matches are found, or if no XML file has been created and linked to the application, the page's URL as recorded is used in RUM reports. For information on RUM reports, see "End User Management Reports Overview" in the BSM User Guide.

The XML file must be created in the `\<RUM root directory>\confresolver\meaningful_pages` directory on the RUM Engine machine. For convenience, we recommend that the file name is the same as the application name. For example, an XML file created for an application called **myapplication** is:

```
\<HP Real User Monitor root directory>\conf\resolver\meaningful_
pages\myapplication.xml
```

Note: RUM includes two default XML files for the PeopleSoft 8.1 and Siebel 7.5 applications.

The XML file contains the following main sections:

- **Formatting.** Contains the formatting commands for changing a URL into a meaningful name.
- **Rules.** Contains the rules that determine whether or not a page's URL is changed to a meaningful name.

Tip: We recommend that you create the rules before the formats.

Formatting Tags

The first main section in the XML file is the formatting section, which contains the XML tags that are used to format parts of a page's URL, which are then used to create a meaningful name for the page.

Note: All parts of a page's URL are converted by RUM to lower case for matching and formatting.

The following formatting tags can be used. For the XML schema to be validated (for details, see "[Validating Meaningful Name XML Files](#)" on page 198), the tags must appear in the XML file in the order in which they are listed below:

- "[URL Decoder](#)" on the next page
- "[Rename](#)" on the next page
- "[Substring](#)" on page 182
- "[ExtractStrToStr](#)" on page 182
- "[ExtractIndexToStr](#)" on page 183

- ["ExtractStrToCount" on page 184](#)
- ["Insert" on page 185](#)
- ["ChangeCase" on page 186](#)
- ["Remove" on page 187](#)
- ["RemoveNonAlpha" on page 187](#)
- ["Replace" on page 187](#)
- ["Alias" on page 188](#)
- ["RegExExtract" on page 188](#)
- ["RegExMatch" on page 189](#)

URL Decoder

The URLDecoder tag is used to decode a source string using a specified decoder.

Syntax	<URLDecoder Name=" Command_Name " EncodingScheme=" Scheme "/>
Explanation	Command_Name. The name of the Substring formatting tag that can be used in Rule tags. Scheme. The decoding scheme to be used.
Example	<URLDecoder Name="DecodeUTF-8" EncodingScheme="UTF-8"/> When the DecodeUTF-8 formatting command is referenced in a rule, the string is decoded using the UTF-8 decoding scheme.
Note	If the URLDeocder tag is used, but no encoding scheme is specified, the UTF-8 scheme is used by default.

Rename

The Rename tag is used to replace the entire contents of a source string.

Syntax	<Rename Name=" Command_Name " NewName=" Rename_String "/>
Explanation	Command_Name. The name of the Rename formatting tag that can be used in Rule tags. Rename_String. The string to be substituted for the source string.

Example	<pre><Rename Name="RenameToABC123" String="HP"</pre> <p>When the RenameToABC123 formatting command is referenced in a rule, the entire source string is renamed to HP.</p>
----------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Substring

The Substring tag is used to extract a sub string from the source string.

Syntax	<pre><SubString Name="Command_Name" BeginIndex="Start_Char_Index" Count="Length"/></pre>
Explanation	<p>Command_Name. The name of the Substring formatting tag that can be used in Rule tags.</p> <p>Start_Char_Index. The position in the source string of the starting character of the substring to be extracted. The first position in the source string is the zero index.</p> <p>Length. The number of characters from the Start_Char to be extracted. If the number used is greater than the number of characters from the Start_Char to the end of the source string, the entire string from the Start_Char to the end of the source string is extracted.</p>
Example	<pre><Substring Name="ExtractTenToTwelve" BeginIndex="10" Count="3"/></pre> <p>When the ExtractTenToTwelve formatting command is referenced in a rule, the tenth, eleventh, and twelfth characters of the source string are extracted.</p>

ExtractStrToStr

The ExtractStrToStr tag is used to extract a string between two given strings from the source string.

Syntax	<pre><ExtractStrToStr Name="Command_Name" fromString="Start_String" fromInclude="Include_Start_String" fromOccurrences="Occurrences_Start_String" toString="End_String" toInclude="Include_End_String" toOccurrences="Occurrences_End_String"/></pre>
---------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Explanation</p>	<p>Command_Name. The name of the ExtractStrToStr formatting tag that can be used in Rule tags.</p> <p>Start_String. The starting string from which the required string is to be extracted.</p> <p>Include_Start_String. Whether to include the starting string as part of the extracted string. Valid options are:</p> <ul style="list-style-type: none"> • True. Include the starting string as part of the extracted string. This is the default used if nothing is specified. • False. Do not include the starting string as part of the extracted string. <p>Occurrences_Start_String. The occurrence number of the starting string at which to start the extraction of the required string. Valid options are 1-100 or last.</p> <p>End_String. The ending string up to which the required string is to be extracted.</p> <p>Include_End_String. Whether to include the ending string as part of the extracted string. Valid options are:</p> <ul style="list-style-type: none"> • True. Include the ending string as part of the extracted string. This is the default used if nothing is specified. • False. Do not include the ending string as part of the extracted string. <p>Occurrences_End_String. The occurrence number of the ending string at which to end the extraction of the required string. Valid options are 1-100 or last.</p>
<p>Example</p>	<pre><ExtractStrToStr Name="ExtractBetweenABCandXYZ" fromString="ABC" fromInclude="true" fromOccurrences="2" toString="XYZ" toInclude="false" toOccurrences="1"/></pre> <p>When the ExtractBetweenABCandXYZ formatting command is referenced in a rule, the string between the second occurrence of ABC and the first occurrence of XYZ in the source string is extracted. The starting string of ABC is also included at the beginning of the extracted string.</p>

ExtractIndexToStr

The ExtractIndexToStr tag is used to extract a string between a given starting position and a given ending string in the source string.

<p>Syntax</p>	<pre><ExtractIndexToStr Name="Command_Name" fromIndex="Start_Char_Index" toString="End_String" toInclude="Include_End_String" toOccurrences="Occurrences_End_String" /></pre>
----------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Explanation</p>	<p>Command_Name. The name of the ExtractIndexToStr formatting tag that can be used in Rule tags.</p> <p>Start_Char_Index. The character number from which to start extracting the required string. The first position in the source string is the zero index.</p> <p>End_String. The ending string up to which the required string is to be extracted.</p> <p>Include_End_String. Whether to include the ending string as part of the extracted string. Valid options are:</p> <ul style="list-style-type: none"> • True. Include the ending string as part of the extracted string. This is the default used if nothing is specified. • False. Do not include the ending string as part of the extracted string. <p>Occurrences_End_String. The occurrence number of the ending string at which to end the extraction of the required string. Valid options are 1-100 or last.</p>
<p>Example</p>	<pre><ExtractIndexToStr Name="ExtractBetween3andXYZ" fromIndex="3" toString="XYZ" toInclude="false" toOccurrences="1"/></pre> <p>When the ExtractBetween3andXYZ formatting command is referenced in a rule, the string between the third index of the source string and the first occurrence of XYZ in the source string is extracted.</p>

ExtractStrToCount

The ExtractStrToCount tag is used to extract a string of a specified number of characters starting at a given string in the source string.

<p>Syntax</p>	<pre><ExtractStrToCount Name="Command_Name" fromString="Start_String" fromInclude="Include_Start_String" fromOccurrences="Occurrences_Start_String" Count="Length" /></pre> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>Note: The parameter names are case sensitive.</p> </div>
----------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Explanation</p>	<p>Command_Name. The name of the ExtractStrToCount formatting tag that can be used in Rule tags.</p> <p>Start_String. The starting string from which the required string is to be extracted.</p> <p>Include_Start_String. Whether to include the starting string as part of the extracted string. Valid options are:</p> <ul style="list-style-type: none"> • True. Include the starting string as part of the extracted string. This is the default used if nothing is specified. • False. Do not include the starting string as part of the extracted string. <p>Occurrences_Start_String. The occurrence number of the starting string at which to start the extraction of the required string. Valid options are 1-100 or last.</p> <p>Length. The number of characters from the Start_String to be extracted. If the number used is greater than the number of characters from the Start_String to the end of the source string, the entire string from the Start_String to the end of the source string is extracted.</p>
<p>Example</p>	<pre><ExtractStrToCount Name="ExtractBetweenABCfor5" fromString="ABC" fromInclude="false" fromOccurrences="1" Count="5"/></pre> <p>When the ExtractBetweenABCfor5 formatting command is referenced in a rule, a string comprising the five characters after the first occurrence of the string ABC in the source string is extracted.</p>

Insert

The Insert tag is used to insert a string into a source string at a specified position.

<p>Syntax</p>	<pre><Insert Name="Command_Name" String="Insert_String" ToIndex="Start_Char_Index" CountFromBeginning="Direction"/></pre>
----------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------

Explanation	<p>Command_Name. The name of the Insert formatting tag that can be used in Rule tags.</p> <p>Insert_String. The string to be inserted in the source string.</p> <p>Start_Char_Index. The character number at which to insert the Insert_String in the source string. The first position in the source string is the zero index.</p> <p>Direction. Whether to start counting the Start_Char index position from the start of the source string (that is, from left to right) or from the end of the source string (that is, from right to left). The valid options are:</p> <ul style="list-style-type: none"> • True. Start counting the Start_Char index position from the start of the source string (that is, from left to right). This is the default used if no direction is specified. • False. Start counting the Start_Char index position from the end of the source string (that is, from right to left).
Example	<pre><Insert Name="InsertABCAfterOrder" String="ABC" ToIndex="5"/></pre> <p>When the InsertABCAfterOrder formatting command is referenced in a rule, the string ABC is inserted in the source string, starting at the fifth index (that is, the letter A becomes the fifth character in the source string).</p>

ChangeCase

The ChangeCase tag is used to change the case of a string.

Syntax	<pre><ChangeCase Name="Command_Name" Type="Case_Type" BeginIndex="Start_Char_Index" Count="Length"/></pre>
Explanation	<p>Command_Name. The name of the ChangeCase formatting tag that can be used in Rule tags.</p> <p>Case_Type. The type of conversion to be carried out. The valid options are:</p> <ul style="list-style-type: none"> • UpperCase. Lower case to upper case. This is the default if no type is specified. • LowerCase. Upper case to lower case. • OppositeCase. Switches the case of characters. <p>Start_Char_Index. The position in the source string of the starting character to be converted The first position in the source string is the zero index.</p> <p>Length. The number of characters from the Start_Char to be converted.</p>

Example	<pre><ChangeCase Name="UpperCaseFirstChar" Type="UpperCase" BeginIndex="0" Count="1"/></pre> <p>When the UpperCaseFirstChar formatting command is referenced in a rule, the first character of the source string is converted to upper case.</p>
Note	<p>If Length is not specified, the ChangeCase conversion is carried out from the Start_Char to the end of the source string.</p>

Remove

The Remove tag is used to remove all occurrences of a specified string from a source string.

Syntax	<pre><Remove Name="Command_Name" String="Remove_String"/></pre>
Explanation	<p>Command_Name. The name of the Remove formatting tag that can be used in Rule tags.</p> <p>Remove_String. The string to be removed from the source string.</p>
Example	<pre><Remove Name="Removeabc" String="abc"/></pre> <p>When the Removeabc formatting command is referenced in a rule, the string abc is removed from the source string.</p>

RemoveNonAlpha

The RemoveNonAlpha tag is used to remove all non-alpha characters from a source string.

Syntax	<pre><RemoveNonAlpha Name="Command_Name"></pre>
Explanation	<p>Command_Name. The name of the RemoveNonAlpha formatting tag that can be used in Rule tags.</p>
Example	<pre><Remove Name="RemoveAllNonAlpha"/></pre> <p>When the RemoveAllNonAlpha formatting command is referenced in a rule, all non-alpha characters are removed from the source string.</p>

Replace

The Replace tag is used to replace all occurrences of a sub string within a source string.

Syntax	<pre><Replace Name="Command_Name" Old="Old_String" New="New_String"/></pre>
---------------	-----------------------------------------------------------------------------------

Explanation	<p>Command_Name. The name of the Replace formatting tag that can be used in Rule tags.</p> <p>Old_String. The sub string within the source string to be replaced.</p> <p>New_String. The string that replaces Old_String.</p>
Example	<pre><Replace Name="ReplaceabcWithXYZ" Old="abc" New="XYZ"/></pre> <p>When the ReplaceabcWithXYZ formatting command is referenced in a rule, all occurrences of abc in the source string are replaced with XYZ.</p>

Alias

The Alias tag is used to replace all occurrences of an alphanumeric sub string within a string with an assigned alias.

Syntax	<pre><Alias Name="Command_Name"> <Pair Name="Source_String" Alias="Assigned_Alias"/> </Alias></pre>
Explanation	<p>Command_Name. The name of the Alias formatting tag that can be used in Rule tags.</p> <p>Source_String. The alphanumeric string to which you are assigning an alias.</p> <p>Assigned_Alias. The alias you are assigning to replace the Source_String.</p>
Example	<pre><Alias Name="RelateLettersToCategory"> <Pair Name="fi" Alias="Fish"/> </Alias></pre> <p>When the RelateLettersToCategory formatting command is referenced in a rule, all occurrences of the string fi are replaced with the alias Fish.</p>
Note	<p>You can include multiple Pair tags within the same Alias tag. Each Alias replacement is carried out on the output string from the previous Alias replacement – that is, there is only one output string at the end.</p>

RegExExtract

The RegExExtract tag is used to extract and build a name from a source string using a regular expression and replacement formula.

Syntax	<pre><RegExExtract Name="Command_Name" regex="Regular_Expression" replacement="Replacement_Formula"/></pre>
---------------	-------------------------------------------------------------------------------------------------------------------

Explanation	<p>Command_Name. The name of the RegExExtract formatting tag that can be used in Rule tags.</p> <p>Regular_Expression. The regular expression for extracting the name from the source string.</p> <p>Replacement_Formula. The formula used by the regular expression to manipulate the extract strings.</p>
Example	<p>RegExExtract tag: <code><RegExExtract Name="ExtractPagePm" regex="/(oracle mysql).*webui/(.*)" replacement="\$3-\$1-MR-\$2"/></code></p> <p>Source string: <code>http://a-ebs.jspic.net/OA_HTML/OA.jsp?page=/oracle/apps/fnd/sso/login/webui/mainloginPG</code></p> <p>Output: <code>pg-oracle-MR-mainlogin</code></p>

RegExMatch

The RegExMatch tag is used to obtain a name by using a regular expression to extract text from a source string by matching a specific pattern.

Syntax	<pre><RegExMatch Name="Command_Name" regex="Regular_Expression" occurrences="Occurrences_in_String"/></pre>
Explanation	<p>Command_Name. The name of the RegExMatch formatting tag that can be used in Rule tags.</p> <p>Regular_Expression. The regular expression for extracting and manipulating the name from the source string.</p> <p>Occurrences_In_String. The matched occurrence in the source string from which to extract and manipulate the strings. Valid options are:</p> <ul style="list-style-type: none"> • 1-100 to use a specific matched occurrence in the source string. For example, 3 to use the third matched occurrence in the source string. • last to use the last matched occurrence in the source string.
Example	<p>RegEXMatch tag: <code><RegExMatch Name="ExtractPagePm" regex="[c h]+..t" occurrences="2"/></code></p> <p>Source string: <code>http://pluto:8080/jpetstore/shop/updateCartQuantitiesHeatAbcde.shtml</code></p> <p>Output: <code>heat</code></p>

Rule Tags

The second main section in the XML file is the rules section, which contains the logic for assigning a meaningful name to a page. The rules section is responsible for matching a page to a single rule and

then using the formatting tags included in the rule to assign a meaningful name to the page. Matching is carried out on the different parts of the URL—URL protocol, URL path, URL host, and parameters (both the GET and POST parameters of a page).

Rules are prioritized, so that if a page's URL matches more than one rule, the rule that has the highest priority is the single rule that is applied to the page.

The rules section uses a default string delimiter of a space (" "), but you can specify a different delimiter by including it in the **Rules** tag that begins the rules section. For example, to set a default delimiter of a right, square bracket: `<Rules DefaultDelimiter="]>`

Individual rules can use a different delimiter than the general default, if specified within the specific rule.

Rules format

Rules are written in the following format:

```
<Rule Priority="Priority" Name="Rule_Name">
  <Path Name="URL_Path">
  <Host Name="URL_Host">
  <Protocol Type="URL_Protocol">
  <Parameters>
    <Param Key="Param_Name" Value="Param_Value">
      <Formatter Index="Index_Number">Format_Name1</Formatter>
      <Formatter Index="Index_Number">Format_Name2          Format_
Name3</Formatter>
      <Formatter Index="Index_Number"></Formatter>
    </Param>
  </Parameters>
</Rule>
```

where:

- **Priority.** The priority in which the rule should be applied. If more than one rule matches the source string, the rule with the highest priority is the one that is applied. 0 is the highest priority, 1 is the second, and so forth.

If more than one rule has the same priority, the last one that appears in the XML file is the rule that is applied.

Tip: When assigning priorities to rules, you can use increments greater than 1. For example, you can assign priorities of 10, 20, 30, and so forth. This allows flexibility for inserting new rules at a later time.

- **Rule_Name.** The name of the rule.
- **URL_Path.** The URL path that is required for the rule to be applied.
- **URL_Host.** The URL host that is required for the rule to be applied. This option does not support the

use of a wildcard.

- **URL_Protocol.** The URL protocol that is required for the rule to be applied. This option does not support the use of a wildcard.
- **Param_Name.** The key (name) of a parameter in the URL that is required for the rule to be applied.
- **Param_Value.** The value in the Param_Name parameter that is required for the rule to be applied. Use "" to denote an empty parameter value.
- **Index_Number.** The position that the formatted string occupies in the meaningful name to be created.
- **Format_Name.** The name of the format to be used on the selected string to format it into a string that is used as part of the created meaningful name for a page. The format name must be one of the formats defined in the formatting section of the XML file (for details, see ["Formatting Tags" on page 180](#)). If no format name is specified, no formatting is applied to the input string, resulting in an identical output string that is used as part of the created meaningful name for a page.

Note: URL_Path, URL_Host, URL_Protocol, Param_Name, and Param_Value are always in lower case.

The following points apply to rules:

- Not all parts of a rule need to exist, but at least one rule should be defined and it should contain a **Formatter** tag.
- If a **Formatter** tag is placed directly under a **Param** tag, the formatting is carried out on the parameter value. If a **Formatter** tag is placed directly under a **Path** tag, the formatting is carried out on the URL path.
- If an asterisk (*) or question mark (?) character is included in a URL path, parameter name, or parameter value, you can specify whether to treat the character as a literal (that is, purely as an asterisk or question mark), or to treat it as a wildcard character. By default, the character is treated as a literal. To treat the character as a wildcard character, you add the setting **CompareMethod="Wildcard"** at the end of the rule tag in which the character appears. For example:

```
<Param Key="myparam" Value="*" CompareMethod="Wildcard">
```

To use an asterisk or question mark character as a literal within a wildcard value, precede the character with a backslash (\). For example, the wildcard value **my*str*** matches the value **my*str123**, but does not match the value **my123str123**.

Note:

- The asterisk wildcard represents any combination of characters, whereas the question mark wildcard represents a single character only.
 - Using the wildcard comparison on page parameters creates significant overhead on the RUM Engine and should be used only when absolutely necessary.
- You can apply multiple format names to a Path or Param tag. If the format names are placed in individual Formatter tags one under the other, each format name is applied to the original path or parameter value and each format name produces its own output for inclusion in the meaningful name. If the format names are included in the same Formatter tag, each format name is applied to the resulting value from the previous format name and only one result is created for inclusion in the meaningful name.

Example of multiple formatting commands in separate Formatter tags:

```
<Path Name="/mypath/home">  
  <Formatter Index="1">Format_Name1</Formatter>  
  <Formatter Index="2">Format_Name2</Formatter>  
  <Formatter Index="3">Format_Name3</Formatter>  
</Path>
```

Each of the format names is applied to the path **/mypath/home**.

Example of multiple formatting commands in the same Formatter tag:

```
<Path Name="/mypath/home">  
  <Formatter Index="1">Format_Name1 Format_Name2</Formatter>  
</Path>
```

Format_Name1 is applied to the path **/mypath/home**; Format_Name2 is applied to the output from Format_Name1.

Sample XML File

The following examples show an XML file with formatting and rule tags defined, and various examples of URLs and the meaningful names created for them based on the formatting and rule tags in the sample XML file:

- ["XML File" on the next page](#)
- ["Examples of Meaningful Names for URL" on page 197](#)

XML File

```
<?xml version="1.0" ?>
- <Meaningful_Pages xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="./meaningfulpages.xsd">
- <Formating>
  <Rename Name="RenameToWelcome" NewName="Welcome" />
  <Rename Name="RenameToSignIn" NewName="Sign In" />
  <Rename Name="RenameToStoreEntrance" NewName="Store Entrance" />
  <Rename Name="RenameToEditAccount" NewName="Edit Account" />
  <Rename Name="RenameToProduct" NewName="Product" />
  <Rename Name="RenameToCheckOut" NewName="Check Out" />
  <Rename Name="RenameToOrderSubmitted" NewName="Order Submitted" />
  <Rename Name="RenameToSignOut" NewName="Signed Out" />
  <SubString Name="ExtractTwoFirstLetters" BeginIndex="0" Count="2" />
  <SubString Name="ExtractItem" BeginIndex="20" Count="4" />
  <SubString Name="ExtractUpdate" BeginIndex="16" Count="6" />
  <SubString Name="ExtractCart" BeginIndex="22" Count="4" />
  <SubString Name="ExtractQuantities" BeginIndex="26" Count="10" />
  <Insert Name="AppendCategory" String="Category" ToIndex="0" />
  <Insert Name="AppendAddItemPrefix" String="Add Item" ToIndex="0" />
  <Insert Name="AppendToCartSuffix" String="to Cart" ToIndex="0"
CountFromBeginning="false" />
  <Insert Name="AppendRemoveItemPrefix" String="Remove Item" ToIndex="0" />
  <Insert Name="AppendFromCartSuffix" String="from Cart" ToIndex="0"
CountFromBeginning="false" />
  <Insert Name="InsertSpaceAfterOrder" String="" ToIndex="5" />
  <Insert Name="InsertSpaceAfterConfirm" String="" ToIndex="7" />
  <Insert Name="InsertNotAfterOrder" String="Not" ToIndex="6" />
  <ChangeCase Name="UpperCaseFirstChar" Type="UpperCase" BeginIndex="0" Count="1"
/>
  <ChangeCase Name="UpperCaseAll" Type="UpperCase" BeginIndex="0" />
  <ChangeCase Name="UpperCaseSixthLetter" Type="UpperCase" BeginIndex="6" Count="1"
/>
  <ChangeCase Name="UpperCaseEighthLetter" Type="UpperCase" BeginIndex="8" Count="1"
/>
  <Remove Name="RemoveNew" String="/jpetstore/shop/new" />
  <Remove Name="RemoveSHTML" String=".shtml" />
  <Replace Name="ReplaceNewWithConfirm" Old="/jpetstore/shop/new" New="Confirm" />
- <Alias Name="RelateLettersToCategory">
  <Pair Name="FI" Alias="Fish" />
  <Pair Name="K9" Alias="Dogs" />
  <Pair Name="RP" Alias="Reptiles" />
  <Pair Name="FL" Alias="Cats" />
  <Pair Name="AV" Alias="Birds" />
</Alias>
- <Alias Name="RelateProductIdToProductName">
  <Pair Name="FI-FW-01" Alias="'Koi'" />
```

```
<Pair Name="FI-FW-02" Alias="'Goldfish'" />
<Pair Name="FI-SW-01" Alias="'Angelfish'" />
<Pair Name="FI-SW-02" Alias="'Tiger Shark'" />
<Pair Name="K9-BD-01" Alias="'Bulldog'" />
<Pair Name="K9-CW-01" Alias="'Chihuahua'" />
<Pair Name="K9-DL-01" Alias="'Dalmation'" />
<Pair Name="K9-PO-02" Alias="'Poodle'" />
<Pair Name="K9-RT-01" Alias="'Golden Retriever'" />
<Pair Name="K9-RT-02" Alias="'Labrador Retriever'" />
<Pair Name="RP-LI-02" Alias="'Iguana'" />
<Pair Name="RP-SN-01" Alias="'Rattlesnake'" />
<Pair Name="FL-DLH-02" Alias="'Persian'" />
<Pair Name="FL-DSH-01" Alias="'Manx'" />
<Pair Name="AV-CB-01" Alias="'Amazon Parrot'" />
<Pair Name="AV-SB-02" Alias="'Finch'" />
</Alias>
- <Alias Name="RelateItemNameToItemDesc">
  <Pair Name="EST-28" Alias="'Adult Female Golden Retriever'" />
  <Pair Name="EST-27" Alias="'Adult Female Chihuahua'" />
  <Pair Name="EST-26" Alias="'Adult Male Chihuahua'" />
  <Pair Name="EST-25" Alias="'Adult Female Labrador Retriever'" />
  <Pair Name="EST-24" Alias="'Adult Male Labrador Retriever'" />
  <Pair Name="EST-23" Alias="'Adult Female Labrador Retriever'" />
  <Pair Name="EST-22" Alias="'Adult Male Labrador Retriever'" />
  <Pair Name="EST-21" Alias="'Adult Female Goldfish'" />
  <Pair Name="EST-20" Alias="'Adult Male Goldfish'" />
  <Pair Name="EST-19" Alias="'Adult Male Finch'" />
  <Pair Name="EST-18" Alias="'Adult Male Amazon Parrot'" />
  <Pair Name="EST-17" Alias="'Adult Male Persian'" />
  <Pair Name="EST-16" Alias="'Adult Female Persian'" />
  <Pair Name="EST-15" Alias="'With tail Manx'" />
  <Pair Name="EST-14" Alias="'Tailless Manx'" />
  <Pair Name="EST-13" Alias="'Green Adult Iguana'" />
  <Pair Name="EST-12" Alias="'Rattleless Rattlesnake'" />
  <Pair Name="EST-11" Alias="'Venomless Rattlesnake'" />
  <Pair Name="EST-10" Alias="'Spotted Adult Female Dalmation'" />
  <Pair Name="EST-9" Alias="'Spotless Male Puppy Dalmation'" />
  <Pair Name="EST-8" Alias="'Male Puppy Poodle'" />
  <Pair Name="EST-7" Alias="'Female Puppy Bulldog'" />
  <Pair Name="EST-6" Alias="'Male Adult Bulldog'" />
  <Pair Name="EST-5" Alias="'Spotless Koi'" />
  <Pair Name="EST-4" Alias="'Spotted Koi'" />
  <Pair Name="EST-3" Alias="'Toothless Tiger Shark'" />
  <Pair Name="EST-2" Alias="'Small Angelfish'" />
  <Pair Name="EST-1" Alias="'Large Angelfish'" />
</Alias>
</Formating>
- <Rules DefaultDelimiter="">
```

```
- <Rule Priority="0" Name="Welcome">
- <Path Name="/jpetstore/">
  <Formatter Index="1">RenameToWelcome</Formatter>
</Path>
</Rule>
- <Rule Priority="1" Name="Welcome">
- <Path Name="/jpetstore/index.html">
  <Formatter Index="1">RenameToWelcome</Formatter>
</Path>
</Rule>
- <Rule Priority="2" Name="Sign In">
- <Path Name="/jpetstore/shop/signonForm.shtml">
  <Formatter Index="1">RenameToSignIn</Formatter>
</Path>
</Rule>
- <Rule Priority="3" Name="Store Entrance">
- <Path Name="/jpetstore/shop/signon.shtml">
  <Formatter Index="1">RenameToStoreEntrance</Formatter>
</Path>
</Rule>
- <Rule Priority="4" Name="Category [any]">
  <Path Name="/jpetstore/shop/viewCategory.shtml" />
- <Parameters>
- <Param Key="categoryId" Value="*" CompareMethod="Wildcard">
  <Formatter Index="1">UpperCaseAll AppendCategory</Formatter>
</Param>
</Parameters>
</Rule>
- <Rule Priority="5" Name="Edit Account">
- <Path Name="/jpetstore/shop/editAccountForm.shtml">
  <Formatter Index="1">RenameToEditAccount</Formatter>
</Path>
</Rule>
- <Rule Priority="6" Name="Any Product [product]">
  <Path Name="/jpetstore/shop/v*Product.shtml" CompareMethod="Wildcard" />
- <Parameters>
- <Param Key="productId" Value="*" CompareMethod="Wildcard">
  <Formatter Index="1">ExtractTwoFirstLetters RelateLettersToCategory</Formatter>
  <Formatter Index="2">RenameToProduct</Formatter>
  <Formatter Index="3">RelateProductIdToProductName</Formatter>
</Param>
</Parameters>
</Rule>
- <Rule Priority="7" Name="Item [any]">
- <Path Name="/jpetstore/shop/viewItem.shtml">
  <Formatter Index="1">ExtractItem UpperCaseFirstChar</Formatter>
</Path>
- <Parameters>
```

```
- <Param Key="itemId" Value="*" CompareMethod="Wildcard">
  <Formatter Index="2">RelateItemNameToItemDesc</Formatter>
</Param>
</Parameters>
</Rule>
- <Rule Priority="8" Name="Add Item [any] To Cart">
  <Path Name="/jpetstore/shop/addItemToCart.shtml" />
- <Parameters>
- <Param Key="workingItemId" Value="*" CompareMethod="Wildcard">
  <Formatter Index="1">RelateItemNameToItemDesc AppendAddItemPrefix
AppendToCartSuffix</Formatter>
  </Param>
</Parameters>
</Rule>
- <Rule Priority="9" Name="Update Cart">
- <Path Name="/jpetstore/shop/updateCartQuantities.shtml">
  <Formatter Index="1">ExtractUpdate UpperCaseFirstChar</Formatter>
  <Formatter Index="2">ExtractCart UpperCaseFirstChar</Formatter>
  <Formatter Index="3">ExtractQuantities UpperCaseFirstChar</Formatter>
</Path>
</Rule>
- <Rule Priority="10" Name="Remove Item [any] From Cart">
  <Path Name="/jpetstore/shop/removeItemFromCart.shtml" />
- <Parameters>
- <Param Key="workingItemId" Value="*" CompareMethod="Wildcard">
  <Formatter Index="1">RelateItemNameToItemDesc AppendRemoveItemPrefix
AppendFromCartSuffix</Formatter>
  </Param>
</Parameters>
</Rule>
- <Rule Priority="11" Name="Check Out">
- <Path Name="/jpetstore/shop/checkout.shtml">
  <Formatter Index="1">RenameToCheckOut</Formatter>
</Path>
</Rule>
- <Rule Priority="12" Name="Order Form">
- <Path Name="/jpetstore/shop/newOrderForm.shtml">
  <Formatter Index="1">RemoveNew InsertSpaceAfterOrder RemoveSHTML
UpperCaseFirstChar UpperCaseSixthLetter</Formatter>
</Path>
</Rule>
- <Rule Priority="13" Name="Order Submitted">
- <Path Name="/jpetstore/shop/newOrder.shtml">
  <Formatter Index="1">RenameToOrderSubmitted</Formatter>
</Path>
- <Parameters>
  <Param Key="confirmed" Value="true" />
</Parameters>
```

```

    </Rule>
- <Rule Priority="14" Name="Order Not Submitted">
- <Path Name="/jpetstore/shop/newOrder.shtml">
  <Formatter Index="1">RenameToOrderSubmitted InsertNotAfterOrder</Formatter>
</Path>
- <Parameters>
  <Param Key="confirmed" Value="false" />
</Parameters>
</Rule>
- <Rule Priority="15" Name="Confirm Order">
- <Path Name="/jpetstore/shop/newOrder.shtml">
  <Formatter Index="1">ReplaceNewWithConfirm InsertSpaceAfterConfirm RemoveSHTML
  UpperCaseEighthLetter</Formatter>
</Path>
</Rule>
- <Rule Priority="16" Name="Sign Out">
- <Path Name="/jpetstore/shop/signoff.shtml">
  <Formatter Index="1">RenameToSignOut</Formatter>
</Path>
</Rule>
</Rules>
</Meaningful_Pages>
    
```

Examples of Meaningful Names for URL

URL	Meaningful Name
http://pluto:8080/jpetstore/	Welcome
http://pluto:8080/jpetstore/index.html	Welcome
http://pluto:8080/jpetstore/shop/signonForm.shtml	Sign In
http://pluto:8080/jpetstore/shop/signon.shtml	Store Entrance
http://pluto:8080/jpetstore/shop/viewCategory.shtml?categoryId=CATS	Category CATS
http://pluto:8080/jpetstore/shop/editAccountForm.shtml	Edit Account
http://pluto:8080/jpetstore/shop/viewProduct.shtml?productId=FI-FW-01	Fish Product 'Koi' (FI=Fish, K9=Dogs, RP=Reptiles, FL=Cats, AV=Birds)

URL	Meaningful Name
http://pluto:8080/jpetstore/shop/viewItem.shtml?itemId=EST-4	Item 'Spotted Koi'
http://pluto:8080/jpetstore/shop/addItemToCart.shtml?workingItemId=EST-6	Add Item 'Male Adult Bulldog' to Cart
http://pluto:8080/jpetstore/shop/updateCartQuantities.shtml	Update Cart Quantities
http://pluto:8080/jpetstore/shop/removeItemFromCart.shtml?workingItemId=EST-6	Remove Item 'Male Adult Bulldog' from Cart
http://pluto:8080/jpetstore/shop/checkout.shtml	Check Out
http://pluto:8080/jpetstore/shop/newOrderForm.shtml	Order Form
http://pluto:8080/jpetstore/shop/newOrder.shtml	Confirm Order
http://pluto:8080/jpetstore/shop/newOrder.shtml?confirmed=true	Order Submitted
http://pluto:8080/jpetstore/shop/newOrder.shtml?confirmed=false	Order Not Submitted
http://pluto:8080/jpetstore/shop/signoff.shtml	Signed Out

Validating Meaningful Name XML Files

You can validate a meaningful name XML file against a predefined XML schema to ensure that the structure and format of the file are valid. The validation is made using the xerces-j 2.8.0 XML parser.

The schema file against which the XML file is validated is:

```
\<RUM root directory>\conf\resolver\meaningfulpages.xsd
```

To validate a meaningful name XML file:

1. Insert the following line at the beginning of the XML file:

```
<Meaningful_Pages xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:noNamespaceSchemaLocation="./meaningfulpages.xsd"
```

Note: If this line is omitted from the XML file and the validation is run, a message that the validation was successful is displayed, but no validation is actually done.

2. Access the JMX console by choosing **JMX Console** from the Configuration drop-down menu in the RUM web console, or by using the following URL in your web browser:

```
http://<RUM Engine machine name>:8180/jmx-console
```

When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).

3. In the JMX Agent View, scroll down to the **RUM.modules** section and click **service=ResolverMeaningfulPagesConfig**.
4. In the **validateConfiguration** option, enter the full name of the XML file you want to validate and click **Invoke**. The XML file is validated against the predefined schema file.
5. Any errors encountered are displayed, or a message that the validation was successful is displayed.

Note: The Formatting tags must be included in the XML file in a specific order (for details, see ["Formatting Tags" on page 180](#)). If the Formatting tags are not in the correct order, a validation error message is displayed, but no indication of the order mismatch is given.

Adding and Deleting Meaningful Name XML Files

If you add or delete a meaningful name XML file in an application in End User Management Administration and would like to apply the change immediately, you can force RUM to reread the End User Management Administration configuration. In the RUM Engine web console, synchronize configuration data by selecting **Tools > Monitoring Configuration Information > Sync All Configuration**. For details, see ["Monitoring Configuration Information" on page 148](#).

(For information on configuring applications for monitoring, see "RUM Application Configuration Wizard" in the BSM Application Administration Guide.)

Changing Meaningful Name XML Files

If you change the content of an existing meaningful page XML file that is used by an application, you must force RUM to reload the configuration for the specific application. For information on configuring applications for monitoring, see "RUM Application Configuration Wizard" in the BSM Application Administration Guide.

To force RUM to reload the configuration for an application:

1. Access the JMX console by choosing **JMX Console** from the Configuration drop-down menu in the RUM web console, or by using the following URL in your web browser:

```
http://<RUM Engine machine name>:8180/jmx-console
```

When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).

2. In the JMX Agent View, scroll down to the **RUM.modules** section and click **service=ResolverMeaningfulPagesConfig**.
3. In the **reloadConfiguration** option, enter the application name (as defined in End User Management Administration) by which the XML file is being used and click **Invoke**. The application's configuration is reloaded in RUM.

Note: To reload the configuration for all applications, click **Invoke** for the **reloadCurrentConfigurations** option.

Viewing Discovered Page Statistics

You can view a table showing statistical information for each application that uses a meaningful name XML file.

To view discovered page statistics:

1. Access the JMX console by choosing **JMX Console** from the Configuration drop-down menu in the RUM web console, or by using the following URL in your web browser:

```
http://<RUM Engine machine name>:8180/jmx-console
```

When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).

2. In the JMX Agent View, scroll down to the **RUM.modules** section and click **service=ResolverMeaningfulPagesConfig**.
3. In the **viewStatistics** option, click **Invoke**. The Meaningful Pages Statistics table opens, showing the following data:

UI Element	Description
Application name	The name of the application as defined in End User Management Administration. (For details on configuring applications in End User Management Administration, see "RUM Application Configuration Wizard" in the BSM Application Administration Guide.)
Configuration file name	The name of the meaningful name XML file used by the application.
Published pages	The total number of pages monitored in the application published to the meaningful pages module.

UI Element	Description
Successful pages	The total number of pages that were successfully processed by the meaningful pages module.
Unmatched pages	The total number of pages successfully processed by the meaningful pages module, but for which no meaningful name was assigned as no match was found.
Failed pages	The total number of pages that were not successfully processed by the meaningful pages module.

Unifying Frames

By default, the RUM Probe reports each frame as a separate page for statistical purposes. However, when replaying a session in the Session Analyzer report, the pages of some frames are listed as sub components of other pages in the hierarchal tree and are displayed accordingly.

RUM uses a default configuration that contains the rules for determining if a page is considered as a parent or a child page. You can change the default settings and can also create new settings for specific pages.

You configure frames to be unified by RUM in the `frame_unification.xml` file on the RUM Engine machine.

To change the default settings for frame unification

1. Edit the `<RUM root directory>\conf\configurationmanager\frame_unification.xml` file on the RUM Engine machine.
2. Locate the **DefaultPage** entry, which is as follows:

```
<DefaultPage>  
  <TimeoutMS>500</TimeoutMS>  
  <InnerFrames maxInnerFrames="-1" />  
  <CanBeInnerFrame>true</CanBeInnerFrame>  
  <MatchInnerFramesReferrer>true</MatchInnerFramesReferrer>  
</DefaultPage>
```

3. Change the settings for your system, where:
 - **TimeoutMS.** The amount of time it takes a frame to load after the previous frame has finished loading. Within this time, if the frame matches the other parameters, such as the referring URL, it is considered as a child of the previous frame, otherwise it is considered as a parent frame.
 - **InnerFrames maxInnerFrame.** The maximum number of children that a parent frame can

contain. Use **-1** for an unlimited number.

- **CanBeInnerFrame.** Set to **true** to enable frames to be considered as children. Set to **false** to consider all frames as parents, unless specific page settings have been defined which are applicable to a frame.
 - **MatchInnerFramesReferrer.** Set to **true** to allow child frames to be matched to parent frames by URLs (if specific page settings have been configured), or **false** to use only the TimeoutMS setting to create child pages.
4. Save the file and exit.

Note: There can be only one **DefaultPage** entry.

To create frame unification settings for specific pages

1. Edit the <RUM root directory>\conf\configurationmanager\frame_unification.xml file on the RUM Engine machine.
2. After the **DefaultPage** entry, create a new **Page** section in the following format:

```
<Page>
  <Pattern>http://www.host.com/.*/</Pattern>
  - <InnerFrames maxInnerFrames="3">
    <Pattern>http://www.host.com/inner1\..*/</Pattern>
    <Pattern>http://www.host.com/inner2.</Pattern>
  </InnerFrames>
  <TimeoutMS>500</TimeoutMS>
  <CanBeInnerFrame>false</CanBeInnerFrame>
  <MatchInnerFramesReferrer>true</MatchInnerFramesReferrer>
</Page>
```

where:

- **Pattern.** A regular expression for the URL pattern to be matched when RUM determines if a frame is to be considered as a parent or child. The first **Pattern** setting at the top of the section determines if the rule is applicable for the frame being matched and is also used as the parent pattern for any matching children. Subsequent **Pattern** settings, within **InnerFrames**, are used to determine if the frame can be considered as a child.
- **InnerFrames maxInnerFrame.** The maximum number of children that the parent frame can contain. Use **-1** for an unlimited number.
- **TimeoutMS.** The amount of time it takes a frame to load after the previous frame has finished loading. Within this time, the frame is considered as a child of the parent frame that matches

the first **Pattern** setting, otherwise it is considered as a parent frame itself.

- **CanBeInnerFrame.** Set to **true** to enable a frame whose URL matches the first **Pattern** setting to be considered as a child, or **false** to consider all frames that match the first **Pattern** setting as parents.
 - **MatchInnerFramesReferrer.** Set to **true** to allow child frames to be matched to the parent frame by the URLs configured in the **Pattern** settings, or **false** to use only the TimeoutMS setting to create child pages.
3. Repeat step 2 to create additional page settings as required.
 4. Save the file and exit.

Note:

- If a page's URL matches the Pattern of more than one Page definition, the first matching Page definition in the file is applied.
- Missing parameters in a Page definition section inherit the DefaultPage setting for that parameter.

Configuring User Name Translation

When configuring a web or SOAP application in BSM (in EUM Administration) for monitoring by RUM, you can configure an application to use a user name translation file if you want RUM to translate a user's login name or IP address located in monitored data to a real name for use in EUM reports.

To enable user name translation for an application in BSM, edit the application in End User Management Administration and in the **General** tab > **User Name Detection** area, select the **Correlate end user names and display aliases** check box.

Tip: We recommend that before changing the **UserNameResolver.xml** file in the procedures below, you back up the original file.

To configure the RUM Engine to translate detected login names to real names

1. In the RUM Engine, ensure that the following values (which are the default settings) are configured in the **confresolver\UserNameResolver.xml** file:

```
<Resolver name="CSVLoginUserNameResolver">
```

```
<class>com.mercury.rum.engine.resolver.usernames.resolvers.  
CSVLoginUserNameResolver</class>  
  <parameters>  
    <param name="file">${rum.home}  
/conf/resolver/UserLoginNames.csv</param>
```

2. Edit the **<RUM Engine root directory>\confresolver\UserLoginNames.csv** file and enter user login names in the first column and the corresponding real names in the second column.
3. Save the file.
4. If you made changes to the **confresolver\UserNameResolver.xml** file, restart the RUM Engine.

To configure the RUM Engine to translate detected IP addresses to real names

1. In the RUM Engine, ensure that the following values are configured in the **confresolver\UserNameResolver.xml** file:

```
<Resolver name="CSVIPUserNameResolver">  
  
<class>com.mercury.rum.engine.resolver.usernames.resolvers.  
CSVIPUserNameResolver</class>  
  <parameters>  
    <param name="file">${rum.home}/conf/resolver/ip2Names.csv</param>
```

2. Edit (or create if it does not exist) the **<RUM Engine root directory>\confresolver\ip2Names.csv** file and enter IP addresses in the first column and the corresponding real names in the second column.
3. Save the file.
4. If you made changes to the **confresolver\UserNameResolver.xml** file, restart the RUM Engine.

Chapter 12: Configuring the RUM Sniffer Probe

You can configure the RUM Sniffer Probe by changing the default settings and adding additional configuration settings.

This chapter includes the following topics:

- ["Changing the Protocol for Accessing the RUM Probe" below](#)
- ["Configuring the RUM Probe for I18N" below](#)
- ["Changing the Header in Which to Locate Client IP Addresses" on the next page](#)
- ["Creating Default Configuration and Properties Files for a Specific Probe" on the next page](#)
- ["Configuring the RUM Probe to Support Multiprotocol Label Switching \(MPLS\)" on page 207](#)

Changing the Protocol for Accessing the RUM Probe

The default protocol used for accessing the RUM Probe is HTTPS with a client certificate. In the RUM Engine web console, you can manually configure the protocol used to access the RUM Probe. For details, see ["Probe Configuration Dialog Box" on page 124](#).

Configuring the RUM Probe for I18N

By default, RUM uses the UTF-8 character set when monitoring data. To enable RUM to support non Unicode encodings, you can configure the RUM Probe to use a different character set.

To change the character set used by the RUM Probe when monitoring data:

In the `<RUM root directory>\conf\configurationmanager\Beatbox_Default_Const_Configuration.xml` file on the RUM Engine, under the `[global]` section, add the following lines:

```
enable_i18n <false/true>
content_charset_search_len <length>
charset <name>
```

where:

- **<false/true>**. Set to **true** to enable RUM to support I18N by using character sets other than UTF-8. The default setting is **false**.
- **<length>**. The number of bytes in the page content in which RUM searches for a character set. By default, RUM does not search the page content for a character set and only searches the page

header. The maximum permissible length is 1024 characters.

- **<name>**. The default character set to use, if RUM does not locate a character set in either the page header or content. Valid character sets are those that are by default supported by the ICU library.

The following example shows the additional lines added to the **[global]** section in the **<RUM root directory>\conf\configurationmanager\Beatbox_Default_Const_Configuration.xml** file on the RUM Engine:

```
<static_global_params>
<![CDATA[
[global]
max_field_length 2048
collect_server_stats false
collect_website_stats false
enable_i18n true
contant_charset_search_len 1024
]]>
```

Changing the Header in Which to Locate Client IP Addresses

By default, RUM tries to locate client IP addresses using the **X-Forward-For** header. If client IP addresses are located in a different header (for example, in a custom header) you can configure RUM to use that header when trying to locate client IP addresses.

To change the header used by the RUM Probe when locating client IP addresses:

1. In the **<RUM root directory>\conf\configurationmanager\Beatbox_Default_Const_Configuration.xml** file on the RUM Engine, under the **[global]** section, add the following line:

```
forwarded_for_header <HEADER_NAME>
```

where **<HEADER_NAME>** is the name of the new header to use for locating client IP addresses.

2. In the RUM Engine web console, synchronize configuration data by selecting **Tools > Monitoring Configuration Data > Sync All Configuration**. For details, see ["Monitoring Configuration Information" on page 148](#).

Creating Default Configuration and Properties Files for a Specific Probe

The RUM Engine uses the same, default, static configuration file and properties file for all the probes attached to it. You can create individual, static configuration and properties files for a specific probe, so that it will be configured with specific settings, instead of the general, default ones.

To create a default configuration file for a specific probe

1. On the RUM Engine, in the **<RUM root directory>\conf\configurationmanager** directory, make a copy of the **Beatbox_Default_Const_Configuration.xml** file.
2. Rename the copy of the file, substituting **Default** with the name of the probe as configured in RUM. For example:

```
Beatbox_123.4.5.67_Const_Configuration.xml
```

3. Edit the file as required with the configuration settings for the specific probe.

To create a default properties file for a specific probe

1. On the RUM Engine, in the **<RUM root directory>\conf\probes** directory, make a copy of the **probe.default.properties** file.
2. Rename the copy of the file, substituting **default** with the name of the probe as configured in RUM. For example:

```
probe.123.4.5.67.properties
```

3. Edit the file as required with the properties for the specific probe.

Configuring the RUM Probe to Support Multiprotocol Label Switching (MPLS)

By default, the RUM Probe does not support MPLS.

To enable MPLS support:

1. Edit the **<RUM root directory>\conf\configurationmanager\Beatbox_Default_Const_Configuration.xml** file on the RUM Engine.
2. Under the **[collector]** section, add the following line:

```
mpls_levels 0
```

Setting the level to 0, instead of to a specific number, configures the probe to calculate the number of MPLS levels needed for the monitored traffic automatically.

3. Save the file.

Chapter 13: Administering the MySQL Database

For RUM to work, it must be connected to a MySQL database that has been created and started.

This chapter includes the following topics:

- ["Overview of the MySQL Database" below](#)
- ["Creating and Connecting to the MySQL Database" below](#)
- ["Starting and Stopping the MySQL Database" on the next page](#)
- ["Maintaining the MySQL Database" on the next page](#)

Overview of the MySQL Database

The MySQL database is the RUM's data repository. The data that is stored in the MySQL database is data that is either not forwarded at all to BSM, or that is only sent on request.

Data that is not forwarded at all to BSM is RUM configuration data. Data that is sent to BSM on request is open session data and session clickstream data (data and snapshots of pages included in sessions). Clickstream data accounts for the majority of the data stored in the MySQL database.

The MySQL database can be installed on the same machine as the RUM Engine or on its own machine. For system requirements for the MySQL database, see "Reviewing System Requirements" in the Real User Monitor Installation and Upgrade Guide.

Creating and Connecting to the MySQL Database

The RUM Engine MySQL database is created during the RUM Engine installation process, if that option is selected. When the MySQL database is created during the installation process, the RUM Engine is connected to it, and the MySQL database is started automatically. The MySQL database to which the RUM Engine is connected must be started for the RUM Engine to work.

You can create a new MySQL database schema and connect the RUM Engine to it, or connect the RUM Engine to a different, existing MySQL database completely, if required.

Note: The RUM Engine can only be connected to one MySQL database.

To create schemas and connect to MySQL databases on an RUM Windows installation:

On the machine on which the RUM Engine is installed, select **Start > Programs > HP Real User Monitor > Administration > RUM Configuration Tool**. The RUM Configuration tool starts. For details on working with the RUM Configuration tool, see "RUM Configuration Wizard" in the Real User Monitor Installation and Upgrade Guide.

Starting and Stopping the MySQL Database

When the MySQL database is created during RUM installation, it is started automatically as part of the process. You can start and stop the MySQL database manually if required.

To start the MySQL database:

On the machine on which the RUM Engine is installed, select **Start > Programs > HP Real User Monitor > Administration > Database > Start Real User Monitor Database**.

To stop the MySQL database:

On the machine on which the RUM Engine is installed, select **Start > Programs > HP Real User Monitor > Administration > Database > Stop Real User Monitor Database**.

Maintaining the MySQL Database

For details on maintaining the MySQL database, including strategies and procedures for backing up and restoring the database, refer to the Database Administration chapter in the MySQL Reference Manual on the MySQL web site (<http://dev.mysql.com/doc/#manual>).

Purging MySQL Binary Log Files

The MySQL binary log contains all statements that updated data in the MySQL database.

The purpose of the binary log is to help update the database to the most current status during a restore operation, as it contains all updates made since the last backup. For details on MySQL binary log files and restoring databases, refer to the Database Administration chapter in the MySQL Reference Manual on the MySQL web site (<http://dev.mysql.com/doc/#manual>).

RUM purges the MySQL binary log files on a daily basis, by deleting all the log files older than five days. You can change the default number of days for which to keep the MySQL binary log files.

To change the default number of days for which to keep MySQL binary log files:

1. Access the JMX console by choosing **JMX Console** from the Configuration drop-down menu in the RUM web console, or by using the following URL in your web browser:

```
http://<RUM Engine machine name>:8180/jmx-console
```

When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).

2. In the JMX Agent View, scroll down to the **RUM.modules** section and click **service=MaintenanceDBConfigurationJMX**.
3. In the **MySQLBinaryLogsDaysCount** parameter, change the setting to the required number of

days.

4. Click the **Apply Changes** button.

Purging MySQL Real User Monitor Data

The data stored in the MySQL database is raw data used by Real User Monitor reports to present session clickstreams and snapshots, and to enable queries for various report filters. The data is sent to HP Business Service Management on request.

Raw data is kept in the MySQL database for a default period of 14 days, after which it is automatically purged from the database. The amount of time raw data is stored in the MySQL database can be changed to any number of days between 7 and 100.

To change the period of time that raw data is stored in the database:

1. Edit the `<RUM root directory>\conf\partitionmanager\pm_tables_config.xml` file on the RUM Engine machine.
2. Change the setting `<archiveDuration units="DAYS" qty="14"/>` from 14 to the required number of days.
3. Save the file.
4. After changing the default Purging policy in RUM, open BSM and change the RUM data purging settings:
 - a. In BSM, click **Admin > Platform > Infrastructure Settings**.
 - b. Select **Applications > End User/System Availability Management**.
 - c. In the End User/System Availability Management - Data table, locate Number of days back to include data in RUM reports and change the value to the new value you just configured in RUM.

Note: By increasing the number of days for which session clickstream data is stored, you may significantly increase the size of the database, which may necessitate additional disk capacity.

Chapter 14: Hardening RUM

You can harden the RUM platform so that it can be part of a secure architecture, and can therefore meet the challenge of dealing with security threats to which it could potentially be exposed.

This chapter includes the following topics:

- ["Hardening the RUM Sniffer Probe" below](#)
- ["Securing Connections to the RUM Engine" on page 215](#)

Note: For details on securing connections between RUM and BSM, see the BSM Hardening Guide.

Hardening the RUM Sniffer Probe

You can harden the RUM Sniffer Probe by changing users and creating passwords for them, disabling non-SSH access, limiting the SSH version that can be used, and by securing the http connection to the probe.

This section includes the following topics:

- ["Changing the Probe's User and Password" below](#)
- ["Limiting Access to the Probe" on the next page](#)
- ["Limiting the SSH Version" on the next page](#)
- ["Securing the HTTP Connection to the Probe" on page 213](#)

Changing the Probe's User and Password

Note: This section applies to the RUM Probe only when it is installed on a Linux system.

When the RUM Probe is installed, a user called **rum_probe** is automatically created, which has access to the probe channels only. This user does not have a password and you should configure one for it.

By default, the RUM Probe is run under the **root** user. It is recommended to run the probe process under the **rum_probe** user, or another specially created user, rather than the **root** user.

To change the user that runs the probe process

1. Log on to the probe as the **root** user.
2. Change the user running the probe process by executing the command:

```
rp_user.pl <USER>
```

where <USER> is the name of the user with which you want to run the probe process.

To configure a password for a user

1. Log on to the probe as the **root** user.
2. Define a password for the user by executing the command:

```
passwd <USER>
```

where <USER> is the name of the user for which you are defining the password. For example, to configure a password for the **rum_probe** user, execute the command:

```
passwd rum_probe
```

3. Follow the on-screen prompts.

Limiting Access to the Probe

The RUM Engine connects to the RUM Probe via the probe's web console. It is recommended to limit access to the RUM Probe by disabling access to other, unnecessary services according to your organization's security policies.

Limiting the SSH Version

Note: This section applies to the RUM Probe only when it is installed on a Linux system.

By default, Linux accepts both SSH 1 and SSH 2 connections. To increase security, it is recommended to configure Linux to accept SSH 2 connections only.

To configure Linux to accept SSH 2 connections only:

On the RUM Probe machine, edit the `/etc/ssh/sshd_config` file and change the line:

```
#Protocol 2,1  
to  
Protocol 2
```

Securing the HTTP Connection to the Probe

You can secure the http connection to the probe by using https connections.

In RUM version 7.0 and later, the RUM Engine by default connects to the probe via an https connection, using default sever and client certificates. In some instances (for example, after upgrading an earlier version of RUM) it might be necessary to manually configure RUM to use https.

This section describes how to manually set an https connection to the probe, as well as how to replace the default, generic, server and client certificates that are included in the probe.

Note: On Windows installations of the probe, the `/etc/rum_probe` directory is located in the RUM Probe root directory.

To manually set an https connection to the probe

1. Log on to the probe machine and edit the `/etc/rum_probe/rpsecurity.conf` file.

2. Uncomment, edit or add the following line:

```
use_ssl true
```

3. Restart the probe:

- For Linux installations use the command `/etc/init.d/rum_probe-capture restart`
- For Windows installations select **Start > Programs > HP Real User Monitor > Administration > Probe > Start RUMProbe**.

4. On the engine machine, edit the `\<RUM root directory>\conf\probes\probe.<PROBE IP>.properties` file, where `<PROBE IP>` is the IP address of the probe machine for which you are configuring basic authentication. If this file does not exist, create it.

5. Uncomment, edit or add the following line:

```
connection.http.ssl=true
```

6. Force an update of the probe configuration by accessing the RUM web console and selecting **Tools > Monitoring Configuration Information > Sync All Configuration**. For details on working with the RUM web console, see ["Using the RUM Web Console" on page 47](#).

To replace the default server certificate

1. Convert the new server certificate and private key to PEM (base64) format, unencrypted (that is, without a password) and copy them to the probe machine.

2. Log on to the probe machine and edit the `/etc/rum_probe/rpsecurity.conf` file.
3. Uncomment, edit or add the following lines:

```
ssl_key <PRIVATE_KEY_FILE>  
ssl_cert <SERVER_CERTIFICATE>
```

Note: The certificate and private key can be included in the same file. In such cases, both lines should refer to that file.

4. Restart the probe:
 - For Linux installations use the command `/etc/init.d/rum_probe-capture restart`
 - For Windows installations select **Start > Programs > HP Real User Monitor > Administration > Probe > Start RUMProbe**.
5. Copy the server certificate (without the private key) to the engine machine.
6. Import the certificate into a new or existing keystore with the command:

```
\<RUM root directory>\JRE\bin\keytool -import -alias rum_probe_cert -keystore  
<KEYSTORE_FILE> -file <CERTIFICATE_FILE>
```

Note: The RUM Engine should be configured to trust the imported certificate.

7. Edit the `\<RUM root directory>\conf\probes\probe.<PROBE IP>.properties` file. If this file does not exist, create it.
8. Uncomment, edit or add the following lines:

```
connection.http.ssl.truststore.file=<KEYSTORE_FILE>  
connection.http.ssl.truststore.password=<KEYSTORE_PASSWORD>
```

9. Force an update of the probe configuration by accessing the RUM web console and selecting **Tools > Monitoring Configuration Information > Sync All Configuration**. For details on working with the RUM web console, see ["Using the RUM Web Console" on page 47](#).

To replace the default client certificate

1. On the engine machine, generate a new private key and certificate into a new, or existing keystore with the command:

```
\<RUM root directory>\JRE\bin\keytool -genkey -alias rum_probe_client_cert -  
keyalg RSA -keystore <KEYSTORE_FILE>
```

2. Enter the details of the certificate and when prompted, approve them.

Note: If you choose a different password for the private key than the keystore password you must also specify this password when configuring the engine to use the keystore (see no. 3).

3. Edit the `\<RUM root directory>\conf\probes\probe.<PROBE IP>.properties` file. If this file does not exist, create it.

4. Uncomment, edit or add the following lines:

```
connection.http.ssl.keystore.file=<KEYSTORE_FILE >  
connection.http.ssl.keystore.password=<KEYSTORE PASSWORD>
```

If you chose a different password for the private key in step 2, edit or add the following line:

```
connection.http.ssl.keystore.PrivateKeypassword=<KEY PASSWORD>
```

5. Export the client certificate with the command:

```
\<RUM root directory>\JRE\bin\keytool -export -rfc -alias rum_probe_client_cert  
-keystore <KEYSTORE_FILE> -file <CERTIFICATE_FILE>
```

6. Copy the certificate file to the probe machine
7. Log on to the probe and edit the `/etc/rum_probe/rpsecurity.conf` file
8. Uncomment, edit or add the following line:

```
ssl_ca_file <CLIENT_CERTIFICATE_FILE>
```

9. Restart the probe:

- For Linux installations use the command `/etc/init.d/rum_probe-capture restart`
- For Windows installations select **Start > Programs > HP Real User Monitor > Administration > Probe > Start RUMProbe**.

10. Force an update of the probe configuration by accessing the RUM web console and selecting **Tools > Monitoring Configuration Information > Sync All Configuration**. For details on working with the RUM web console, see ["Using the RUM Web Console" on page 47](#).

Securing Connections to the RUM Engine

You can access the RUM Engine by different http access points, for the following purposes:

- RUM web console
- RUM JMX console
- RUM Gateway/Proxy Server (for BSM and the replay applet)

You can secure access to the RUM Engine by using authentication and https connections.

This section includes the following topics:

- ["Using Authentication" below](#)
- ["Using HTTPS" below](#)

Using Authentication

All http access points on the RUM Engine are protected via authentication mechanisms. The two main authentication mechanisms used are:

- **User and password protection.** Used for access to the RUM Engine web and JMX consoles.
- **Basic authentication.** Used for all other access points to the RUM Engine.

You can add users for access to the web console and change passwords for users to access both the web and JMX consoles. For details on adding, changing, and deleting users to access the web console, and changing their passwords, see ["Using the RUM Web Console" on page 47](#).

To change the password for a user to access the JMX console:

1. On the engine machine, edit the `\<RUM root directory>\EJBContainer\server\mercury\conf\users.xml` file.
2. In the appropriate line, enter the new password in the **password** parameter.
3. Ensure that the **encryptedPassword** parameter is blank and the **Roles** parameter value is **RUMAdmin**.
4. Save the file and restart the engine.

Using HTTPS

When you configure the RUM Engine to work with https, all connections to the engine are affected. This means that HP Business Service Management must also be configured to communicate with the RUM Engine using https. For details on hardening HP Business Service Management, including creating, configuring, and trusting client and server certificates, see the BSM Hardening Guide.

In BSM, when viewing session details in RUM reports, you can view snapshots of pages and replay a session. By default, the Session Replay applet retrieves data from the RUM Engine via the BSM Gateway Server, but can be configured to retrieve data directly from the RUM Engine (for details, see ["Determining How the RUM Snapshot Applet Retrieves Snapshots"](#) in the BSM User Guide). If the

Session Replay applet is configured to retrieve data directly from the RUM Engine and the RUM Engine is configured to require a client certificate, you must copy and import the necessary certificate on the client machine running the Session Replay applet.

To copy and import a client certificate on a machine running the Session Replay applet:

1. Export the certificate from the keystore on the RUM Engine with the command:

```
\<RUM root directory>\JRE\bin\keytool -export -rfc -alias rum_client_cert -  
keystore <KEYSTORE_FILE> -file <CERTIFICATE_FILE>
```

2. For each client machine on which the Session Replay applet is run:

- a. Copy the certificate exported in step 1 to the client machine.
- b. Import the certificate to the default BSM truststore with the command:

```
<Latest JRE home>\bin\keytool -import -alias rum_client_cert -keystore > -  
keystore <Latest JRE home>\JRE\lib\security\cacerts" -file <CERTIFICATE_  
FILE>
```

Tip: We recommend that you locate truststore and keystore files outside of the <Real User Monitor Engine root directory> to avoid possible upgrade issues.

- c. Restart the browser.

Note: We recommend that you configure the Session Replay applet to retrieve data from the RUM Engine via the BSM Gateway Server, when the RUM Engine is configured to require a client certificate.

Chapter 15: Deploying RUM in a SiteMinder Environment

You use the RUM SiteMinder identity adapter to work with the SiteMinder Web Agent that enables retrieving the USER's attributes from the SiteMinder Server Policy Server.

This chapter includes the following topics:

- ["Overview" below](#)
- ["Prerequisites" on the next page](#)
- ["System Flow" on the next page](#)
- ["Configuring the SiteMinder Policy Server" on page 220](#)
- ["Installing and Configuring the SiteMinder Web Agent" on page 224](#)
- ["Configuring the Web Server" on page 226](#)
- ["Configuring the RUM Engine" on page 232](#)
- ["Changing the Configuration of the TCP Port" on page 233](#)
- ["Testing and Troubleshooting" on page 233](#)

Overview

Note: This chapter describes the configuration of Internet Information Server (IIS) 6.0 for Windows 2003 only. (While neither Apache Server nor IIS 7.0 configurations are included, they are supported and are conceptually the same.)

This chapter is intended for system administrators experienced in the configuration and maintenance of the following components:

- IIS
- SiteMinder Policy Server
- SiteMinder Web Agent
- RUM Engine

Refer to the relevant RUM and SiteMinder documentation as necessary.

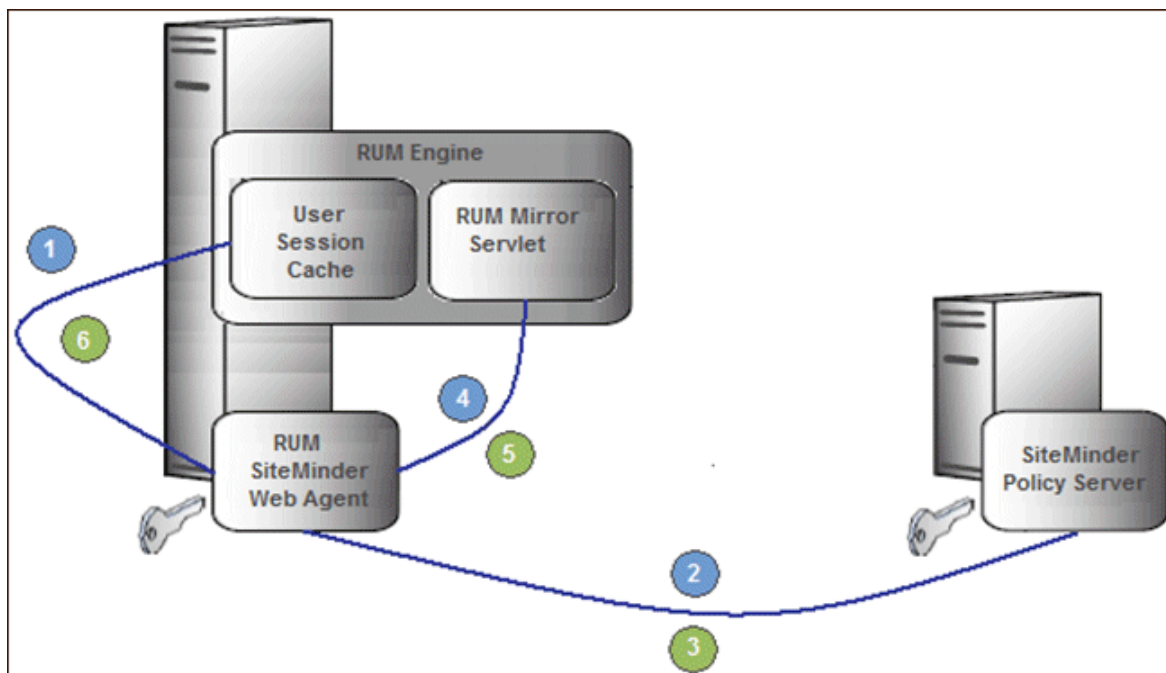
Prerequisites

The following are prerequisite for the RUM–SiteMinder integration:

- The RUM Engine and SiteMinder Web Agent must be installed on the same machine.
- RUM version 9.12 or later.
- IIS.

System Flow

The following diagram illustrates the flow between the RUM Engine, the RUM SiteMinder Web Agent, and the SiteMinder Policy Server.



Processing Steps:

1. The User Session Cache component sends a request with an SMSESSION cookie to the RUM Mirror Servlet for retrieving the USER name (through the RUM SiteMinder Web Agent).
2. The RUM SiteMinder Web Agent intercepts the request and requests the USER data from the SiteMinder Policy Server (relies on the SMSESSION cookie).
3. The SiteMinder Policy Server validates the SMSESSION cookie and sends the Server Policy Response object with USER data.

4. The RUM SiteMinder Web Agent transfers the Server Policy Response object with USER data to a RUM Mirror Servlet.
5. The RUM Mirror Servlet extracts the USER data and sends a response with USER Name back to the User Session Cache component through the RUM SiteMinder Web Agent.
6. The RUM SiteMinder Web Agent redirects the response back to the User Session Cache component.

Configuring the SiteMinder Policy Server

This section describes the following steps for configuring the SiteMinder Policy Server:

- ["Create an Agent" below](#)
- ["Create the Agent Conf Object" on the next page](#)
- ["Create the Authentication Scheme" on the next page](#)
- ["Configure the Domain" on page 222](#)

Create an Agent

To create an agent, use the SiteMinder Administration console to add the RUM Web Agent to the Policy Server.

1. Right-click **Agents** and select **Create Agent**. The SiteMinder Agent dialog box opens.
2. In the **Name** field, enter the hostname of the machine on which the RUM SiteMinder Web Agent is installed. If you are not using the standard, default port **80**, you must also specify the port number after the name (separated by a colon). By default, the RUM Engine's mirror servlet uses port number **8181**, so you enter the name as:

```
<agent_host_machine>:8181
```

Note: If you change the port value in this dialog box, you must also change the port value in other places. For details, see ["Changing the Configuration of the TCP Port" on page 233](#).

3. For the Description, enter **RUM SM Web Agent**.
4. For the Agent Type, select **Web Agent**.
5. Click **OK**.

Create the Agent Conf Object

Use the SiteMinder Administration console to create the Agent Conf Object to the Policy Server.

1. In the left pane of the SiteMinder Administration console, click **AgentConfObjects**.
2. In the right pane, right-click **IISDefaultSettings** and select **Duplicate Configuration Object** from the menu. The SiteMinder Agent Configuration Object dialog box opens.
3. For the Name, enter the hostname of the machine on which the **RUM SiteMinder Web Agent** is installed.
4. For the Description, enter **RUM SM Web Agent**.
5. Edit the **#DefaultAgentName** configuration value:
 - a. Select the **#DefaultAgentName** configuration value.
 - b. Click **Edit**. The Edit Parameter dialog box opens.
 - c. Select the **Plain** radio button.
 - d. For the Parameter Name, enter **DefaultAgentName**.
 - e. For the Value, enter the agent name exactly as it appears in the SiteMinder Agent Properties dialog box.
 - f. Click **OK**.
6. Click **OK**.

Create the Authentication Scheme

In the SiteMinder Administration console, add the Authentication Scheme to the Policy Server.

1. Right-click **Authentication Schemes** and select **Create Authentication Scheme**. The SiteMinder Authentication Scheme dialog box opens.
2. For the Name, enter **RUM Scheme**.
3. For the Description, enter **RUM SM Web Agent**.
4. For the Authentication Scheme Type, select **HTML Form Template**.
5. In the Scheme tab, for the Web Server Name enter the hostname of the machine on which the Web Agent performs authentication.
6. Click **OK**.

Configure the Domain

To configure the domain, perform the following steps:

- ["Create the Realm" below](#)
- ["Create the Response" below](#)
- ["Create the Rules" on the next page](#)
- ["Configure the Policy" on page 224](#)

Create the Realm

In the SiteMinder Administration console, open the domain of the monitored application as provided by your SiteMinder contact.

1. In the left pane of the SiteMinder Administration console, right-click **Domain**.
2. In the right pane, right-click the relevant domain and select **Properties of Domain** from the menu. The SiteMinder Domain dialog box opens.
3. Select the **Realms** tab.
4. Click **Create**. The SiteMinder Realm dialog box opens.
5. For the Name, enter **RUM Mirror Servlet**.
6. For the Resource Filter, enter **/iam/mirror**.
7. Click **Lookup** to search for and select the agent's hostname.
8. For the Authentication Schema, select the **RUM Authentication Schema** created previously.
9. For the Default Resource Protection, select **Protected**.
10. Click **OK** (in the SiteMinder Realm dialog box).
11. Click **OK** (in the SiteMinder Domain dialog box).

Create the Response

In the SiteMinder Administration console, open the domain of the monitored application as provided by your SiteMinder contact.

1. In the left pane of the SiteMinder Administration console, right-click **Domain**.
2. In the right pane, right-click the relevant domain and select **Create Response** from the menu. The

SiteMinder Response dialog box opens.

3. For the Name, enter **RUM Response**.
4. For the Agent, select **Web Agent**.
5. Click **Create**. The SiteMinder Response Attribute Editor opens.
 - a. For the Attribute, select **WebAgent-HTTP-Header-Variable**.
 - b. For the Attribute Kind, select **User Attribute**.
 - c. For the Variable Name, enter **RUM_SM_USER**.

Note: If you change the Variable Name value, you must also change the value of the **requestHeaderUserNameParamName** tag in the **HPRUM\conf\configurationmanager\configuration\IAM_config.xml** file.

- d. Set the Attribute Name as the name of the LDAP attribute that holds the user name value.

Note: The Attribute name depends on your specific LDAP implementation. (For example, the **uid** attribute for Sun One LDAP.)

- e. Click **OK** (in the SiteMinder Response Attribute Editor).
6. Click **OK** (in the SiteMinder Response dialog box).

Create the Rules

1. Create the RUM SMA Authentication rule for the RUM Mirror Servlet realm.
 - a. In the left pane of the SiteMinder Administration console, right-click the **RUM Mirror Servlet** realm and select **Create Rule under Realm** from the menu. The SiteMinder Rule dialog box opens.
 - b. For the Name, enter **RUM SMA Authentication Rule**.
 - c. For the Action, select **Authentication events**.
 - d. In the Action drop-down list, select **onAuthAccept**.
 - e. Click **OK**.
2. Create the RUM SMA Web Action rule for the RUM Mirror Servlet realm.

- a. In the left pane of the SiteMinder Administration console, right-click the **RUM Mirror Servlet** realm and select **Create Rule under Realm** from the menu. The SiteMinder Rule dialog box opens.
- b. For the Name, enter **RUM SMA Web Action Rule**.
- c. For the resource, enter an asterisk (*).
- d. For the Action, select **Web Agent actions**.
- e. In the Action list, select **Get, Post, and Put**.
- f. Click **OK**.

Configure the Policy

In the SiteMinder Administration console, edit the policy of the domain.

Note: If there is more than one policy, you must add the rule and response to each of them.

1. In the left pane of the SiteMinder Administration console, click **Policies**.
2. In the right pane, right-click the relevant policy and select **Properties of Policy** from the menu. The SiteMinder Policy dialog box opens.
3. Select the **Rules** tab.
4. Click **Add/Remove Rules**. The Rule Items dialog box opens.
5. Move the **RUM SMA Web Rule** and the **RUM MA Authentication Rule** from Available Members to Current Members.
6. Click **OK**.
7. In the Rules tab of the SiteMinder Policy dialog box, select the **RUM SMA Authentication Rule**.
8. Click **Set Response**. The Set Response dialog box opens.
9. Select **RUM Response**.
10. Click **OK** (in the Set Response dialog box).
11. Click **OK** (in the SiteMinder Policy dialog box).

Installing and Configuring the SiteMinder Web Agent

This section describes how to install and configure the SiteMinder Web Agent and includes the following topics:

- ["Prerequisites" below](#)
- ["Installing the SiteMinder Web Agent" below](#)
- ["Configuring the SiteMinder Web Agent" on the next page](#)

Prerequisites

Ensure the following prerequisites before installing the SiteMinder Web Agent:

- The Web Server is installed.
- You have an account with Administrative privileges for your Web Server.
- The Policy Server is configured.
- You have an appropriate version of the Web Agent setup file.
- The setup file is compatible with the host's operating system.

Installing the SiteMinder Web Agent

To install the SiteMinder Web Agent:

1. If necessary, extract all the files from the ZIP file provided by SiteMinder.
2. Start the Web Agent executable.

For example: `nete-wa-6qmr6-win64.exe`
3. The CA SiteMinder Web Agent Introduction screen appears. Click **Next**.
4. On the License Agreement screen, scroll down and select **I accept the terms of the License Agreement**, and then click **Next**.
5. On the Important Information screen, click **Next**.
6. On the Choose Install Location screen, accept the default location for installing the Web Agent, or click **Choose** to select a different location. Click **Next**.
7. On the Choose Shortcut Folder screen, click **Next**.
8. On the Pre-Installation Summary screen, click **Install**.
9. On the Install Complete screen, select **Yes, I would like to configure the Agent now** and click **Next**.

Configuring the SiteMinder Web Agent

To configure the SiteMinder Web Agent:

1. On the Host Registration screen, select **Yes, I would like to do Host Registration now**, but do not select the Enable PKCS11 DLL Cryptographic Hardware check box. Click **Next**.
2. On the Admin Registration screen, type the SiteMinder administrator name and password provided by your SiteMinder contact. Do **not** select the Enable Shared Secret Rollover check box. Click **Next**.
3. On the Trusted Host Name and Configuration Object screen, type the trusted hostname and Host Conf Object provided by your SiteMinder contact. Click **Next**.
4. On the Policy Server IP Address screen, type the SiteMinder Policy Server IP address provided by your SiteMinder contact and click **Add**. Click **Next**.
5. On the Host Configuration file location screen, accept the default file name and location and click **Next**.
6. On the Select Web Server(s) screen, select the Web server that you want to configure as a Web Agent and click **Next**.
7. On the Agent Configuration Object screen, enter the Agent Conf Object provided by the SiteMinder contact and click **Next**. (For details, see ["Create the Agent Conf Object" on page 221](#))
8. On the Self Registration screen, select **No, I don't want to configure Self Registration**. Click **Next**.
9. On the Web Server Configuration Summary screen, click **Install**. The Web Agent configuration process starts and when completed, the Configuration Complete screen is displayed.
10. Click **Done** to complete the configuration process.

Configuring the Web Server

This section describes how configure the Web Server and includes the following topics:

- ["Configuring IIS to Work with RUM" below](#)
- ["Configuring IIS to Work with the SiteMinder Web Agent" on page 230](#)

Configuring IIS to Work with RUM

To configure IIS to work with RUM:

1. Download the ISAPI redirector server plug-in **isapi_redirect.dll**, which is available at:
 - Win32 i386
<http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/windows/tomcat-connectors-1.2.37-windows-i386-iis.zip>
 - Win64 x86
http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/windows/tomcat-connectors-1.2.37-windows-x86_64-iis.zip
 - AMD64
http://archive.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/jk-1.2.31/amd64/isapi_redirect-1.2.31.dll
2. Unzip the zip file and copy the **isapi_redirect.dll** file to the **/bin/IIS** directory in your RUM Engine installation.

For example: `C:\HPRUM\bin\IIS\isapi_redirect.dll`

Caution: If you are installing on a WinNT or Win2k system, make sure IIS runs with a user that can access this directory.

3. Open the **/bin/IIS/isapi_redirect.properties** file that contains the configuration settings for the redirector plug-in file.
4. Change **%LOG_DIR%** to the full path of any directory that is not under the RUM home directory.

Caution: Placing the log file in the RUM home directory may cause an automatic uninstallation of the RUM Engine and interference with the re-installation process.

5. Change **%HPRUM%** to the full path of the installation directory of your RUM Engine.

For example: `C:\HPRUM\bin\IIS\isapi_redirect.properties`

```
# Configuration file for the Jakarta ISAPI Redirector
# The path to the ISAPI Redirector Extension, relative to the website
# This must be in a virtual directory with execute privileges
extension_uri=jakarta/isapi_redirect.dll

# Full path to the log file for the ISAPI Redirector
log_file=C:\Users\john DOE\AppData\Local\Temp\isapi.log

# Log level (debug, info, warn, error or trace)
log_level=error

# Full path to the workers.properties file
worker_file=C:\HPRUM\conf\workers.properties.minimal

# Full path to the uriworkermap.properties file
worker_mount_file=C:\HPRUM\conf\uriworkermap.properties
```

6. Save your changes.
7. Open Internet Information Services (IIS) Manager. You must be logged on as a member of the Administrators group on the local computer to perform the following procedures, or you must have been delegated the appropriate authority.

To open IIS Manager at a command prompt:

- a. On the Start menu, click **Run**.
- b. In the Open dialog box, type **inetmgr** and then click **OK**.

For more information, see <http://msdn.microsoft.com/en-us/library/bb763170.aspx>.

8. Using the IIS management console, set TCP port **8181** to **Default Web Site**. This port is used for accessing the mirror servlet from the RUM Engine.

Note: If you change the port value in this dialog box, you must also change the port value in other places. For details, see "[Changing the Configuration of the TCP Port](#)" on page 233.

- a. Right-click the Default Web Site and select **Properties** from the menu. The Default Web Site Properties dialog box opens.
- b. On the Web Site tab, click **Advanced** to open the Advanced Web Site Identification dialog box.
- c. Select the current line with port 80 and click **Edit** to open the Add/Edit Web Site Identification dialog box.
- d. Select the (All Unassigned) IP address option and set the TCP port to **8181**. Click **OK**. The new configuration appears in the **Multiple identities for this Web site** list in the Advanced Web Site Identification dialog box.

9. Using the IIS management console, add a new virtual directory to Default Web Site. The name of the virtual directory **must** be **jakarta**. Its physical path should be the directory in which you placed **isapi_redirect.dll** (for example, C:\HPRUM\bin\IIS). While creating this new virtual directory, assign execute permission to it.

Right-click the Default Web Site and select **New>Virtual Directory** from the menu. The Virtual Directory Creation Wizard opens. In the wizard:

- Enter **jakarta** as an alias of the virtual directory.
- Add a path to the directory that contains **isapi_redirect.dll** (for example, C:\HPRUM\bin\IIS).
- Assign execute permission.

Caution: The name of the virtual directory must be **jakarta**.

10. Using the IIS management console, grant access to the jakarta resource from the local machine only.
 - a. In the left pane, right-click **jakarta** and select **Properties** from the menu.
 - b. Select the **Directory Security** tab.
 - c. In the **IP address and domain restrictions** panel, click **Edit**. The IP Address and Domain Name Restrictions dialog box opens.
 - Select **Denied Access**.
 - Click **Add**.
 - Select **Single computer**.
 - Enter the **IP address** of the machine on which the RUM SiteMinder Web Agent is installed.
 - Click **OK**.
 - d. Click **OK**.
11. Using the IIS management console, add **isapi_redirect.dll** as a filter in Default Web Site (DWS). The name of the filter should reflect its task (uses the name tomcat) and its executable must be C:\HPRUM\bin\IIS\isapi_redirect.dll.
 - a. In the left pane, right-click **Default Web Site** and select **Properties**. The Default Web Site Properties dialog box opens.
 - b. Select the **ISAPI Filters** tab and click **Add**. The Add/Edit Filter Properties dialog box opens.

- c. Enter **tomcat** as the filter name
- d. Add the full path to the **isapi_redirect.dll** as the executable field (for example, C:\HPRUM\bin\IIS\isapi_redirect.dll).
- e. Click **OK**.

Note: At this stage, the status of the added filter is inactive.

12. Using the IIS management console, add the jakarta ISAPI Redirector to the Web Service Extensions.
 - a. In the left pane, right-click **Web Service Extensions** and select **Add a new Web Service extension**. The New Web Service Extension dialog box opens.
 - b. Enter **tomcat** as the Extension Name
 - c. Add the full path to the **isapi_redirect.dll** to the required files. (for example, C:\HPRUM\bin\IIS\isapi_redirect.dll)
 - d. Select the **Set extension status to Allowed** check box.
 - e. Click **OK**.
13. Restart the IIS Web Server.
 - a. On the Start menu, click **Run**.
 - b. In the Open dialog box, type **IISReset** and then click **OK**.

Configuring IIS to Work with the SiteMinder Web Agent

To configure IIS to work with the SiteMinder Web Agent:

1. Open the IIS management console.
2. In the left pane, ensure that the **siteminderagent** virtual directory has been added under the Default Web Site.
3. Check the status of the ISAPI filter for SiteMinder:
 - a. In the left pane, right-click **Web Sites** and select **Properties**. The Web Sites Properties dialog box opens.
 - b. Select the **ISAPI Filters** tab.
 - c. The status of SiteMinder Web Agent must be green.

4. In the IIS management console, add the **ISAPI6 SiteMinder WEbAgent service** to the Web Service Extensions:
 - a. In the left pane, right-click **Web Service Extensions** and select **Add a new Web Service extension** from the menu. The New Web Service Extension dialog box opens.
 - b. Enter **ISAPI6 WEbAgent** as the Extension Name.
 - c. Add the full path to the **netegrity\webagent\bin\ISAPI6WebAgent.dll** to the required files (for example, C:\Program Files\netegrity\webagent\bin\ISAPI6WebAgent.dll).
 - d. Select the **Set extension status to Allowed** check box.
 - e. Click **OK**.
5. In the IIS management console, add the **SM PW** service to the Web Service Extensions:
 - a. In the left pane, right-click **Web Service Extensions** and select **Add a new Web Service extension** from the menu. The New Web Service Extension dialog box opens.
 - b. Enter **SM PW Services** as the Extension Name.
 - c. Add the full path to the **netegrity\webagent\pw\smpwservicescgi.exe** to the required files (for example, C:\Program Files\netegrity\webagent\pw\smpwservicescgi.exe).
 - d. Select the **Set extension status to Allowed** check box.
 - e. Click **OK**.
6. In the IIS management console, add the **SM PW Default** service to the Web Service Extensions:
 - a. In the left pane, right-click **Web Service Extensions** and select **Add a new Web Service extension** from the menu. The New Web Service Extension dialog box opens.
 - b. Enter **SM PW Default Services** as the Extension Name.
 - c. Add the full path to the **netegrity\webagent\pw_default\smpwservicescgi.exe** to the required files (for example, C:\Program Files\netegrity\webagent\pw_default\smpwservicescgi.exe).
 - d. Select the **Set extension status to Allowed** check box.
 - e. Click **OK**.
7. In the IIS management console, allow all unknown CGI and ISAPI Extensions:
 - a. In the left pane, select **Web Service Extensions**.
 - b. In the right pane:

- o Select **All Unknown CGI Extensions**.
 - o Click **Allow**.
 - o Select **All Unknown ISAPI Extensions**.
 - o Click **Allow**.
8. Enable the SiteMinder Web Agent:
 - a. Edit the **netegrity/webagent/bin/IIS/WebAgent.conf** file (for example, C:\Program Files\netegrity\webagent\bin\IIS\ WebAgent.conf).
 - b. Change NO to YES in the **EnableWebAgent** field.
 9. Restart IIS.
 10. Check that SiteMinder is running by selecting **Start > Administrative Tools > Event Viewer**.

Configuring the RUM Engine

This section describes how to configure the RUM Engine:

1. Open the **\EJBContainer\server\mercury\deploy\jbossweb-tomcat50.sar\server.xml** file in a text editor.

For example: C:\HPRUM\EJBContainer\server\mercury\deploy\jbossweb-tomcat50.sar\server.xml

2. Enable the AJP entry by uncommenting it (by default it is commented out).

```
<!-- A AJP 1.3 Connector on port 8009 -->  
<Connector port="8009" address="{jboss bind address}"  
emptySessionPath="true" enableLookups="false" redirectPort="8443"  
protocol="AJP/1.3" URIEncoding="UTF-8"/>
```

3. Save your changes.
4. Open the **\conf\configurationmanager\Beatbox_Default_Const_Configuration.xml** file in a text editor.

For example: C:\HPRUM\ conf\configurationmanager\Beatbox_Default_Const_Configuration.xml

5. Change the value of **max_log_field_length** from 2048 (the default value) to 10240.

For example: max_log_field_length 10240

6. Save your changes.
7. Restart the RUM Engine.

Changing the Configuration of the TCP Port

The deployment of SiteMinder resources (Policy Web agent and RUM Engine mirror servlet) is configured by default to use TCP port **8181**. If you want to change the configured port value, you must also set the port value in the following:

- **Policy server:**
 - Change the **Web agent** name in the SiteMinder Agent dialog box to include the port value. For details, see ["Create an Agent" on page 220](#).
 - Change the **DefaultAgentName** parameter value in the SiteMinder Agent Configuration Object dialog box to the agent's name. For details, see ["Create the Agent Conf Object" on page 221](#).
- **IIS:** Change the **TCP Port** parameter in the Default Web Site Properties dialog box in the IIS Manager. For details, see ["Configuring IIS to Work with RUM" on page 226](#).
- **RUM Engine:** Change the **http_settings > port** XML tag in the **HPRUM\conf\configurationmanager\configuration\IAM_config.xml** file.

Testing and Troubleshooting

This section describes various testing and troubleshooting procedures for the following:

- ["RUM Engine" below](#)
- ["SiteMinder Web Agent" on the next page](#)
- ["Mirror Servlet" on page 235](#)

RUM Engine

Note: Before carrying out the following procedures, the SiteMinder Agent must be disabled.

1. Invoke the URL **http://localhost:8180/rumwebconsole**. If the Login page of the RUM Engine is not displayed, check that the RUM Engine is running.
2. Invoke the URL **http://localhost:8181/iam/mirror**. If an Error page is displayed, check if the status of the ISAPI Filter on the Default Web Site is green.

- a. Right-click **Default Web Site** and select **Properties**. The Default Web Site Properties dialog box opens.
- b. Select the **ISAPI Filters** tab.
- c. If the status is red, check the Application Event Log for the W3SVC-WP. To open the Event Viewer, select **Start > Administrative Tools > Event Viewer**.
 - o Make sure you use an **isapi_redirect.dll** that is compatible with for the host's operating system.
 - o Make sure IIS runs with a user that can access the C:\HPRUM\bin\IIS directory.
- d. If the status is green, examine the last line in the IIS server log file, located in SYSTEM32\LogFiles\W3SVC1. Take the appropriate action according to the error code in the last line:

Error Code	Action
404	Make sure you entered the URL correctly.
505	<ul style="list-style-type: none">o Make sure the virtual directory created is called jakarta.o Make sure that the extension_uri setting is correct.o Check the workers.properties file and make sure the port setting for worker.ajp13w.port is the same as the port specified in the server.xml for the Apache AJP13 support.
202 or 403	Make sure you have checked Execute Access for the jakarta virtual directory in the Advanced Options of the Personal Web Manager.

SiteMinder Web Agent

Invoke the URL **http://localhost:8181/iam/mirror**. The SiteMinder Login Page should be displayed. If an Error page is displayed:

1. **Enable logging**. In the SiteMinder Administration console, right-click your Agent Conf Object and select **Properties of Configuration Object**. The SiteMinder Agent Configuration Object dialog box opens.
 - a. Select **LogFileName**.
 - b. Click **Edit**.
 - c. Enter the full log file path as the value (for example,

C:\Users\johndoe\AppData\Local\Temp\siteminder.log).

Caution: Placing the log file in the RUM home directory may cause an automatic uninstallation of the RUM Engine and interference with the re-installation process.

- d. Click **OK**.
- e. Select **Logfile**.
- f. Click **Edit**.
- g. Enter **yes** as the value.
- h. Click **OK**.

Note: No restart is required.

2. **Check Error in the Event Viewer.** Make sure that the **HostConfigFile** parameter in the **WebAgent.conf** file has the path to the host configuration file.

For example:

```
C:\Program Files\netegrity\webagent\bin\IIS\WebAgent.conf
```

```
HostConfigFile="C:\Program Files\netegrity\  
webagent\config\SmHost.conf.bk1"
```

Mirror Servlet

To check that the mirror servlet is alive and operating correctly with the SiteMinder Web agent, invoke the following URL: **http://localhost:8181/iam/mirror?IDENTITY_PARAM_USER_NAME=RUM_SM_USER**

The **IDENTITY_PARAM_USER_NAME** parameter indicates the header name that is returned at the Web agent's response and that contains the logged-in user name. The header name **RUM_SM_USER** is the same value that was defined in the policy server. For details, see ["Create the Response" on page 222](#).

The result on the page will be the user name that was entered in the login page, followed by the prefix **IAM_UID=**. For example, **IAM_UID=JohnSmith**.

If this result is not accepted:

1. Verify that **RUM_SM_USER** is the configured value in the Policy server.
2. Test and troubleshooting the RUM Engine. For details, see ["RUM Engine" on page 233](#).

3. Test and troubleshooting the SiteMinder Web Agent. For details, see ["SiteMinder Web Agent" on page 234](#).

Chapter 16: RUM Data Export

Data export enables you to extract requested raw data from RUM and provide it to users. You can then use this data to create your own reports, giving you different views than those provided in the standard End User Management reports in BSM. Another benefit of exporting data is that you are not dependent on the RUM purging cycle and can save the exported data for as long as you need.

This chapter includes the following topics:

- ["Enable Data Export" below](#)
- ["How Data is Exported" below](#)
- ["Data Export XML File" on the next page](#)
- ["Valid Channel Types and Fields" on page 242](#)

Enable Data Export

To enable data export, you create and configure an XML file in the **\<RUM root directory>\conf\datapublisher\consumers** directory. This file contains settings such as what data you want extracted, how it should be formatted, where it should be saved, when to close and save a data file and open a new one, and so forth. For details on the XML file, see ["Data Export XML File" on the next page](#).

You can create multiple XML files so that different data can be extracted for different consumers. For convenience, it is recommended that each file name is the same as the relevant consumer name.

A template XML file called **consumer-template.xml** is located in the **\<RUM root directory>\conf\datapublisher** directory. You can copy and edit this file and then save it in the **\<RUM root directory>\conf\datapublisher\consumers** directory.

While a background process checks if configuration files have been changed, you can force an immediate update by synchronizing the configuration in the RUM web console (select **Tools > Monitoring Configuration Data > Sync All Configuration**).

How Data is Exported

When the RUM Engine is started, it checks to see if there are data export configuration XML files in the **\<RUM root directory>\conf\datapublisher\consumers** directory. For each XML file found, the RUM Engine creates a directory for the configured consumer in the configured output directory, and in the consumer's directory creates further sub-directories for each configured channel type. For example, the following directories are created for a consumer called **XYZ**, with a configured output directory of **C:\MyDataPublishing\DpOutput** and with configured channel types of **Page** and **Transaction**:

- C:\MyDataPublishing\DpOutput\XYZ\Page
- C:\MyDataPublishing\DpOutput\XYZ\Transaction

Note:

- RUM must have read and write (RW) permissions for the configured output directory.
- The output directory can be a local or remote directory.

Files are opened in the relevant directories and data is saved to them according to the configuration in the XML file. Data is continuously saved to the files.

A file is closed when it reaches a certain size, or a specific timeout is encountered. You configure the maximum file size and/or timeout in the XML file. When a file is closed, a new file is automatically opened when new data is received. File names are made up of the consumer name, channel type, and the time in milliseconds that the file was created (for example, XYZ_PAGE_12345678).

You can also limit the output directories by size, or by the number of files in them. When the maximum size or the maximum number of files is reached, no more new files will be opened. You must manually manage the output directories and files to ensure that you have enough space.

To stop the export of data, remove the XML files from the **\<RUM root directory>\conf\data\publisher\consumers** directory. Removing the XML file for a specific consumer stops the export of data for that consumer only.

Data Export XML File

This section describes the elements and attributes used in the data export configuration XML file.

A template XML file called **consumer-template.xml** is located in the **\<RUM root directory>\conf\data\publisher** directory.

Elements Table

Element	Description	Attribute For details, see "Attributes Table" below
consumer	Initial element in block containing all the data export configuration.	<ul style="list-style-type: none"> • name • disable

Element	Description	Attribute For details, see "Attributes Table" below
consumerDescription	Optional consumer description.	
collector	Initial element for configuration of a specific collector. Note: You can configure only one collector for data export.	
formats	Initial element for configuring the format for common data types for all exported data.	
DOUBLE	Format for double precision numbers. Default value: <DOUBLE>{#.000}</DOUBLE>	
DATE	Format for dates. Default value: <DATE>{MM-dd-yyyy hh:mm:ss:SS}</DATE>	
channels	Initial element for configuring what data to export.	
channel	Initial element for configuring a specific type of data for export. Note: <ul style="list-style-type: none"> • For each channel type, you configure separate fields and field elements. • If you declare a channel type, but do not declare any fields for that type, all fields are exported by default. 	type
fields	The initial element for configuring the specific fields to export for each channel type. Note: For details on the available fields for each channel type, see "Valid Channel Types and Fields" on page 242 .	
field	Specific data field to export for the configured channel type.	<ul style="list-style-type: none"> • name • title
publisher	Configuration for the actual export of the data.	

Element	Description	Attribute For details, see "Attributes Table" below
type	The type of output in which to export the data. Note: The only valid option is FILE .	
outputDirectory	The directory path in which to save the output files. Caution: Do not locate the output directory on the same disk used by the MySQL database.	
maxDirectorySizeMb	The maximum size of the output directory. After this limit is reached, no more output files are saved.	
maxFilesInDirectory	The maximum number of saved output files that can exist in the output directory. After this limit is reached, no more output files are saved until old files are removed.	
maxFileSizeMb	The maximum size for the open data export file. After this limit is reached, the file is closed and saved and a new file is opened when new data is received.	
timeoutInSec	The maximum timeout that triggers the closing of the data export file. After this limit is reached, the file is closed and saved and a new file is opened when new data is received.	
publisherFileType	The exported data file type. Note: The only valid option is CSV.	
readyFileExtension	The extension to add to the output file when it is closed and saved.	
useHeaders	If set to true , a line of field headers (or alternate names if configured) is added to the saved output file.	
fieldDelimiter	The delimiter to use for separating fields in the output file.	
newLineDelimiter	The delimiter between records (lines) in a file. Valid options are: <ul style="list-style-type: none"> • WINDOW • UNIX • MAC 	

Element	Description	Attribute For details, see "Attributes Table" below
useZip	If set to true , the output file is zipped.	
comment	The sign to use to denote a comment in the output file. Note: This is limited to a single character.	

Attributes Table

Attribute	Parent Element	Description	Example
name	consumer	The consumer name for whom data is exported. Note: <ul style="list-style-type: none"> The consumer name is also used in the exported data file name. The consumer name must be unique within all the configured XML files. 	<consumer name="consumer_XYZ">
disable	consumer	When set to true , data publishing for the consumer is disabled. Default value: false	<consumer name="consumer_XYZ" disable="false">
type	channel	The type of data to export. Valid options are: <ul style="list-style-type: none"> Page Session Transaction Action 	<channel type="Page">
name	field	The name of the field to be exported. Note: For details on the available fields for each channel type, see " Valid Channel Types and Fields " on the next page.	<field name="x-end-user-id" title="x-end-user-id" />

Attribute	Parent Element	Description	Example
title	field	An alternate title for the field name. Note: For details on the available fields for each channel type, see "Valid Channel Types and Fields" below .	<field name="x-end-user-id" title="x-end-user-id" />

Valid Channel Types and Fields

The tables in the following topics list the valid fields for each channel for which you can export data:

- ["Page" below](#)
- ["Transaction" on page 246](#)
- ["Session" on page 248](#)
- ["Action" on page 251](#)

Page

Field Name	Type	Units	Description
all-login-names	string		Login name of end user
c-browser-name	string		Describes the web browser used by the visitor
c-host-id	object		The BSM host ID associated with client
c-host-name	string		The host name associated with client
c-os-name	string		Describes the operating system used by the visitor
cs-app-bytes	int	byte	The number of bytes received by the software element
cs-version	string		HTTP version used for the action
referrer	string		Entire raw referrer string sent in the action
s-host-id	object		The BSM server ID
s-host-name	string		The server name
s-sw-element-id	object		The BSM software element ID
s-sw-element-name	string		The software element name
sc-app-bytes	int	byte	The number of bytes sent by the software element

Field Name	Type	Units	Description
sc-server-firstbut-time-ms	long	ms	Time taken for the server to process the request
sc-status	int		Status or code sent by the server in response to the action
server-time-threshold-ms	long	ms	Server time threshold for the action
timestamp	date	date	Action start time
x-action-descriptor	string		Descriptor for given action
x-action-download-threshold-time-ms	long	ms	Download time threshold for the action
x-action-download-time-ms	long	ms	Total download of the action, from the beginning of the first request until the end of the last request
x-action-external-time-ms	long	ms	Sum totaling the gaps of time within loading of a page during which there are no components being transferred
x-action-id	long		The internal ID of the action
x-action-name	string		The configured name of the action
x-action-requests	int		Total number of component requests for this action
x-application-id	object		The BSM application ID number
x-application-name	string		The BSM application name
x-application-tier-id	object		The BSM application tier ID number
x-available	boolean		Indicates if the action was available
x-cancelled	boolean		Page request that was prematurely interrupted
x-classify	boolean		Indicates that the page was classified
x-connect-time-ms	long	ms	Time taken for the client and server to initialize a TCP connection
x-end-user-id	object		The BSM end-user group ID
x-end-user-packet-latency-time-threshold-ms	long	ms	End user packet latency threshold
x-end-user-subnet-id	object		The BSM end-user subnet ID

Field Name	Type	Units	Description
x-end-user-username	string		The BSM end-user group name
x-errors-events-num	int		Total number of application error events on page
x-event-id1	int		The event ID that has occurred within a particular visitor session on the action
x-event-id2	int		The event ID that has occurred within a particular visitor session on the action
x-event-id3	int		The event ID that has occurred within a particular visitor session on the action
x-geo-ip-num	string		IP Address
x-geo-net-end-num	string		Last IP Address of the client's network block
x-geo-net-start-num	string		First IP Address of the client's network block
x-host-parameterization	string		The host name
x-info-event-num	int		Total number of information (non error) events on page
x-is-backend-tier	boolean		Indicates if the action belongs to back-end tier
x-is-encrypted	boolean		Indicates if the action was encrypted
x-is-over-server-time-threshold	boolean		Indicates if the action was over server time threshold
x-location-id	object		The BSM end-user location ID
x-location-name	string		The BSM end-user location name
x-location-packet-latency-time-threshold-ms	long	ms	Location packet latency threshold
x-location-parent-id1	object		The BSM location ID
x-location-parent-id2	object		The BSM location ID
x-location-parent-id3	object		The BSM location ID
x-location-parent-id4	object		The BSM location ID
x-location-parent-id5	object		The BSM location ID
x-location-parent-name1	string		The BSM location name
x-location-parent-name2	string		The BSM location name
x-location-parent-name3	string		The BSM location name

Field Name	Type	Units	Description
x-location-parent-name4	string		The BSM location name
x-location-parent-name5	string		The BSM location name
x-network-time-ms		ms	Network time
x-packet-latency-time-threshold-ms	long	ms	Packet latency threshold
x-page-title	string		Title of the web page, which is normally displayed along the top of a visitor's web browser window
x-parent-action-seq-id	int		This field is used to correlate frames of the frame sets or other dependent pages
x-performance-event-num	int		Total number of performance (non error) events on page
x-retransmission-time-ms	long	ms	Time spent on retransmitting packets
x-rum-probe-id	int		Internal ID of the RUM Probe
x-server-time-ms	long	ms	Time taken for the server to respond to the request
x-server-time-to-firstbuf-threshold-ms	long	ms	Time to first buffer threshold for the action
x-session-action-seq	int		Number of action views (such as page views) associated with the session
x-session-application-id	string		The internal ID of the session application
x-session-id	string		Universally unique identifier (UUID) automatically assigned to each unique visitor session
x-session-property-tag1	string		The application session property was tagged by RUM
x-session-property-tag2	string		The application session property was tagged by RUM
x-session-property-tag3	string		The application session property was tagged by RUM
x-session-property-tag4	string		The application session property was tagged by RUM
x-session-property-tag5	string		The application session property was tagged by RUM
x-session-start-time	date	date	The session start time
x-ssl-time-ms	long	ms	Time taken for the client and server to initialize an SSL connection
x-total-packets	int		Total number of packets in the request and response

Field Name	Type	Units	Description
x-uri-parameterization	string		The URI
x-url-extracted-data	string		The URL extracted data
x-url-host	string		Name of the host requested by the client
x-url-http-method	string		HTTP request method used
x-url-port	int		HTTP request port
x-url-post-data	string		Query string data sent by a POST request
x-url-protocol	string		Identifier of the protocol
x-url-query-original	string		Query string data sent by a GET request
x-url-query-parameterization	string		URL query string data sent by a GET request
x-url-uri	string		URI string data sent by a GET request

Transaction

Field Name	Type	Units	Description
all-login-names	string		Login name of end user
c-browser-name	string		Web browser used by the visitor
c-host-id	object		The BSM host ID associated with client
c-host-name	string		The host name associated with client
c-os-name	string		Operating system used by the visitor
c-session-start	date	date	Session start time
c-transaction-client-time-ms	long	ms	Time of total processing time between components
c-transaction-gross-download-time-ms	long	ms	Gross download time
c-transaction-net-download-time-ms	long	ms	Net download time
s-host-id	object		The BSM server ID
s-host-name	string		The BSM server name
s-sw-element-id	object		The BSM software element ID

Field Name	Type	Units	Description
s-sw-element-name	string		The software element name
s-transaction-server-firstbuf-time-ms	long	ms	Time taken for the server to process the transaction
s-transaction-server-time-ms	long	ms	Time taken for the server to respond to the transaction
timestamp	date	ms	Transaction start time
x-application-id	object		The BSM application ID number
x-application-name	string		The BSM application name
x-application-tier-id	object		The BSM application tier ID number
x-end-user-id	object		The BSM end-user group ID
x-end-user-subnet-id	object		The BSM end-user subnet ID
x-end-user-user-name	string		The BSM end-user group name
x-geo-ip-num	string		IP Address
x-geo-net-end-num	string		Last IP Address of the client's network block
x-geo-net-start-num	string		First IP Address of the client's network block
x-is-backend-tier	boolean		Indicates if the action belongs to back end tier
x-is-transaction-available	boolean		Indicates if the transaction was available
x-is-transaction-complete	boolean		Indicates if the transaction was completed
x-location-id	object		The BSM end-user location ID
x-location-name	string		The BSM end-user location name
x-location-parent-id1	object		The BSM location ID
x-location-parent-id2	object		The BSM location ID
x-location-parent-id3	object		The BSM location ID
x-location-parent-id4	object		The BSM location ID
x-location-parent-id5	object		The BSM location ID
x-location-parent-name1	string		The BSM location name
x-location-parent-name2	string		The BSM location name
x-location-parent-name3	string		The BSM location name

Field Name	Type	Units	Description
x-location-parent-name4	string		The BSM location name
x-location-parent-name5	string		The BSM location name
x-rum-probe-id	int		Internal ID of the RUM Probe
x-session-application-id	string		Internal ID of the session application
x-session-id	string		Universally unique identifier (UUID) automatically assigned to each unique visitor session
x-threshold-offset-percent			The location threshold offset in percent
x-transaction-bytes	long		Total number of bytes sent and received for the transaction
x-transaction-components	int		Number of components associated with the transaction
x-transaction-connect-time-ms	long	ms	Time taken for the client and server to initialize a TCP connection
x-transaction-errors-events-num	int		Total number of application error events associated with the transaction
x-transaction-id	object		The BSM transaction ID
x-transaction-info-events-num	int		Total number of information (non error) events on transaction
x-transaction-name	string		The BSM transaction name
x-transaction-network-time-ms	long	ms	Network time
x-transaction-performance-events-num	int		Total number of performance (non error) events on transaction
x-transaction-retransmission-time-ms	long	ms	Time spent on retransmitting packets
x-transaction-ssl-time-ms	long	ms	Time taken for the client and server to initialize an SSL connection

Session

Field Name	Type	Units	Description
all-login-names	string		Login name of end user

Field Name	Type	Units	Description
c-browser-name	string		Web browser used by the visitor
c-host-id	object		The BSM host ID associated with client
c-host-name	string		The host name associated with client
c-os-name	string		Operating system used by the visitor
cs-session-bytes	long	byte	Total number of bytes received for the session
s-host-id	object		The BSM server ID
s-host-name	string		The server name
s-sw-element-id	object		The BSM software element ID
s-sw-element-name	string		The software element name
sc-session-bytes	long	byte	Total number of bytes sent for the session
timestamp	date	date	Session start time
x-application-id	object		The BSM application ID number
x-application-name	string		The BSM application name
x-application-tier-id	int		The internal ID of the tier
x-avg-download-time-ms	long	ms	Average download time for all actions associated with the session
x-end-user-id	object		The BSM end-user group ID
x-end-user-subnet-id	object		The BSM end-user subnet ID
x-end-user-username	string		The BSM end-user group name
x-expected-actions-count	int		Expected number of action hits associated with the session
x-geo-ip-num	string		IP Address
x-geo-net-end-num	string		Last IP Address of the client's network block
x-geo-net-start-num	string		First IP Address of the client's network block
x-is-backend-tier	boolean		Indicates the session associated with a back-end tier
x-is-session-available	boolean		Indicates if the session was available
x-is-session-ssl	boolean		Indicates that the session was over SSL connection
x-location-id	object		The BSM end-user location ID

Field Name	Type	Units	Description
x-location-name	string		The BSM end-user location name
x-location-parent-id1	object		The BSM location ID
x-location-parent-id2	object		The BSM location ID
x-location-parent-id3	object		The BSM location ID
x-location-parent-id4	object		The BSM location ID
x-location-parent-id5	object		The BSM location ID
x-location-parent-name1	string		The BSM location name
x-location-parent-name2	string		The BSM location name
x-location-parent-name3	string		The BSM location name
x-location-parent-name4	string		The BSM location name
x-location-parent-name5	string		The BSM location name
x-rum-probe-id	int		Internal ID of the RUM Probe
x-session-application-id	string		The internal ID of the session application
x-session-duration-ms	long	ms	Duration time of the session
x-session-dwell-time-ms	long	ms	Session's total dwell time, or the total number of milliseconds the visitor spent looking at pages during the current session
x-session-error-events-num	int		Total number of application error events associated with the session
x-session-failed-actions	long		Number of failed actions on the session
x-session-id	string		This is a universally unique identifier (UUID) automatically assigned to each unique visitor session
x-session-info-events-num	int		The total number of information (non error) events associated with the session
x-session-last-page	date	date	Time of last page associated with the session
x-session-latency-time-ms	long	ms	Total session latency
x-session-packets	long		Total number of packets sent and received for the session
x-session-pageviews-num	int		Number of page views associated with the session

Field Name	Type	Units	Description
x-session-performance-events-num	int		The total number of performance (non error) events associated with the session
x-session-property-tag1	string		The application session property was tagged by RUM
x-session-property-tag2	string		The application session property was tagged by RUM
x-session-property-tag3	string		The application session property was tagged by RUM
x-session-property-tag4	string		The application session property was tagged by RUM
x-session-property-tag5	string		The application session property was tagged by RUM
x-session-referrer	string		Entire raw referrer string sent in the session's first request
x-session-requests-num	int		Number of hits or HTTP requests associated with the session
x-total-download-time-for-available-actions-ms	long	ms	Total download time of available action associated with the session
x-total-download-time-for-unavailable-actions-ms	long	ms	Total download time of unavailable action associated with the session

Action

Field Name	Type	Units	Description
x-action-id	int		Action ID
x-action-id-as-integer	int		Action ID as an integer
x-action-name	string		Action name
x-additional-properties	string		A string containing all additional properties of an action relevant for the specific protocol
x-action-requests	string		Total number of component requests for this action
x-action-seq-id	int		The sequential number of the action from the total actions for the entire session
x-availability-threshold	long		Availability threshold
x-available	boolean		Indicates if the action was available

Field Name	Type	Units	Description
x-bytes-in	int		Number of received bytes
x-bytes-out	int		Number of sent bytes
x-client-time-MS	long	ms	Action client time
x-conditional-follower-time-diff-threshold	int		Relevant for Seibel protocol only
x-connect-time-MS	long	ms	The time taken for the client and server to initialize a TCP connection, in microseconds.
x-download-threshold-offset-percent	int		Download threshold offset percent
x-download-time-threshold-MS	long	ms	Download time threshold
x-download-time-MS	long	ms	Time taken from page first packet to page last packet
x-dynamic-download-time-Th	long		If true - download time threshold is computed dynamically from historical data
x-dynamic-server-time-Th	long		If true - server time threshold is computed dynamically from historical data
x-end-time-micros	long	ms	Action end time
x-event-app-error-count	int		Number of event application errors
x-event-info-count	int		Number of info events
x-event-string	string		String contains event IDs
x-events	int		Number of events
x-extracted-parameters	string		A string containing all extracted parameters for an action</description
x-extracted-parametersMap	string		A string containing a map of all extracted parameters for an action
x-event-category-protocol-count	int		Number of category protocol events
x-event-performance-count	int		Number of performance events

Field Name	Type	Units	Description
x-generic-descriptor	string		Descriptor for a given action
x-generic-parameters	string		A string containing generic parameters for the specific protocol
x-hierarchy-tag	string		Relevant for Seibel protocol only
x-integration-diag	string		Data from Diagnostics integration
x-integration-TV	string		Data from TransactionVision integration
x-is-backend-tier	boolean		Indicates if the action belongs to a back-end tier
x-is-classify	boolean		Action has been classified
x-is-SSL	boolean		Indicates that the action was over an SSL connection
x-network-time-MS	long	ms	Action network time
x-orig-action-properties-as-string	string		A string containing all the original properties of an action for the specific protocol
x-parameters	string		String contains protocol parameters
x-parent-action-seq-id	int		This field is used to correlate frames of the frame sets or other dependent pages
x-retransmission-time-MS	long	ms	The time spent on retransmitting packets
x-server-availability-threshold	int		Server availability threshold
x-server-time-threshold-MS	long	ms	Server time threshold
x-server-time-MS	long	ms	Time taken for the server to respond to the request
x-server-time-to-first-buf-MS	long	ms	Server time to first buffer
x-server-time-to-first-buf-threshold-MS	long	ms	Server time to first buffer
x-session-property-tag1	string		The application session property was tagged by RUM

Field Name	Type	Units	Description
x-session-property-tag2	string		The application session property was tagged by RUM
x-session-property-tag3	string		The application session property was tagged by RUM
x-session-property-tag4	string		The application session property was tagged by RUM
x-session-property-tag5	string		The application session property was tagged by RUM
x-session-start-time	long		The session start time
x-specific-descriptor	string		The BSM action name
x-specific-parameters	string		A string containing specific extracted parameters
x-ssl-time-MS	long	ms	The time taken for the client and server to initialize a TCP connection, in microseconds.
x-start-time-micros	long	ms	Action start time
x-status-code	int		Protocol status code
x-stopped	long		The number of page requests that were prematurely interrupted, including the page itself and all subsequent non-page or image transactions.
x-template-parameters	string		A string containing all action parameters relevant for the specific protocol
x-time-stamp	date		Action start time
x-total-latency-MS	long	ms	Total action latency
x-total-packets	int		Number of packets

Part 4: Supporting Specific Protocols

Chapter 17: Parsing Supported Protocols

Parsing supported protocols are protocols on which RUM can carry out deep analysis, thus providing detailed data about monitored applications for use in End User Management reports.

RUM supports the following protocols for parsing:

HTTP Protocols

- HTTP/S
- Flash/ActionScript AMF – HTTP Based

SOA Protocols

- SOAP – HTTP Based
- WCF – TCP Based

Database Protocols

- IBM DB2
- Microsoft SQL Server
- MySQL Database Server
- Oracle DB (Thin JDBC Client)

Application Servers

- Citrix XenApp
- IBM WebSphere MQ
- Oracle Forms NCA
- SAPGUI

Mail Protocols

- IMAP (Internet Message Access Protocol)

- POP3 (Post Office Protocol)
- SMTP (Simple Mail Transfer Protocol)

Generically Supported Protocols

- DNS – Generic UDP
- Microsoft Terminals Services (RDP) – Generic Streaming TCP
- RMI Registry – Generic TCP
- SSH – Generic Streaming TCP

Others

- FTP (File Transfer Protocol)
- ISO 8583 (financial transaction card originated messages for Visa and Mastercard)
- LDAP (Lightweight Directory Access Protocol)

Chapter 18: Customizing Error Codes for SAPGUI

Error capturing is based on matching status messages against a template list. Out-of-the-box, RUM is configured to match only some of the SAPGUI error messages. You can add additional error messages (predefined or custom) to the list for matching.

To add additional error messages, on the RUM Probe machine edit the **<HPRUMProbe>/etc/rum_probe/protocols/sapgui.def** file and under the **[sapgui_custom]** section add a line for each error code in the following format:

```
status_code <CODE> <MESSAGE_REGEX>
```

For example, the line **status_code 1 Function module \w* does not exist** means that an action is reported as having a status code of 1 if it results in a status message that matches the regular expression 'Function module \w* does not exist'.

BSM uses the SAPGUI status codes to create predefined events for applications configured with the SAPGUI template. By default, only error codes 1 (Object not found) and 2 (Invalid function) are predefined in BSM and are both included in an event called **SAPGUI error**. To add additional predefined events for SAPGUI applications using other codes, on the BSM Gateway Server edit the **<HPBSM>\conf\rum_templates\SapGui.xml** file and under the **<events>** tag, create a new, single event in the following format:

```
<event>
  <active>true</active>
  <snapshot>true</snapshot>
  <name>Unique event name</name>
  <report_as_error>true</report_as_error>
  <category>error</category>
  <collect_session_snapshot>>false</collect_session_snapshot>
  <scope>GLOBAL</scope>
  <type>0</type>
  <error_codes>
    <code>Unique error code number</code>
  </error_codes>
  <actions/>
</event>
```

Note: The event name and the error code number must be unique within the template. That is, they cannot be used in any other event configured in the template.

Example

To report actions that contain an 'Invalid key specified' message:

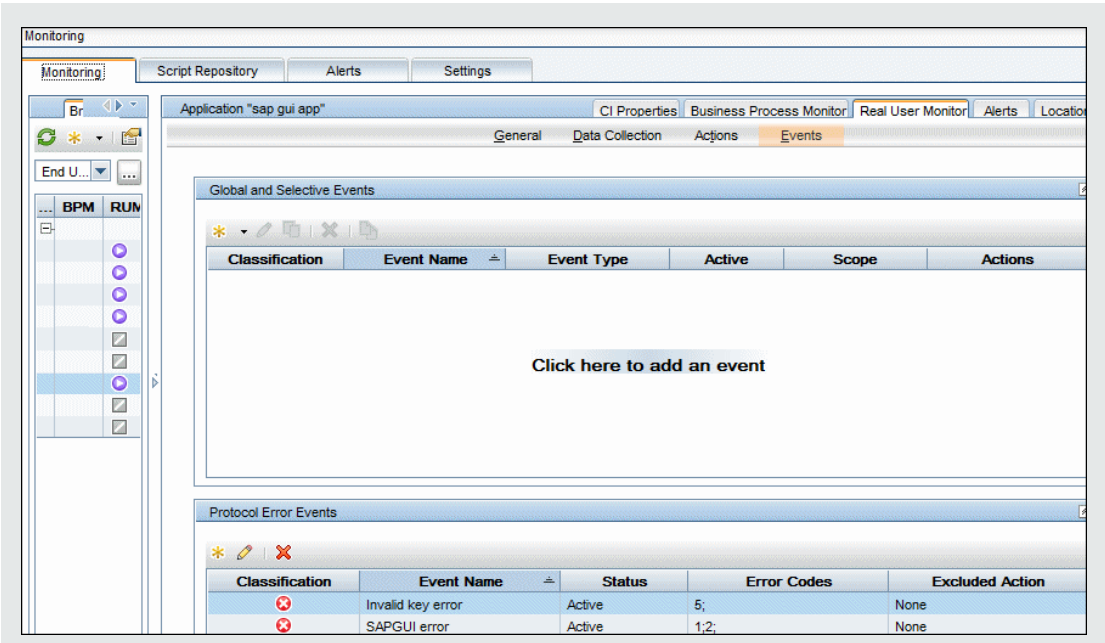
1. On the RUM Probe machine, add the following line under the **[sapgui_custom]** section in the **<HPRUMProbe>/etc/rum_probe/protocols/sapgui.def** file:

```
status_code 5 Invalid key specified
```

2. On the BSM Gateway Server, add the following event to the SAPGUI template (**<HPBSM>\conf\rum_templates\SapGui.xml**):

```
<event>  
  <active>true</active>  
  <snapshot>true</snapshot>  
  <name>Invalid key error</name>  
  <report_as_error>true</report_as_error>  
  <category>error</category>  
  <collect_session_snapshot>>false</collect_session_snapshot>  
  <scope>GLOBAL</scope>  
  <type>0</type>  
  <error_codes>  
    <code>5</code>  
  </error_codes>  
  <actions/>  
</event>
```

3. In BSM, an 'Invalid key error' event is added as a default Protocol Error Event for applications configured with the SAPGUI template:



Chapter 19: Monitoring Citrix with RUM

You can use RUM's VDI agent to monitor Citrix traffic.

This chapter includes the following topics:

- ["Overview of Citrix Monitoring with RUM" below](#)
- ["Overview of the RUM VDI Agent" on page 262](#)
- ["Configurations for Working with the RUM VDI Agent for HTTP Traffic" on page 263](#)
- ["Advanced Configuration for HTTP Traffic" on page 265](#)
- ["Using the RUM VDI Agent with Terminal Services for HTTP Traffic" on page 267](#)

Overview of Citrix Monitoring with RUM

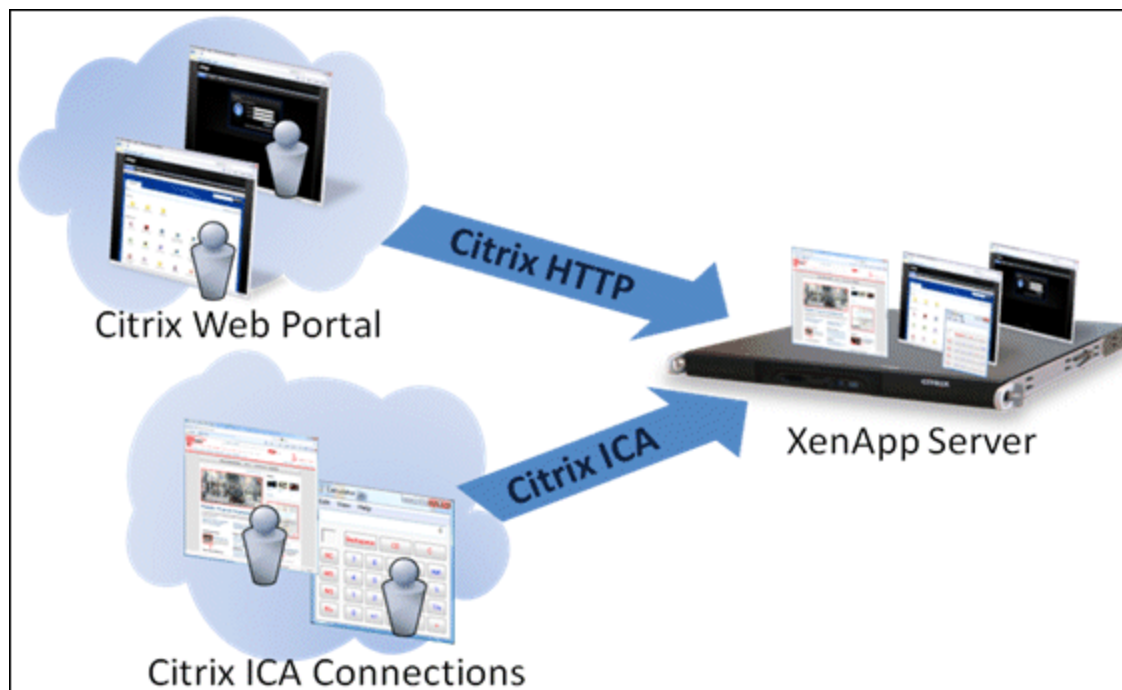
End users can connect to a Citrix XenApp server via a web portal or a direct ICA connection. When multiple users connect to the same XenApp server, requests sent from the XenApp server all originate from the same client, regardless of the originating end user.

This section includes:

- ["Monitoring Traffic Between End Users and a XenApp Server" on the next page](#)
- ["Monitoring Outgoing Traffic from a XenApp Server" on the next page](#)

Monitoring Traffic Between End Users and a XenApp Server

The following diagram shows typical traffic between end users and a Citrix XenApp server:



An end user starts by opening a Citrix web portal and selecting one of the published applications. An ICA session is created, in which the selected application runs on the XenApp server, and the user uses the application remotely.

Alternatively, a user can create an ICA connection directly, without going through a web portal.

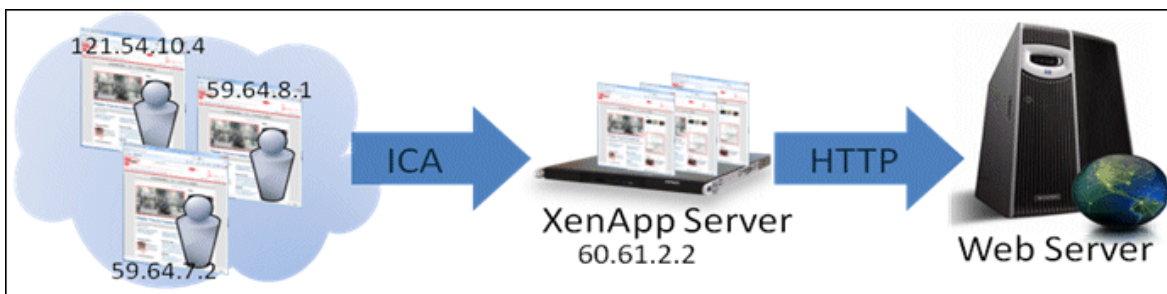
To monitor this traffic with RUM 9.x or later, no agent installation is required. You simply configure the following applications in BSM, using specific templates:

- The XenApp application, using the **Citrix ICA** template.
- The Login application, using the **Citrix Http** template.

For user interface details on creating RUM applications in BSM, see "RUM Application Configuration Wizard" in the BSM Application Administration Guide.

Monitoring Outgoing Traffic from a XenApp Server

The following diagram shows multiple users connected to the same XenApp server, each running an instance of the Internet Explorer browser to connect to a web server. In this scenario, all connections opened to the web server originate from the same client, which is the XenApp server.



To monitor this, you must define the web application (web servers) using the **General Web Application** template.

To monitor the XenApp Server as a VDI tier of the General Web Application, you must define the monitoring VDI tier to use the **Citrix ICA VDI** template.

When monitoring this scenario with RUM, it is desirable to see the real end users as the clients, rather than having a single client combining all the traffic. To achieve such functionality, you must install the RUM VDI Agent on the XenApp server.

The following table shows the difference between RUM reports when the RUM VDI Agent is, or is not, installed on the XenApp server:

Request URL	Without RUM VDI Agent		With RUM VDI Agent	
	Client IP	User Name	Client IP	User Name
/index.html	60.61.2.2	-	121.54.10.4	John
/index.html	60.61.2.2	-	59.64.8.1	Rosetta
/search?q=agent	60.61.2.2	-	121.54.10.4	John
/checkout.jsp	60.61.2.2	-	59.64.8.1	Rosetta
/index.html	60.61.2.2	-	59.64.7.2	Steve
/view?item=agent	60.61.2.2	-	121.54.10.5	Peter

Overview of the RUM VDI Agent

You use the RUM VDI Agent to monitor traffic from a XenApp server for the initiating end user.

This section includes:

- ["Supported Browsers for HTTP Traffic" on the next page](#)
- ["How the RUM VDI Agent Works for HTTP Protocol" on the next page](#)

Supported Browsers for HTTP Traffic

For details on the supported browsers and ActiveX components, see the *RUM VDI Agent Requirements* in the Real User Monitor Installation and Upgrade Guide.

How the RUM VDI Agent Works for HTTP Protocol

The RUM VDI Agent tags outgoing HTTP traffic with the IP address and user name of the real end user (connected to the XenApp server). This information is added to the preconfigured HTTP header.

The new configuration mode (which is the default mode) adds the following HTTP headers:

- RUM_USER_NAME
- RUM_CLIENT_ADDRESS

In compatibility mode, the information is added to the **UserAgent HTTP** header

For more information see ["Advanced Configuration for HTTP Traffic" on page 265](#).

Note: Tagging the user agent HTTP header may slow down the browser. However, you can assume that the browser and website are on the same network (or at least geographically near each other), so any slow down is not significant.

Configurations for Working with the RUM VDI Agent for HTTP Traffic

You must configure user name detection in the applications you want monitored using the RUM VDI Agent. Additionally, you can configure RUM to use the IP of the real user connected to a XenApp server as the client IP in the web application.

This section includes:

- ["To configure user name detection in applications" below](#)
- ["To configure Real User Monitor to use the IP of the real user connected to a XenApp server as the client IP in the web application" on the next page](#)

To configure user name detection in applications

1. In End User Management Administration in BSM, configure a new application or edit an existing application.
2. Select **Real User Monitor > General** and in the **Real User Monitor Application General** page,

expand the **User Name Detection** area.

3. Click the **New User Name Detection** button. The **User Name Detection** dialog box opens in a new window.
4. In the **User Name Detection** dialog box, configure the following:
 - In compatibility mode:

Field	Value
Search in	HTTP Header
Header name	User-Agent
Extract text:	
Between	RUM_USER_NAME=
and	;

- In the new configuration mode:

Field	Value
Search in	HTTP Header
Header name	RUM_USER_NAME
Content	All content

5. Click **OK** to save the configuration changes.

Note: The web application may require users to log on when opening the application in the web browser. In such cases, you should decide whether you prefer configuring the user name for the web application as the Citrix user name, or as the web application's user name. In either case, you may consider configuring the other user name (Citrix or web application) as a Session Property.

To configure Real User Monitor to use the IP of the real user connected to a XenApp server as the client IP in the web application

1. On the RUM Engine, edit the file:

<HPRUM>\conf\configurationmanager\Beatbox_Default_Const_Configuration.xml

2. Add the following line at the end of the **[Global]** section:

- In compatibility mode, add:

```
forwarded_for_header User-Agent .*RUM_CLIENT_ADDRESS=IPV4\\\[^\];.* $1
```

- In the new configuration mode, add:

```
forwarded_for_header RUM_CLIENT_ADDRESS IPV4\\\[^\];.* $1
```

3. Save the file.

4. In the RUM Engine web console, synchronize configuration data by selecting **Tools > Monitoring Configuration Information > Sync All Configuration**. For details, see "[Monitoring Configuration Information](#)" on page 148.

Advanced Configuration for HTTP Traffic

You configure advanced settings by editing the **<All users Application Data path>\HP\RumHttpAgent\settings\RumHttpAgent.cfg** file on the Citrix XenApp server on which the RUM VDI Agent is installed.

(For example, C:\Documents and Settings\All Users\Application Data\HP\RumHttpAgent\settings\RumHttpAgent.cfg.)

To set the configuration mode for VDI Agent

The following files appear in the settings directory:

- RumHttpAgent.cfg
- RumHttpAgent.cfg.update

By default, VDI Agent works in the new configuration mode using **RumHttpAgent.cfg**. In the new configuration mode, new headers are created and the UserAgent header is not used.

To work in compatibility mode (in which information is added to the User-Agent field), rename the **RumHttpAgent.cfg.update** file to **RumHttpAgent.cfg**.

To disable the RUM VDI Agent

In the **[common]** section of the file, change the **disable** parameter value to **true**. The change takes effect for new IE browser instances.

To disable the RUM VDI Agent for a specific browser type

In the **[IE]** or **[Firefox]** section of the file, change the **disable** parameter value to true. The change takes effect for new instances of the specific browser.

To filter and rename header fields (for example, User Agent)

To avoid the following limitation, we recommended you work in the new configuration mode.

However, if you do decide to work in compatibility mode, be aware that some versions of ASP.NET limit the length of the User-Agent HTTP header to 256 byte (see <http://support.microsoft.com/kb/974762/en-us>). If the User-Agent HTTP header exceeds this threshold, the web browser is not able to browse through the web pages. Although Microsoft released a patch for this issue, not all environments worldwide have been updated.

The current implementation of the RUM VDI Agent cannot control the entire User-Agent HTTP header. The RUM VDI Agent tells the browser to include a substring like `RUM_USER_NAME=<john_smith>;RUM_DOMAIN_NAME=<company_domain>;RUM_CLIENT_ADDRESS=IPV4*<11.22.33.44>; RUM_CLIENT_NAME=<JOHN-WORK-NOTEBOOK>` in the header. This substring may exceed the 256 character limit.

Starting from version 9.23, you can configure which fields RUM VDI Agent will publish and, optionally, you can configure these fields to be renamed with a shorter alias.

To achieve this goal, `<ProgramData>\HP\RumHttpAgent\settings\RumHttpAgent.cfg` has a new parameter **allowedFieldList** under the **[Common]** section:

```
# With the aim to reduce the User-Agent header, you can specify only some of the
fields

# If you want to use all of the field:

# allowedFieldList=RUM_USER_NAME,RUM_CLIENT_ADDRESS,RUM_CLIENT_NAME,RUM_DOMAIN_
NAME

# Optionally, you can specify an alias for those fields, use (shorter_name)
syntax:

# allowedFieldList=RUM_USER_NAME(RUNAME), RUM_CLIENT_ADDRESS(RCADDR), RUM_
CLIENT_NAME(RCLIENT)

# By default, we do not publish RUM_DOMAIN_NAME

allowedFieldList=RUM_USER_NAME, RUM_CLIENT_ADDRESS, RUM_CLIENT_NAME
```

As one can see, by default, `RUM_DOMAIN_NAME` is not published anymore, as the field is not used in either User Name Detection or Real User IP detection. `RUM_CLIENT_NAME` also could be eliminated from the list, since User Name Detection is configured solely by `RUM_USER_NAME` (see *To configure Real User Monitor to use the IP of the real user connected to a XenApp server as the client IP in the web application* in "[Configurations for Working with the RUM VDI Agent for HTTP Traffic](#)" on page 263).

Using field aliases, you can save some more space in the User-Agent header. For example, if you enter:

```
allowedFieldList=RUM_USER_NAME(RUNAME), RUM_CLIENT_ADDRESS(RCADDR)
```

the following appears in the User-Agent header:

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; RUNAME=<john_smith>;RCADDR=IPV4*<11.22.33.44>)
```

Renaming the fields affects the User Name detection and Real User IP detection. Therefore, you need to edit the contents of the 'Between' field in the User Name Detection dialog box, and the `forwarded_for_header` variable. In our example :

1. In the User Name Detection dialog box, configure the following:

Field	Value
Search in	HTTP Header
Header name	User-Agent
Extract Text	
Between	RUNAME=
and	;

2. Add the following line at the end of the [Global] section:

```
forwarded_for_header User-Agent .*RCADDR=IPV4\\*([\^;]*) ;.* $1
```

To turn on logging

In the **[common]** section of the file, change the **enableLog** parameter value to **true**.

Log files are located in the `<COMMONAPPDATA>\HP\RumHttpAgent\logs` directory, where `<COMMONAPPDATA>` is the file system directory that contains application data for all users. (This directory differs between operating systems. For example, in Windows 7 it is `C:\ProgramData`, and for Windows XP it is `C:\Documents and Settings\All Users\Application Data`.)

Using the RUM VDI Agent with Terminal Services for HTTP Traffic

The RUM VDI Agent can be used with Terminal Sessions in a similar way as with Citrix. If an end user is browsing a web application via a Remote Desktop connection, the RUM VDI Agent can be used to extract the real client's IP address and user name when monitoring the web traffic with RUM.

Chapter 19: Supporting ISO8583 Based Protocols

ISO8583 is the standard for building financial communication protocols. However, this standard does not cover all aspects of a particular implementation. Some things (such as optional headers and field

definitions) need to be defined according to your implementation.

RUM provides ISO8583 core support as well as two implementations (MasterCard and Visa) which are supported out of the box. RUM also has a mechanism to adapt the custom flavor of the protocol.

Note: There are different implementations of Visa/MasterCard protocol. Only part of them are supported by RUM. In order to verify if your specific implementation is supported by RUM, record a PCAP file and open a support ticket.

Monitoring ISO8583-based protocols can be supported either with standard or custom templates. If you have a custom implementation, you need to change the configuration files to adapt to your implementation.

If the custom protocol implementation is not supported with standard templates, you can customize the template as follows:

1. Locate the documentation for the custom implementation of the protocol.
2. In RUM probe `/etc/rum_probe/protocols`, open the file **MC.xml** or **VisaNet.xml** and change the protocol specification.
3. Use the modified version of the template to monitor the application.

If there are several versions of the protocol and all of them have to be monitored with the same RUM Probe instance, you need to have dedicated templates and configurations on BSM, RUM Engine, and RUM Probe.

ISO8583 includes a variety of custom flavor implementations some of which are supported by RUM. We recommend consulting HP Support at an early development stage to provide support of custom flavor implementations.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Real User Monitor Administration Guide (Real User Monitor 9.25)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to SW-doc@hp.com.

We appreciate your feedback!