HP Business Service Management

for the Windows and Linux operating systems

Software Version: 9.12

Real User Monitor Administration

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 Notices

© Copyright 2005 - 2011 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:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

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

HP Software online 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:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Table of Contents

PART II: INSTALLING HP REAL USER MONITOR

PART IV: SUPPORTING SPECIFIC PROTOCOLS

Welcome to This Guide

This guide provides detailed instructions on how to install, configure, and administer the HP Real User Monitor data collector.

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 HP Real User Monitor.

This chapter includes:

➤ How This Guide Is Organized on page 11

➤ Who Should Read This Guide on page 12

➤ How Do I Find the Information That I Need? on page 13

➤ Additional Online Resources on page 14

➤ Documentation Updates on page 15

How This Guide Is Organized

The guide contains the following parts:

Part I   **HP Real User Monitor Introduction and System Requirements**

Introduces HP Real User Monitor and the platform system requirements, and explains how HP Real User Monitor works.

Part II   Installing HP Real User Monitor

Explains how to install and uninstall the HP Real User Monitor engine. Also explains how to install one or more HP Real User Monitor probes.

Part III   Configuring and Administering HP Real User Monitor

Explains how to configure an HP Real User Monitor probe by changing the default settings as well as how to configure and administer the HP Real User Monitor engine and how to administer HP Real User Monitor's MySQL database. Also provides guidelines for hardening HP Real User Monitor.

Part IV   Supporting Specific Protocols

Explains how to configure and work with HP Real User Monitor for monitoring specific protocols.

Who Should Read This Guide

This guide is intended for the following users of HP Business Service Management:

➤ HP Business Service Management administrators

➤ HP Business Service Management data collector administrators

Readers of this guide should be knowledgeable about enterprise system administration and HP Business Service Management data collectors.

How Do I Find the Information That I Need?

This guide is part of the HP Business Service Management Documentation Library. This Documentation Library provides a single-point of access for all Business Service Management documentation.

You can access the Documentation Library by doing the following:

➤ In Business Service Management, select **Help** > **Documentation Library**.

➤ From a Business Service Management Gateway Server machine, select **Start** > **Programs** > **HP Business Service Management** > **Documentation**.

Additional Online Resources

Troubleshooting & Knowledge Base accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help** > **Troubleshooting & Knowledge Base**. The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp.

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport user ID, go to:

http://h20229.www2.hp.com/passport-registration.html

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

Documentation Updates

HP Software is continually updating its product documentation with new information.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals).

Part I

HP Real User Monitor Introduction and System Requirements

1

Introducing HP Real User Monitor Administration

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

This chapter includes:

Overview of HP Real User Monitor

HP Real User Monitor 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 proactively alerts application managers who, using the HP Real User Monitor 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 Real User Monitor to monitor applications, see "How to Set up Real User Monitors" in *Using End User Management*.

How the HP Real User Monitor Works

HP Real User Monitor consists of three major components: the probe, the engine, and the MySQL database.

➤ The **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.

➤ 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, 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 HP Business Service Management Gateway Server. The HP Business Service Management Gateway Server then distributes the data to the relevant HP Business Service Management components, which create HP Real User Monitor alerts, reports, and Service Health views.

Note: If the HP Real User Monitor engine fails or is temporarily unavailable, or is unable to copy data from the HP Real User Monitor probe, the HP Real User Monitor probe continues to collect data. The last two hours worth of data is saved on the HP Real User Monitor probe and this data is copied by the HP Real User Monitor engine when it becomes available again.

➤ The **MySQL database** acts as HP Real User Monitor's repository for data that the HP Real User Monitor engine does not forward to HP Business Service Management immediately, or at all. The MySQL database stores the HP Real User Monitor engine's configuration settings, session click-streams (pages and snapshots included in a session), and the open sessions summary.

The following diagram shows how HP Real User Monitor receives client-server and server-server traffic and passes it on to HP Business Service Management.
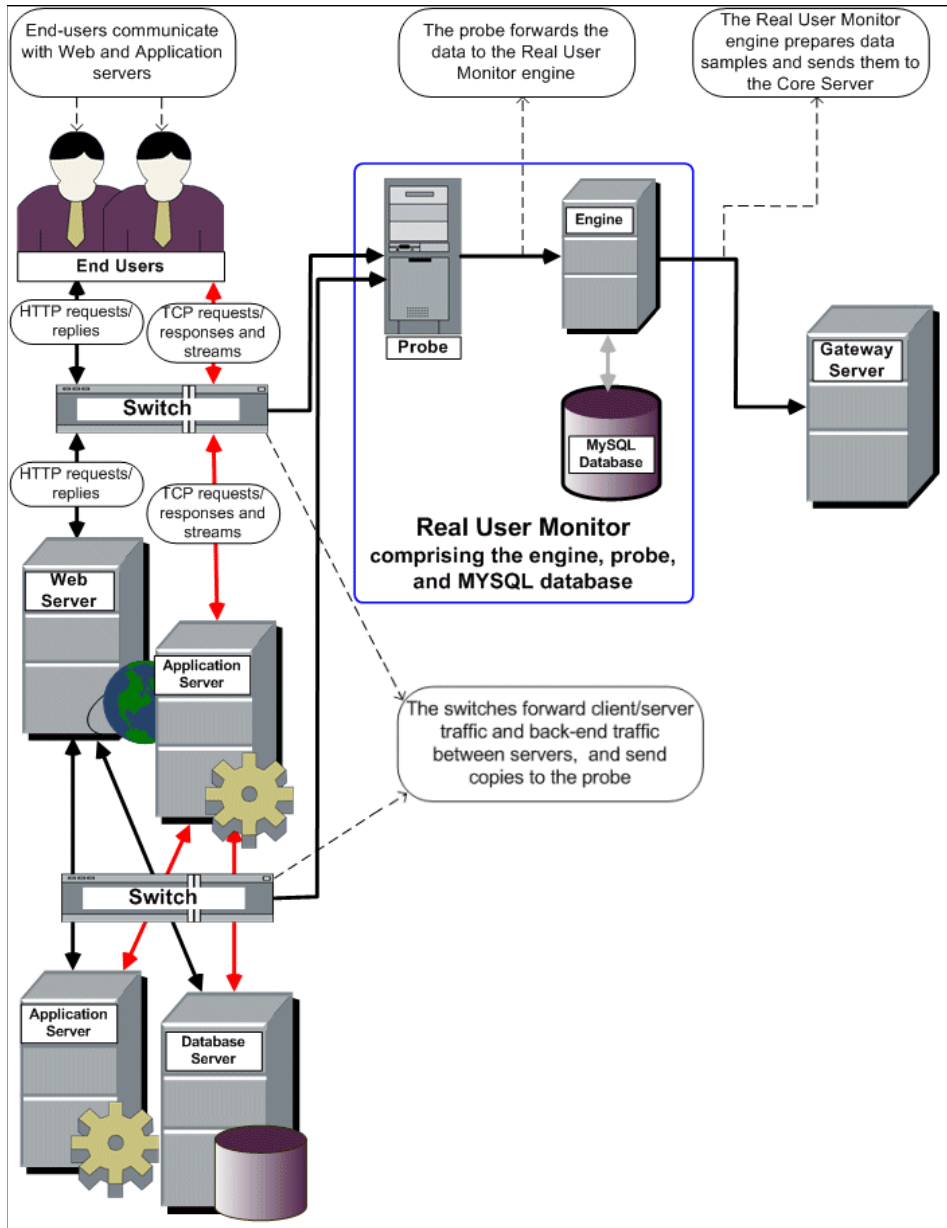
Use the HP Real User Monitor reports to analyze network and application performance and availability data for the servers, applications, pages, transactions, events, and end users that you configure for monitoring, as well as general statistics that are collected and sent by the probes to the engine. 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 HP Real User Monitor reports, see "End User Management Reports" in *Using End User Management.*

In addition, HP Real User Monitor data is included in Service Health. For information on displaying HP Real User Monitor data in Service Health, see "Predefined Views for End User Management" in *Using End User Management.*

Ports and Types of Communication Used by HP Real User Monitor

The following diagram shows the various ports and type of communications used by HP Real User Monitor, both internally and externally.

* If the Real User Monitor engine is configured to communicate with the Gateway Server via SSL, this port may change. The default port for SSL is 443.
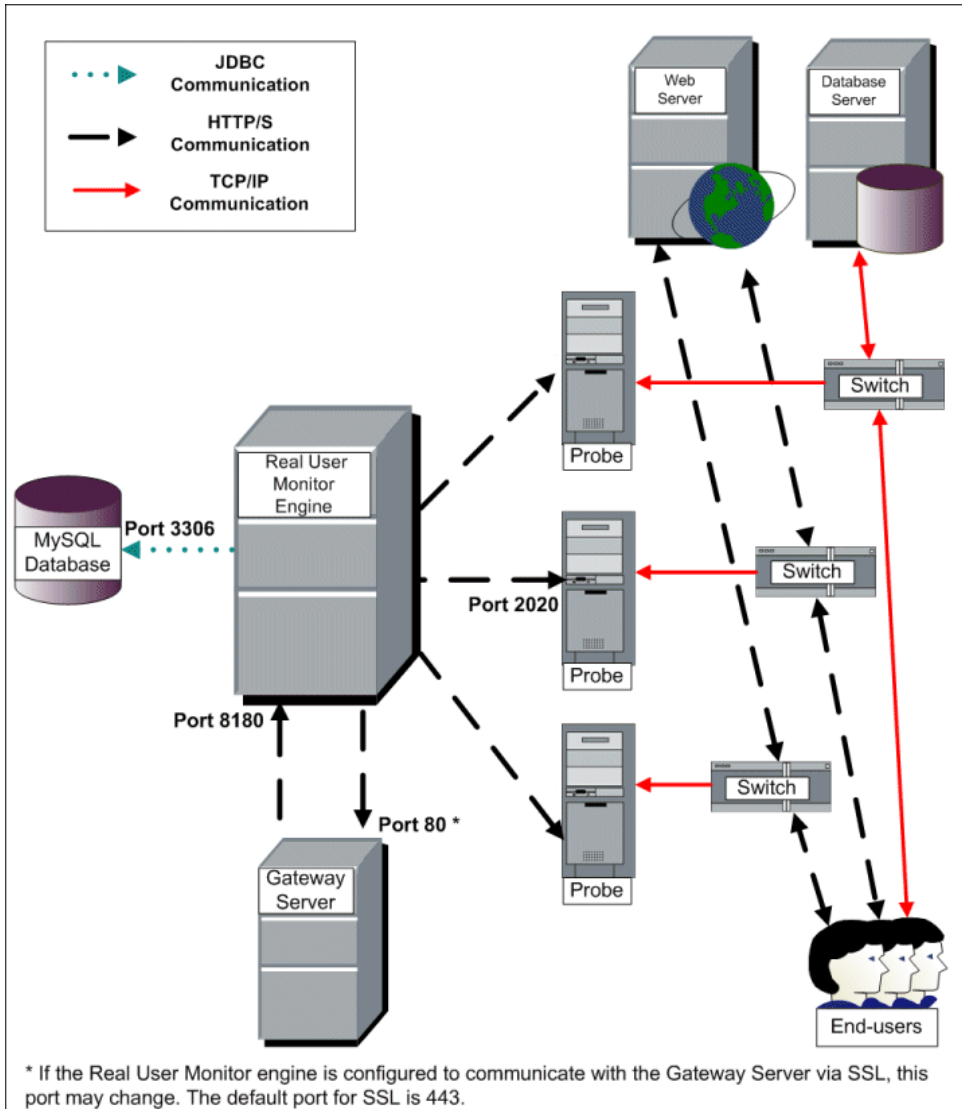
Note:

➤ The HP Business Service Management Gateway Server initiates a connection to the Real User Monitor engine on port 8180 for retrieving various types of data.

➤ The Real User Monitor engine initiates a connection to the HP Business Service Management Gateway Server on port 80 (default) for sending samples.

➤ The Real User Monitor engine initiates a connection to the Real User Monitor probe on port 2020 for https (which is the default type of communication in Real User Monitor version 7.0 and later) and http.

➤ The Real User Monitor probe does not initiate a connection to any other server in the system.

➤ There is no direct connection from HP Business Service Management to the Real User Monitor probe.

➤ By default, the Snapshot Replay applet retrieves data to a user's machine via an HP Business Service Management server. You can configure the applet to retrieve data directly from the Real User Monitor 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 *Using End User Management*.

Overview of HP Real User Monitor Performance Measurements

This section describes the measurements provided by HP Real User Monitor for the data that it monitors.

This section includes the following topics:

Introduction to Performance Measurements

To understand HP Real User Monitor 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.** 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 HP Real User Monitor 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).
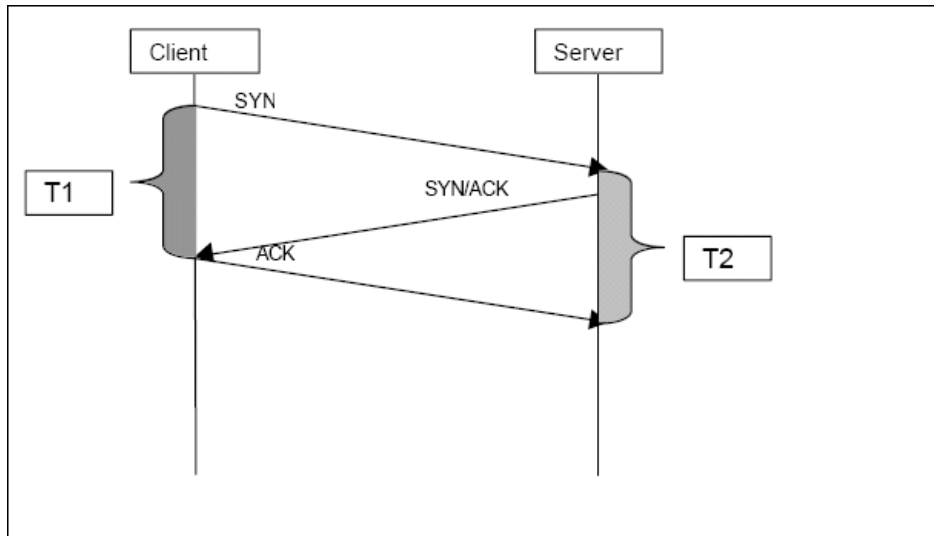
TCP Request-Response Measurements

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 HP Real User Monitor:

➤ **Average Response Time.** The time from the first packet of the request, until client acknowledgement of the last packet of the response. Average download time is the sum of average server time and average network time.

➤ **Average Server Time.** By understanding the TCP protocol, HP Real User Monitor 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 average server time. This measurement is better than server time to first buffer as it considers all of the response time.

➤ **Average Network Time.** The time intervals that were spent by the server waiting for client acknowledgement to arrive are incorporated into the average network time.

HTTP Measurements

HTTP measurements are used by HP Real User Monitor to report page and transaction data to HP Business Service Management.

This section includes the following topics:

Page Performance Measurements

The following table describes the performance measurements of pages that appear in HP Real User Monitor 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.	N/A
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 HP Business Service Management, 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 HP Real User Monitor:

➤ **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.

➤ **Component Server Time.** By understanding the TCP protocol, HP Real User Monitor 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 is better than server time to first buffer as it considers all of the response time.

➤ **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.

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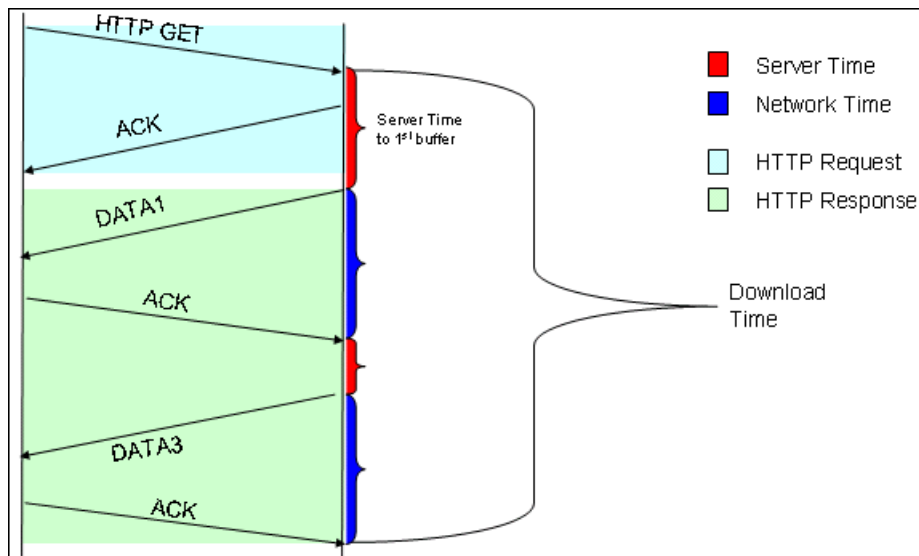
Page Measurements

Each HTML page can contain sub-components (such as GIFs, JPGs, and so forth). HP Real User Monitor 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 HP Real User Monitor:

➤ **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, HP Real User Monitor users relative measurements for page breakdown:
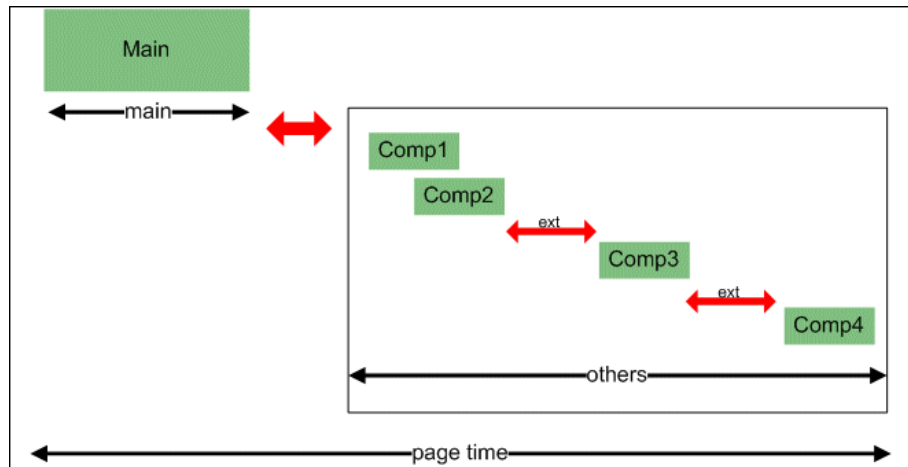
➤ **Page client/external time.** A collection of all the time intervals in the page time in which no component was downloaded. These gaps, which are shown in red in the above diagram, are usually caused by client application processing (such as JavaScript).

➤ **Page Server Time.** The relative part of the Page Time that was spent on server processing. The formula used to calculate this is:

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

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

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

Transaction Measurements

An HP Real User Monitor transaction consists of a series of pages. A transaction is matched when HP Real User Monitor has monitored all the pages in the series in the correct order.

The following transaction measurements are used in HP Real User Monitor:

➤ **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) for a packet between the server and the client. This calculation is made only for packets that were not delayed because of server or client processing, as server time and client time are not part of the latency measurement.

Installing and Administering HP Real User Monitor

To begin using HP Real User Monitor, you must perform the following steps (once you have installed HP Business Service Management):

1 Install the HP Real User Monitor engine.

For information on installing the HP Real User Monitor engine and setting up the engine to connect to the Gateway Server, see "Installing the HP Real User Monitor Engine" on page 49.

2 Create and connect to the MySQL database.

You can create and connect to the MySQL database either as part of the HP Real User Monitor engine installation procedure or separately, at a later time. For details on creating the MySQL database as part of the HP Real User Monitor engine installation procedure, see "Installing the HP Real User Monitor Engine" on page 49. For details on creating the MySQL database at a later time, see "Overview of the MySQL Database" on page 299.

3 Install one or more HP Real User Monitor probes.

For information on installing an HP Real User Monitor probe and setting it up to report real-user activity data to the engine, see "Installing the HP Real User Monitor Probe" on page 77.

 4 If necessary, reconfigure the connection between the HP Real User Monitor and HP Business Service Management.

 If connection parameters (such as SSL, proxy, and authentication) have changed since the installation of HP Business Service Management, use the HP Real User Monitor engine's Web console to reconfigure the connection between the HP Real User Monitor and HP Business Service Management. For detailed information, see "Using the HP Real User Monitor Web Console" on page 137.

 5 Configure HP Real User Monitor in HP Business Service Management 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 *Using End User Management*.

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

2

Reviewing System Requirements

This section describes the recommended system requirements for running HP Real User Monitor.

This chapter includes:

HP Real User Monitor Engine Requirements

	Minimum	Recommended
Computer/Processor	Dual-CPU Xeon 3.0 GHz Server	Dual-CPU Xeon 3.0 GHz Dual-Core Server
Operating System	**Windows:**	**Windows:**
	Microsoft Windows Server 2003 SP2 (32/64 bit) Standard and Enterprise Editions	Microsoft Windows Server 2003 SP2 (32/64 bit) Standard and Enterprise Editions
	Microsoft Windows Server 2003 R2 (32/64 bit) Standard and Enterprise Editions	Microsoft Windows Server 2003 R2 (32/64 bit) Standard and Enterprise Editions
	Microsoft Windows Server 2008 SP2 (32/64 bit) Standard and Enterprise Editions	Microsoft Windows Server 2008 SP2 (32/64 bit) Standard and Enterprise Editions
	Microsoft Windows Server 2008 R2 (32/64 bit) Standard and Enterprise Editions	Microsoft Windows Server 2008 R2 (32/64 bit) Standard and Enterprise Editions
	Microsoft Windows Server 2008 R2 SP1 (32/64 bit) Standard and Enterprise Editions	Microsoft Windows Server 2008 R2 SP1 (32/64 bit) Standard and Enterprise Editions
Memory	2 GB	4 GB
Hard Drive	70 GB	70 GB
Network Card	Gigabit network adaptor	2 Gigabit network adaptors (one for database connectivity and one for probe connectivity)

HP Real User Monitor Repository (MySQL Database) Requirements

	Minimum	Recommended
Computer/Processor	Dual-CPU Xeon 3.0 GHz Server	Dual-CPU Xeon 3.0 GHz Server
Operating System	**Windows:** Microsoft Windows Server 2003 SP2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2003 R2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 SP2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 SP1 (32/64 bit) Standard and Enterprise Editions	**Windows:** Microsoft Windows Server 2003 SP2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2003 R2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 SP2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 SP1 (32/64 bit) Standard and Enterprise Editions
Memory	2 GB	4 GB
Hard Drive	200 GB fast hard drive	400 GB SCSI disks RAID 0 (RAID 0 + 1 for high availability)
Network Card	Gigabit network adaptor	Gigabit network adaptor
MySQL Version	5.1 (installed by the HP Real User Monitor installation program)	5.1 (installed by the HP Real User Monitor installation program)

Requirements for Installing the HP Real User Monitor Engine and Repository (MySQL Database) on the Same Machine

	Minimum	Recommended
Computer/Processor	Quad-CPU Xeon 3.0 GHz Server	Quad-CPU Xeon 3.0 GHz Dual-Core Server
Operating System	**Windows:** Microsoft Windows Server 2003 SP2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2003 R2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 SP2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 SP1 (32/64 bit) Standard and Enterprise Editions	**Windows:** Microsoft Windows Server 2003 SP2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2003 R2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 SP2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 SP1 (32/64 bit) Standard and Enterprise Editions
Memory	4 GB	4 GB

	Minimum	Recommended
Hard Drive	2 Disks: ➤ 70 GB for the Real User Monitor engine installation ➤ 200 GB fast hard drive for the Real User Monitor repository	2 Disks: ➤ 70 GB for the Real User Monitor engine installation ➤ 400 GB SCSI disks RAID 0 (RAID 0 + 1 for high availability) for the Real User Monitor repository.
	Note: It is important not to install the Real User Monitor engine on the same disk as the Real User Monitor repository. You must select a different disk for the Real User Monitor repository during the installation.	
Network Card	Gigabit network adaptor	Gigabit network adaptor

HP Real User Monitor Probe Requirements

Hardware and Operating System Requirements

	Minimum	Recommended
Computer/Processor	Dual-CPU Xeon 3.0 GHz Server	Dual-CPU Xeon 3.0 GHz Server
	Note: For Windows installations, you can install an HP Real User Monitor probe on the same machine as an HP Real User Monitor engine if the environment is a very low traffic one.	

	Minimum	Recommended
Operating System	**Linux:** Red Hat Enterprise Linux Version 5.0 (RHEL5) – 64 and 32 bit versions Version 4.0 (RHEL4) – 32 bit versions **Windows:** Microsoft Windows Server 2003 SP2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2003 R2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 SP2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 SP1 (32/64 bit) Standard and Enterprise Editions	**Linux:** Red Hat Enterprise Linux Version 5.0 (RHEL5) – 64 and 32 bit versions **Windows:** Microsoft Windows Server 2003 SP2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2003 R2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 SP2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (32/64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 SP1 (32/64 bit) Standard and Enterprise Editions
Memory	2 GB	**Windows and Linux 32 bit:** 4 GB **Linux 64 bit:** 8 GB

	Minimum	Recommended
Hard Drive	70 GB IDE/SATA	150 GB SCSI
		SCSI required for high traffic levels of more than 15 MB.
		Large disk space required for more than one page back on Snapshot on Error (SSOE).
	Note: For Linux installations, it is recommended to allocate most of the disk space to the **/var/spool/rum_probe** directory, as this directory contains the majority of the probe data. It is sufficient to allocate 10 GB of space each to the **/var/log/rum_probe** and **/etc/rum_probe** directories.	

	Minimum	Recommended
Network Card	**For connecting port mirrored cable:** 1 Intel Pro/1000 (10/100/1000 auto-sensing) **For connecting to management port (used by RUM engine):** 1 Intel Pro/100 (10/100 auto-sensing) set for full duplex For copper connections, MT type card required. For fiber optic connections, MF type card required.	**For connecting tap:** 2 Intel Pro/1000 (10/100/1000 auto-sensing) **Note:** Two network cards are required if the TAP to which the Real User Monitor probe is connected uses different ports for transmitting and receiving data. You can also use two network cards to monitor traffic from two separate sources, providing bandwidth restrictions are not exceeded. **For connecting to management port (used by RUM engine):** 1 Intel Pro/100 (10/100 auto-sensing) set for full duplex For copper connections, MT type card required. For fiber optic connections, MF type card required.
PCI Slot		1 free 133/100/66 MHz 64 bit PCI slot

Environment and System Requirements

Requirement	Description
Linux installations only:	

Probe watchdog prerequisites	The following are required for the probe watchdog and must be installed on the Linux machine prior to installing the RUM probe:
	
	➤ libcrypto.so
	➤ libssl.so
	Note: These libraries are part of the openssl package.
	
	➤ Perl must be installed with the following libraries:
	    ➤ LWP::UserAgent
	    ➤ URI::URL

rum_probe user	A user called **rum_probe** is automatically created during installation, but you must manually configure a password for this user. When entering the HP Real User Monitor probe user and password in End User Management Administration, you must use either the **root** or **rum_probe** user (for details, see "New/Edit Real User Monitor Engine Page" in *Using End User Management*).
Permissions	The following directories must have **2770** permissions, be owned by **rum_probe** and belong to the **rum_probe** group: ➤ /var/spool/rum_probe (and subdirectories) ➤ /etc/rum_probe ➤ /var/log/rum_probe
Linux and Windows installation:	
Probe console port	Port 2020 is the default port used for accessing the HP Real User Monitor probe console. By default, HTTPS with client certificate is used.

Real User Monitor on Virtual Platforms

You can install both the Real User Monitor Engine and Probe on a virtual platform. The following virtualization platforms are supported:

➤ VMware ESX 3.x

➤ VMware ESX 4.x

For details on duplicating traffic for a Real User Monitor Probe on a virtual machine, see "Duplicating Traffic for HP Real User Monitor with VMware" on page 105.

Part II

Installing HP Real User Monitor

3

Installing the HP Real User Monitor Engine

To monitor real user activity, you must first install the HP Real User Monitor (RUM) engine on a Windows platform.

You download the RUM engine installation file from the Downloads page, which you access from the Setup and Maintenance tab in Platform Administration.

The RUM installation procedure installs both the RUM engine and the MySQL database. You can install both the engine and the database on the same machine, or on different machines. To install the engine and database on different machines, install the MySQL database first and then install the engine and connect it to the database.

Note: Before beginning the installation, review the information in the RUM Readme file for any last minute notes and limitations, as well as for upgrade and service pack install instructions.

This chapter includes:

Installing the HP Real User Monitor Engine

For details on the system requirements for installing the HP Real User Monitor (RUM) engine, see "HP Real User Monitor Engine Requirements" on page 38.

Note: Before installing the RUM engine on Windows 2008 using Windows Remote Desktop, refer to "Installing Real User Monitor on Windows 2008 Using Windows Remote Desktop" on page 69.

Tip: For better performance, we recommend installing the RUM engine and the RUM probe on the same local area network (LAN).

To install the RUM engine:

1 Click the **HP Real User Monitor Engine for Windows** link on the Downloads page to download the **HPRumEngine_<version number>_ setup.exe** file to the machine on which you want to install the engine.

Note: For the RUM engine setup file to be available on the Downloads page, it must first be installed to HP Business Service Management (BSM). For details on installing BSM components setup files, see "Installing Component Setup Files" in the *HP Business Service Management Deployment Guide* PDF.

If you prefer, you can copy the RUM engine setup program directly from the Data Collectors and Components directory on the BSM DVD, for versions delivered on DVD.

---

2 On this machine, navigate to the downloaded file and double click **HPRUMEngine_<version number>_setup.exe**.

3 When prompted, select the installation language (default English) and click **OK**. The HP Real User Monitor Engine Setup wizard begins.

4 When the Introduction page is displayed, click **Next**.

5 Accept the terms of the license agreement and click **Next**.

6 Select whether to run a typical installation (which installs both the RUM engine and the MySQL database), or a custom installation (in which you select specific features to install). Click **Next**.

If you select **Typical** installation, skip to step 8 on page 52 to continue.

Note: You are able to select the installation path in both types of installations (typical and custom).

---

7 Select the features you want to install from the following, by checking the box to the left of the required feature:

➤ **HP RUM - Core.** Installs the RUM engine.

➤ **HP RUM - DB.** Installs the MySQL database.

➤ **HP RUM - Common.** Installs common components required by both the RUM engine and the MySQL database. (This feature is selected by default and you cannot change the selection.)
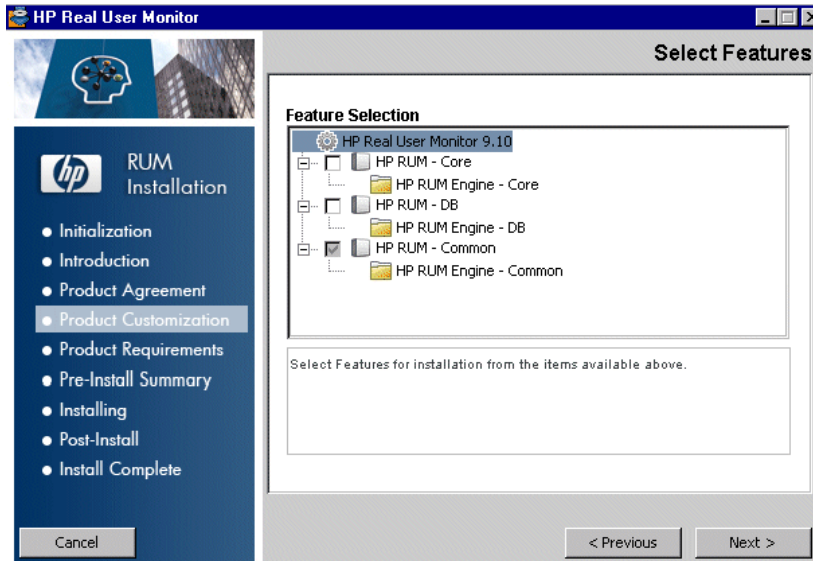
Click **Next**.

Note: If you select **HP RUM DB** only, the MySQL database is installed in the specified location, but no database schema is created.

8 Select the path of the folder in which you want to install the RUM engine. Either accept the default path (**C:\HPRUM**), or click **Browse** to create a new folder in a different path. (You can reset the path to the default folder by clicking **Reset**.) Click **Next**.

Note:

➤ Do not use non-ASCII characters in the RUM installation path.

➤ Do not select an existing folder.

9 The Setup wizard verifies the following system parameters and displays the verification details:

➤ Free disk space

➤ Previous RUM installations

➤ Selected components for installation

➤ The installation directory (which should be a new directory)

If any of the verification checks fail, go back and make the necessary corrections according to the information displayed (for example, free up more disk space, or change the selected components).

10 Read the pre-install summary information. If it is correct, click **Install** to continue with the installation. If it is not correct, click **Previous** to correct the information you previously provided.

 11 The installation begins and its progress is displayed. You can choose whether to view summary or detailed progress data, by clicking the appropriate tab.
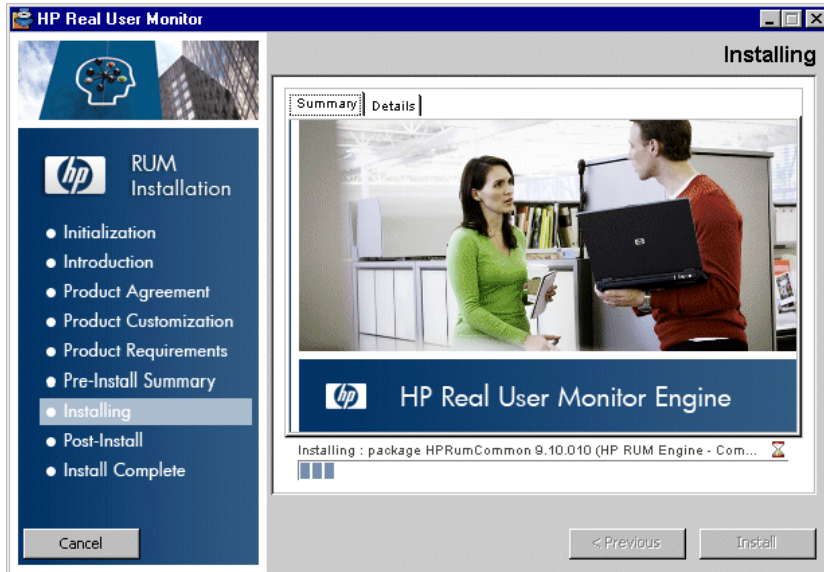
When the installation has finished, the HP Real User Monitor Configuration wizard is automatically started. The wizard includes the following pages:

Page	Enables you to ...	For user interface details, see ...
MySQL Database Properties	Configure the path in which the MySQL database is installed, as well as the user name and password for accessing the database.	"MySQL Database Properties Page" on page 57
Import User Configuration Data	Select whether you want to import user data settings from a previous RUM installation.	"Import User Configuration Data Page" on page 59
Import Source Directory	Select the path from which to import user data settings from a previous RUM installation.	"Import Source Directory Page" on page 61

Page	Enables you to ...	For user interface details, see ...
Connect to Database	Configure whether to connect the RUM engine to a MySQL database.	"Connect to Database Page" on page 62
RUM Database Connection Parameters	Configure the parameters used by the RUM engine to connect to its MySQL database.	"RUM Database Connection Parameters Page" on page 64
RUM Engine Credentials	Configure the credentials that the RUM engine uses to connect to the JMX and Web consoles.	"RUM Engine Credentials Page" on page 66
Finish	View the status of the Configuration wizard.	"Finish Page" on page 68

12 When the Real User Monitor Configuration wizard has finished, the status of the HP Real User Monitor Engine Setup wizard is displayed. You can choose whether to view summary or detailed status data. You can view the installation log file by clicking the **View log file** link.

13 Click **Done** to exit the Setup wizard.

After successfully installing the RUM engine and connecting the engine to the MySQL database, start RUM on the machine on which it is installed and configure the connection settings to BSM.

To start RUM and configure connection settings:

1 Start RUM by selecting **Start** > **Programs** > **HP Real User Monitor** > **Administration** > **Enable HP Real User Monitor**.

Note: You can stop RUM by selecting **Start** > **Programs** > **HP Real User Monitor** > **Administration** > **Disable HP Real User Monitor**.

For additional information on starting and stopping RUM, see "Administering HP Real User Monitor" on page 99.

---

2 Configure the connection settings to BSM in the RUM Web Console. For details, see "BSM Connection Settings" on page 185.

Real User Monitor Configuration Wizard

Description	Enables you to import configuration data from a previous Real User Monitor (RUM) installation, as well as to configure various connection parameters.
	To access: The Real User Monitor Configuration wizard is automatically launched during a RUM installation, after the setup program has installed the RUM application.
Wizard Map	The Real User Monitor Configuration wizard contains:
	MySQL Database Properties Page > Import User Configuration Data Page > Import Source Directory Page > Connect to Database Page > RUM Database Connection Parameters Page > RUM Engine Credentials Page > Finish Page
Useful Links	"Installing the HP Real User Monitor Engine" on page 50

MySQL Database Properties Page

The following is an example of the MySQL Database Properties page.

Description	Enables you to configure the path in which the MySQL database is installed, as well as the user name and password for accessing the database.

Important Information	➤ General information about the wizard is available in "Real User Monitor Configuration Wizard" on page 56.
	➤ If you are installing the MySQL database only, after completing this page and clicking **Next**, the wizard continues with the Finish page and the other wizard pages are not accessed.
	➤ If you are installing the RUM engine only, this wizard page is not accessed and the wizard starts with the Import Source Directory page.
Wizard Map	The Real User Monitor Configuration Wizard contains:
	MySQL Database Properties Page > Import User Configuration Data Page > Import Source Directory Page > Connect to Database Page > RUM Database Connection Parameters Page > RUM Engine Credentials Page > Finish Page

The following elements are included:

UI Element	Description
MySQL installation path	The path in which to install the MySQL database.
	Note: The path should be for a directory that does not already exist, or for a directory that already contains a MySQL database.
User name	The user name for accessing the MySQL database.
	Default value: rum_user
Password	The password for accessing the MySQL database.
Verify password	Retype the password for verification.

Import User Configuration Data Page

The following is an example of the Import User Configuration Data page.

Description	Enables you to select whether you want to import user data settings from a previous RUM installation.
Important Information	General information about the wizard is available in "Real User Monitor Configuration Wizard" on page 56.
Wizard Map	The Real User Monitor Configuration Wizard contains: MySQL Database Properties Page > **Import User Configuration Data Page** > Import Source Directory Page > Connect to Database Page > RUM Database Connection Parameters Page > RUM Engine Credentials Page > Finish Page

The following elements are included:

UI Element	Description
Import	Select this radio button if you want to import user data settings that you exported when uninstalling a previous version of RUM.
	Note:
	➤ If you want to include settings from an earlier version as part of a RUM upgrade, you must import the user data settings you saved when uninstalling the previous version.
	➤ If you import user data settings from a previous installation of RUM, the RUM Engine Credentials page is not accessed in the wizard.
Do not import	Select this radio button if you do not want to import configuration settings from a previous version of RUM.
	Note: If you select this option, the wizard continues with the "Connect to Database Page" on page 62.

Import Source Directory Page

The following is an example of the Import Source Directory page.

Description	Enables you to select the path from which to import user data settings from a previous RUM installation.
Important Information	General information about the wizard is available in "Real User Monitor Configuration Wizard" on page 56.
Wizard Map	The Real User Monitor Configuration Wizard contains: MySQL Database Properties Page > Import User Configuration Data Page > **Import Source Directory Page** > Connect to Database Page > RUM Database Connection Parameters Page > RUM Engine Credentials Page > Finish Page

The following elements are included (unlabeled UI elements are shown in angle brackets):

UI Element	Description
<Source directory>	Enter the source directory from which user configuration data will be imported. You can click **Browse** to locate and select a directory.

Connect to Database Page

The following is an example of the Connect to Database page.
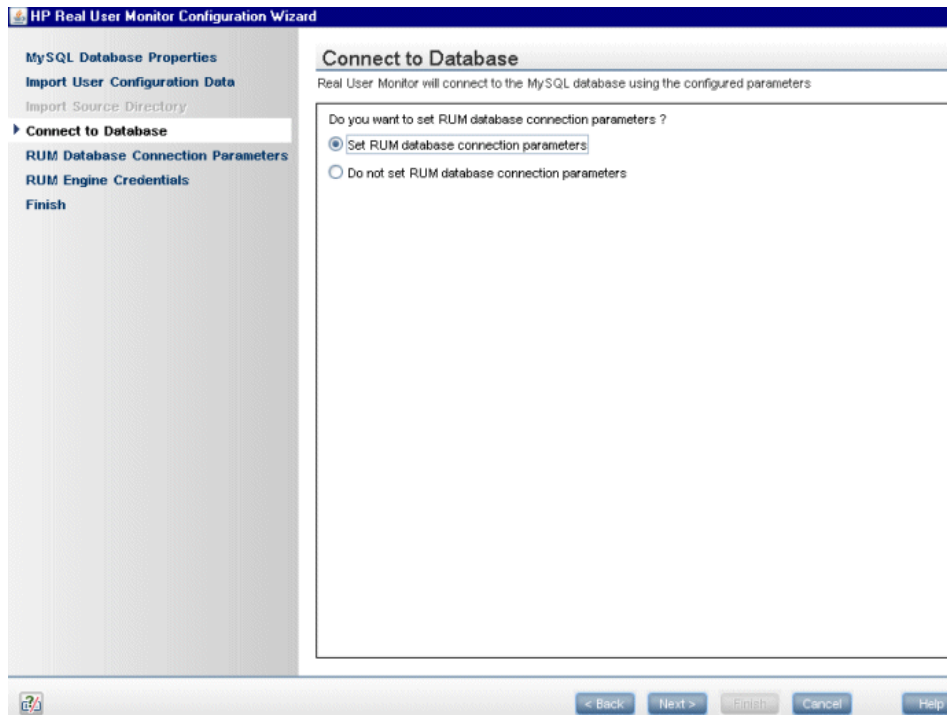
Description	Enables you to configure whether to connect the RUM engine to a MySQL database.
Important Information	General information about the wizard is available in "Real User Monitor Configuration Wizard" on page 56.
Wizard Map	The Real User Monitor Configuration Wizard contains:
	MySQL Database Properties Page > Import User Configuration Data Page > Import Source Directory Page > **Connect to Database Page** > RUM Database Connection Parameters Page > RUM Engine Credentials Page > Finish Page

The following elements are included:

UI Element	Description
Set RUM database connection parameters	Select this radio button to configure connection parameters and connect the RUM engine to a MySQL database.
Do not set RUM database connection parameters	Select this radio button if you do not want to connect the RUM engine to a MySQL database.
	Note:
	➤ If you select this option, the wizard continues with the "RUM Engine Credentials Page" on page 66.
	➤ You can connect to a MySQL database, or change an existing connection, after installing RUM, by running the RUM Configuration wizard (**Start** > **All Programs** > **HP Real User Monitor** > **Administration** > **HP Real User Monitor Configuration Tool**).

RUM Database Connection Parameters Page

The following is an example of the RUM Database Connection Parameters page.

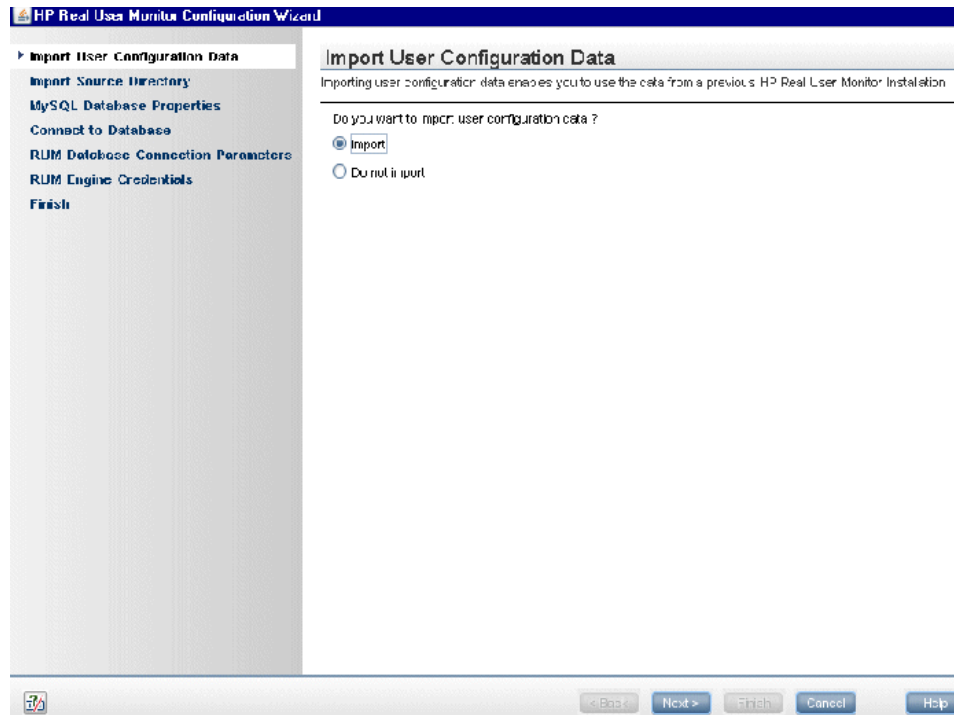| Description	Enables you to configure the parameters used by the RUM engine to connect to its MySQL database.
Important Information	General information about the wizard is available in "Real User Monitor Configuration Wizard" on page 56.
Wizard Map	The Real User Monitor Configuration Wizard contains:
	MySQL Database Properties Page > Import User Configuration Data Page > Import Source Directory Page > Connect to Database Page > **RUM Database Connection Parameters Page** > RUM Engine Credentials Page > Finish Page

The following elements are included:

UI Element	Description
Connect to an existing schema	Select this check box if you want to connect to an existing schema. Clear this check box if you want to create a new schema. **Default value:** Not selected **Note:** When upgrading from an earlier version of RUM, you must connect to the previous, existing schema.
Host name	The host name of the machine where the MySQL database resides. **Default value:** localhost
Port	The port number for accessing the host machine. **Default value:** 3306
User name	The configured user name for connecting to the MySQL database. This must match the user name that you configured as part of the database parameters in the "MySQL Database Properties Page" on page 57.
Password	The configured password for connecting to the MySQL database. This must match the password that you configured as part of the database parameters in the "MySQL Database Properties Page" on page 57.
Schema name	The name for the existing MySQL database schema to which you want the RUM engine to connect, or the name of the new schema you want it to create. **Syntax exceptions:** ➤ The name must begin with a letter or digit. ➤ The name cannot contain the characters: ; ` { } ➤ The name cannot end with a space.

RUM Engine Credentials Page

The following is an example of the RUM Engine Credentials page.

Description	Enables you to configure the credentials that the RUM engine uses to connect to the JMX and Web consoles.
Important Information	➤ General information about the wizard is available in "Real User Monitor Configuration Wizard" on page 56. ➤ If you imported user data settings from a previous RUM installation, this wizard page is not accessed.
Wizard Map	The Real User Monitor Configuration Wizard contains: Import User Configuration Data Page > Import Source Directory Page > MySQL Database Properties Page > Connect to Database Page > RUM Database Connection Parameters Page > **RUM Engine Credentials Page** > Finish Page

The following elements are included:

UI Element	Description
JMX console and Gateway User Password	The password for the JMX console and BSM Gateway user. **Default value:** Admin **Note:** The JMX console and Gateway password must match the password configured for the connection settings of the RUM engine in End User Management Administration. If they do not match, BSM is unable to communicate with the RUM engine to obtain data for End User Management reports. For details on configuring RUM engine connection settings in End User Management Administration, see "Edit Real User Monitor Engine Properties Dialog Box" in *Using End User Management.*
RUM Web Console User Name	The user name you use for accessing the RUM Web console. **Default value:** admin
RUM Web Console Password	The password for the RUM Web console user. **Default value:** admin
Verify password	Retype the password (JMX console and Gateway user password, or RUM Web console password) for verification.

Finish Page

The following is an example of the Finish page.

Description	Displays a message showing the status of the Configuration wizard. Click **Finish** to exit and return to the HP Real User Monitor Engine Setup wizard.
Important Information	General information about the wizard is available in "Real User Monitor Configuration Wizard" on page 56.
Wizard Map	The Real User Monitor Configuration Wizard contains:
	MySQL Database Properties Page > Import User Configuration Data Page > Import Source Directory Page > Connect to Database Page > RUM Database Connection Parameters Page > RUM Engine Credentials Page > **Finish Page**

Installing Real User Monitor on Windows 2008 Using Windows Remote Desktop

If you want to install the Real User Monitor (RUM) engine and/or MySQL database on Windows 2008 using Windows Remote Desktop, you must first install Terminal Server Role Service on the remote machine on which you want to install them and then carry out the installation using the Terminal Server.

This section includes the following topics:

➤ "To install the Terminal Server Role Service" on page 69

➤ "To install Real User Monitor using Terminal Server" on page 71

To install the Terminal Server Role Service

1 Open **Server Manager** (Start > Administrative Tools > Server Manager).

2 In the left pane, right-click **Roles** and select **Add Roles**.

3 On the **Add Roles** wizard > **Before You Begin** page, click **Next**.

4 On the **Select Server Roles** page, under **Roles**, select the **Terminal Services** check box and click **Next**.

Note: If Terminal Services is already installed on the server, the **Terminal Services** check box is selected and dimmed.

---

5 On the **Terminal Services** page, click **Next**.

6 On the **Select Role Services** page, select the **Terminal Server** check box and click **Next**.

Note: Installing the Terminal Server role service on a domain controller is not recommended. If you are installing the Terminal Server role service on a domain controller a warning message is displayed. For more information, see Installing Terminal Server on a Domain Controller in the Windows Server 2008 Technical Library (http://go.microsoft.com/fwlink/?linkid=109277).

---

 7 On the **Uninstall and Reinstall Applications for Compatibility** page, click **Next**.

 8 On the **Specify Authentication Method for Terminal Server** page, select the appropriate authentication method for the terminal server and click **Next**. For more information about authentication methods, see Configure the Network Level Authentication Setting for a Terminal Server in the Terminal Server Help in the Windows Server 2008 Technical Library (http://go.microsoft.com/fwlink/?linkid=109280).

 9 On the **Specify Licensing Mode** page, select the appropriate licensing mode for the terminal server and click **Next**. For more information about licensing modes, see Specify the Terminal Services Licensing Mode in the Windows Server 2008 Technical Library (http://go.microsoft.com/fwlink/?linkid=101638).

 10 On the **Select User Groups Allowed Access To This Terminal Server** page, add the users or user groups that you want to be able to remotely connect to this terminal server and click **Next**. For more information, see Configure the Remote Desktop User Group i in the Windows Server 2008 Technical Library (http://go.microsoft.com/fwlink/?linkid=109278).

 11 On the **Confirm Installation Selections** page, verify that the Terminal Server role service will be installed and click **Install**.

 12 The installation progress is displayed on the **Installation Progress** page.

 13 On the **Installation Results** page, you are prompted to restart the server to finish the installation process. Click **Close** and then click **Yes** to restart the server.

14 If you are prompted that other programs are still running, do one of the
following:

> ➤ To close the programs manually and restart the server later, click
>   **Cancel**.

> ➤ To automatically close the programs and restart the server, click
>   **Restart now**.

15 After the server restarts and you log on to the remote machine, the
remaining installation steps are automatically completed. When the
Installation Results page is displayed, verify that the installation was
successful.

Note: You can also confirm that Terminal Server is installed using the
following steps:

> ➤ Start S**erver Manager**.

> ➤ Under **Roles Summary**, click **Terminal Services**.

> ➤ Under **System Services**, confirm that Terminal Services has a status of
>   **Running**.

> ➤ Under **Role Services**, confirm that Terminal Server has a status of
>   **Installed**.

To install Real User Monitor using Terminal Server

On the remote machine on which you are installing Real User Monitor, in
the **Control Panel** select **Install using Terminal Server** and then select the
Real User Monitor installation file.

Follow the installation process as described in "Installing the HP Real User
Monitor Engine" on page 50.

Running a Silent Installation

You can use a silent installation procedure to run the Real User Monitor (RUM) setup. A silent installation is an installation that is performed automatically, without the need for user interaction. Instead, all configuration parameters are allocated predetermined values that are stored in a configuration file.

Note: When running an installation in silent mode, no messages are displayed. Instead, you can view installation information in the log files, including information on whether the installation was successful.

This section includes:

➤ "How a Silent Installation Assigns Values" on page 73

➤ "Prerequisites" on page 73

➤ "Silent Installation for Windows" on page 74

➤ "Configuring the RUMInstallationDefaults.properties File" on page 74

How a Silent Installation Assigns Values

A silent installation uses the following files to obtain parameter values for use during the installation:

➤ **%temp%\ovinstalllparams.ini**. This file contains values for the settings used by the setup program such as the original setup file path, the installation path, the installation type, the default maintenance mode selection, and so forth. The installation process copies this file to the machine's %temp% directory, if a file with the same name does not already exist in that location.

➤ **RUMInstallationDefaults.properties**. This file contains the parameter values used by the Real User Monitor Configuration wizard (for details, see "Real User Monitor Configuration Wizard" on page 56).

The installation process copies this file to the **<RUM installation directory>\bin** directory. (The default RUM installation directory is **C:\HPRUM**.) For a silent installation, edit this file and set the values you want the silent installation to use, and then copy the file to the machine's **%temp%** directory. For details on configuring the RUMInstallationDefaults.properties file, see "Configuring the RUMInstallationDefaults.properties File" on page 74.

Prerequisites

Before you begin a silent installation of RUM, make sure of the following:

➤ You must uninstall any previous versions of RUM from the machine on which you run the silent installation. For details on uninstalling RUM, see "Uninstalling HP Real User Monitor" on page 91.

➤ You must have administration privileges for the machine on which you are installing RUM.

➤ If you want to configure specific settings to be used by a silent installation, edit the **RUMInstallationDefaults.properties** file accordingly. Make sure that the file is located in the **%temp%** or **<RUM installation directory>\bin** directory on the machine on which you run the silent installation, and that no other copy of this file exists in either directory. For details on configuring the RUMInstallationDefaults.properties file, see "Configuring the RUMInstallationDefaults.properties File" on page 74.

Silent Installation for Windows

To run a silent installation, use the following procedure:

1 Download and start installing the RUM engine. For details, see "Installing the HP Real User Monitor Engine" on page 50.

2 When the Real User Monitor Configuration wizard opens, click **Cancel** and then quit the RUM installation.

3 Copy the **\HPRUM\bin\RUMInstallationDefaults.properties** file to the location of your choice.

4 Uninstall RUM. For details, see "Uninstalling HP Real User Monitor" on page 91.

5 Configure the saved **RUMInstallationDefaults.properties** file with the values you want the silent installation to use, and copy the file to the machine's **%temp%** directory.

6 Run the setup program (downloaded in step 1) using the following command:

HPRum_<version number>_setup.exe -i silent

The silent installation begins.

Caution: If the same version of RUM as the one you are installing already exists on the machine, the silent installation automatically runs in **uninstall** mode and removes the existing installation.

Configuring the RUMInstallationDefaults.properties File

The **RUMInstallationDefaults.properties** file is used by a silent installation to obtain the parameter values required by the Real User Monitor Configuration wizard during the installation of a specific RUM machine. For details on how the silent installation assigns values, see "How a Silent Installation Assigns Values" on page 73.

The following table describes the RUMInstallationDefaults.properties file and the values that can be set:

Parameter	Description	Default Value
doImport	Import user data settings from a previous RUM installation.	false
importSourceDirectory	The path from which to import user data settings from a previous RUM installation.	
dbPath	The path in which the MySQL database is installed.	c:\\
dbUserName	The user name for accessing the MySQL database.	rum_user
dbPassword	The password for accessing the MySQL database.	
doConnectToDB	Connect the RUM engine to a MySQL database.	true
dbConnectionHostName	The host name of the machine where the MySQL database resides.	
dbConnectionPort	The port number for accessing the host machine.	
dbConnectionUserName	The configured user name for connecting to the MySQL database. This must match the user name that you configured for the **dbUserName** parameter.	
dbConnectionPassword	The configured password for connecting to the MySQL database. This must match the user name that you configured for the **dbPassword** parameter.	

Parameter	Description	Default Value
dbConnectionSchema	The name for the existing MySQL database schema to which you want the RUM engine to connect, or the name of the new schema you want it to create.	
connectToExistingSchema	Connect to an existing schema.	false
webConsoleUserName	The user name you use for accessing the RUM Web console.	admin
webConsolePassword	The password for the RUM Web console user.	admin
jmxPassword	The password for the JMX and Gateway user. **Note:** The JMX and Gateway password must match the password configured for the connection settings of the RUM engine in End User Management Administration. If they do not match, BSM is unable to communicate with the RUM engine to obtain data for End User Management reports. For details on configuring RUM engine connection settings in End User Management Administration, see "Edit Real User Monitor Engine Properties Dialog Box" in *Using End User Management*.	admin
doExport	Export user data settings for use by a future RUM installation. **Note:** This parameter is used when running a silent uninstall.	true
exportDestDirectory	The path to which to export RUM user data settings. **Note:** This parameter is used when running a silent uninstall.	

4

Installing the HP Real User Monitor Probe

After installing the HP Real User Monitor engine, you must install at least one HP Real User Monitor probe. You must then set up the probe to collect real-user data and report this data to the engine.

Note:

➤ Before beginning the installation, review the information in the RUM Readme file for any last minute notes and limitations, as well as for upgrade and service pack install instructions.

➤ For details on installing and working with a probe on a VMware platform, see "Duplicating Traffic for HP Real User Monitor with VMware" on page 105.

This chapter includes:

Physically Connecting the Probe

This section describes how to physically connect the HP Real User Monitor probe to the network.

The HP Real User Monitor probe runs on a Linux or Windows machine and uses two network interfaces; one assigned to sniffing and the other assigned to management (which the HP Real User Monitor engine uses to connect to the probe machine). The interface used for sniffing should not have an IP address assigned to it. For details on the system requirements for the HP Real User Monitor probe, see "HP Real User Monitor Probe Requirements" on page 41.

Using taps or port spanning, the sniffer interface listens to the traffic on the servers you are monitoring.
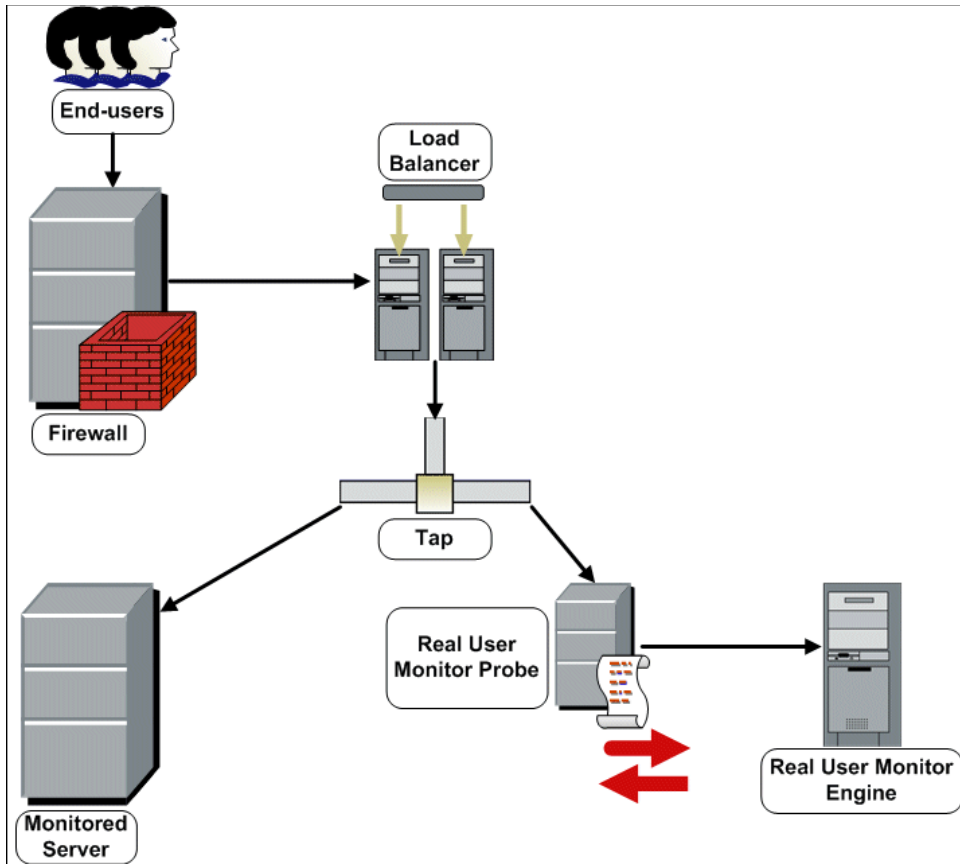
Note:

➤ If you are using a load balancer, it is recommended to place the network tap behind the load balancer.

➤ Load balancers should be configured to use the **x-forward-for** header to preserve end-user IP addresses for use by HP Real User Monitor.

➤ For small installations with a low amount of network traffic, instead of using a network tap, an Ethernet port of the HP Real User Monitor probe can be connected to a switch that is configured for port mirroring for the monitored server.

Installing the Probe

This section describes how to install the probe.

The HP Real User Monitor probe is installed on a machine running either the Linux or Windows operating system. For details on the system requirements for the HP Real User Monitor probe, see "HP Real User Monitor Probe Requirements" on page 41.

Tip: For better performance, it is recommended to install the HP Real User Monitor engine and the HP Real User Monitor probe on the same local area network (LAN).

This section includes the following topics:

➤ "Installing the Real User Monitor Probe on a Linux System" on page 81

➤ "Installing the Real User Monitor Probe on a Windows System" on page 82

Installing the Real User Monitor Probe on a Linux System

Download the HP Real User Monitor probe installation file for Linux from the **Downloads** page, which you access from **Admin** > **Platform** > **Setup and Maintenance**.

Note: The HP Real User Monitor probe installation must be carried out as the root user.

To install the HP Real User Monitor probe:

1 Click **HP Real User Monitor probe** on the Downloads page to download the **HPRUMProbeSetup_linux.bin** file to the **/var/tmp** directory on the machine on which you want to install the probe. Note that if you cannot download this file directly to the Linux machine on which you are installing the probe, make sure that you download the file to a machine from which you can later FTP (in binary mode) the file to the Linux machine.

Note: For the HP Real User Monitor probe setup file to be available on the Downloads page, it must first be installed to HP Business Service Management. For details on installing HP Business Service Management components setup files, see "Installing Component Setup Files" in the *HP Business Service Management Deployment Guide* PDF.

If you prefer, you can copy the HP Real User Monitor probe setup program directly from the Data Collectors and Components directory on the HP Business Service Management DVD, for versions delivered on DVD.

---

2 Run the installation script with the following commands:

➤ **cd /var/tmp**

➤ **chmod 777 HPRUMProbeSetup_linux.bin**

➤ **HPRUMProbeSetup_linux.bin**

Note: You can install the probe to a non default path using the following command:

HPRUMProbeSetup_linux.bin –prefix=/<full path name>/

---

3 Start the HP Real User Monitor probe with the command

/etc/init.d/rum_probe-capture start.

4 Verify that the HP Real User Monitor probe has successfully started with the command **/etc/init.d/rum_probe-capture status**. The following is displayed:

/etc/init.d/rum_probe-capture status

HPRUMProbe is responding properly.

Installing the Real User Monitor Probe on a Windows System

Note: The HP Real User Monitor probe installation must be carried out as an administrator.

To install the HP Real User Monitor probe:

1 Click **HP Real User Monitor probe (Windows)** on the Downloads page to download the **HPRUMProbeSetup_win.msi** file to the machine on which you want to install the probe.

Note: For the HP Real User Monitor probe setup file to be available on the Downloads page, it must first be installed to HP Business Service Management. For details on installing HP Business Service Management components setup files, see "Installing Component Setup Files" in the *HP Business Service Management Deployment Guide* PDF.

If you prefer, you can copy the HP Real User Monitor probe setup program directly from the Data Collectors and Components directory on the HP Business Service Management DVD, for versions delivered on DVD.

 2 Run the **HPRUMProbeSetup_win.msi** setup file that you downloaded by double-clicking it.

 3 When prompted, accept the default installation path (recommended) or select a different path.

 4 When the installation ends, if WinPcap is not already installed on the probe machine, the setup program automatically installs the recommended version of WinPcap.

Note: To avoid version conflicts, it is recommended to remove any prior installation of WinPcap from the probe machine and to let the probe setup program automatically install the recommended version.

5 If you are installing the Real User Monitor Probe on Windows 2008:

    a Open **Windows Services** (In My Computer, right-click Manage and select Configuration > Services)

    b Edit the properties of **HPRUMProbeService**

    c In the **Log on** tab select **This account**

    d Set an administrator user

    e Apply the changes

6 Start the HP Real User Monitor probe.

Stopping and Starting the Probe

The HP Real User Monitor probe is started automatically each time the machine on which it is installed is started. You can also manually start and stop the HP Real User Monitor probe.

To start the HP Real User Monitor probe manually on a Linux machine:

1 Log on to the HP Real User Monitor probe machine as the root user.

2 Start the HP Real User Monitor probe with the command **/etc/init.d/rum_probe-capture start**.

To start the HP Real User Monitor probe manually on a Windows machine:

Select **Start** > **Programs** > **HP Real User Monitor** > **Administration** > **Probe** > **Start RUMProbe**.

To stop the HP Real User Monitor probe manually on a Linux machine:

1 Log on to the HP Real User Monitor probe machine as the root user.

2 Stop the HP Real User Monitor probe with the command **/etc/init.d/rum_probe-capture stop**.

To stop the HP Real User Monitor probe manually on a Windows machine:

Select **Start** > **Programs** > **HP Real User Monitor** > **Administration** > **Probe** > **Stop RUMProbe**.

Connecting the Probe to the Real User Monitor Engine

After you have installed and started the Real User Monitor Probe, you must connect it to a Real User Monitor Engine in Probe Management in the Real User Monitor Web Console. For details, see "Probe Management" on page 190.

Installing an nCipher Card on the HP Real User Monitor Probe

Note: This section applies to the HP Real User Monitor Probe only when it is installed on a Linux system.

You can install an nCipher card on the HP Real User Monitor Probe to enable the probe to use high level security when monitoring SSL encrypted traffic. For details on installing and configuring the nCipher card, refer to the nCipher documentation.

This section describes:

➤ "Prerequisites for Installing an nCipher Card" on page 86

➤ "Verifying an nCipher Card with Apache Web Server" on page 87

➤ "Customizing the HP Real User Monitor Probe" on page 87

➤ "Troubleshooting" on page 89

Prerequisites for Installing an nCipher Card

Note the following before installing an nCipher card on the HP Real User Monitor Probe:

➤ nCipher currently supports JRE/JDK version 1.4.x.

➤ To work with nCipher's KeySafe product, Sun Java runtime environment version 1.5, or the equivalent developer kit, must be installed on the HP Real User Monitor Probe machine.

➤ It is recommended to install the Sun Java runtime environment on the HP Real User Monitor Probe machine prior to installing the nCipher components.

➤ The Java executable must be included in the environment path of the HP Real User Monitor Probe machine.

Verifying an nCipher Card with Apache Web Server

Once you have installed a nCipher card on the HP Real User Monitor Probe machine, it is recommended that you check that the card works with the Apache Web Server. For details on integrating the nCipher components with the Apache Web Server installation on the HP Real User Monitor Probe, refer to the instructions on the nCipher Web site (http://www.thales-esecurity.com/en/Resources/Integration%20Guides/Apache%202-2-15%20UNIX.aspx).

Customizing the HP Real User Monitor Probe

To customize HP Real User Monitor to work with the nCipher card, you must configure the HP Real User Monitor Engine and Probe machines and send the updated HP Real User Monitor Engine configuration to the HP Real User Monitor Probe.

To configure the HP Real User Monitor Engine machine:

Edit the **<HP Real User Monitor root directory>\conf\ configurationmanager\Beatbox_Default_Const_Configuration.xml** file and make the following additions:

➤ Under the **global** heading in the **static_global_params** section, add the line **ssl_hardware chil**. For example:

```
<static_global_params>
<![CDATA[
[global]
max_field_length 2048
collect_server_stats false
collect_website_stats false
ssl_hardware chil
]]>
</static_global_params>
```

➤ Under the **collector** heading in the **collector** section, add the path and name of the **PEM** file created by nCipher. This file contains the name of a key that is protected by the nCipher security world. For example:

```
<collector>
<![CDATA[
[collector]
device          all
servers         0.0.0.0/0.0.0.0   80
ssl_servers 192.168.81.96 444 /root/nCipherpem_file.pem
]]>
</collector>
```

To configure the HP Real User Monitor Probe machine:

1 Add the environment variable definition for **LD_LIBRARY_PATH** to the file /etc/bashrc:

LD_LIBRARY_PATH=/opt/nfast/toolkits/hwcrhk;export LD_LIBRARY_PATH

2 Restart the probe with the following command:

/etc/init.d/rum_probe-capture restart

To send the updated HP Real User Monitor Engine configuration to the HP Real User Monitor Probe:

Force an update of the HP Real User Monitor Probe configuration by accessing the HP Real User Monitor Web console and selecting **Tools > Monitoring Configuration Information > Sync All Configuration**. For details on working with the HP Real User Monitor Web console, see "Using the HP Real User Monitor Web Console" on page 137.

Troubleshooting

If the Apache Web Server is configured for SSL, but is unable to access pages after the nCipher card is installed, change the **LD_ASSUME_KERNEL** parameter to use Linux Kernel version 2.4.1. To change the LD_ASSUME_KERNEL parameter, use the following commands from the command line prompt on the HP Real User Monitor Probe machine's console:

```
$ echo LD_ASSUME_KERNEL=2.4.1 >> /etc/nfast.conf
$ echo export LD_ASSUME_KERNEL >> /etc/nfast.conf
```

Restart the nCipher hardserver for the new setting to take effect.

5

Uninstalling HP Real User Monitor

If you no longer want to use HP Real User Monitor, you can uninstall the engine and probe.

This chapter includes:

➤ Uninstalling the HP Real User Monitor Engine on a Windows Platform on page 91

➤ Uninstalling the HP Real User Monitor Probe on page 98

Uninstalling the HP Real User Monitor Engine on a Windows Platform

You can uninstall the Real User Monitor (RUM) engine using the Windows Control Panel, or by running a silent installation.

This section includes the following topics:

➤ "Uninstalling the RUM Engine Using the Windows Control Panel" on page 91

➤ "Real User Monitor Configuration Wizard" on page 93

➤ "Running a Silent Uninstall" on page 98

Uninstalling the RUM Engine Using the Windows Control Panel

To uninstall the RUM engine:

1 On the machine from which you are uninstalling the RUM engine:

   a Select **Start** > **Settings** > **Control Panel**

    b Select **Add/Remove Programs**

    c Select **HP Real User Monitor**

    d Click **Change/Remove**

2 When prompted, select the installation language (default English) and click **OK**. The HP Real User Monitor Engine Setup wizard begins.

3 When the Application Maintenance page is displayed, select **Uninstall** and click **Next**.

4 The pre-uninstall summary information displays the RUM components that will be removed. Click **Uninstall**.

The HP Real User Monitor Configuration wizard is automatically started. For details on the user interface, see "Real User Monitor Configuration Wizard" on page 93.

Note: When uninstalling a MySQL database only, the HP Real User Monitor Configuration wizard is not accessed and the uninstall procedure continues directly with step 5.

---

5 When the Real User Monitor Configuration wizard has finished, the uninstall process begins and its progress is displayed. You can choose whether to view summary or detailed progress data by clicking the appropriate tab.

6 Once the RUM engine has been uninstalled, you can view the uninstall log file by clicking the **View log file** link.

7 Click **Done** to exit the uninstall process.

Note: If you uninstall the MySQL database only, the RUM engine does not work without the MySQL database.

Real User Monitor Configuration Wizard

Description	Enables you to export user configuration data for use in a future RUM installation. **To access:** The Real User Monitor Configuration wizard is automatically launched as part of the RUM uninstall procedure.
Important information	➤ If your are uninstalling RUM as part of an upgrade, you must export the user data settings so that you can import them when installing the new version of Real User Monitor. ➤ You can only export user data settings for installations that include a RUM engine. When uninstalling a MySQL database only, you are not prompted to export data.
Wizard Map	The Real User Monitor Configuration wizard contains: Export User Configuration Data Page > Export Target Directory Page > Finish Page
Useful Links	➤ "Uninstalling the RUM Engine Using the Windows Control Panel" on page 91 ➤ "Installing the HP Real User Monitor Engine" on page 50

Export User Configuration Data Page

The following is an example of the Export User Configuration Data page.
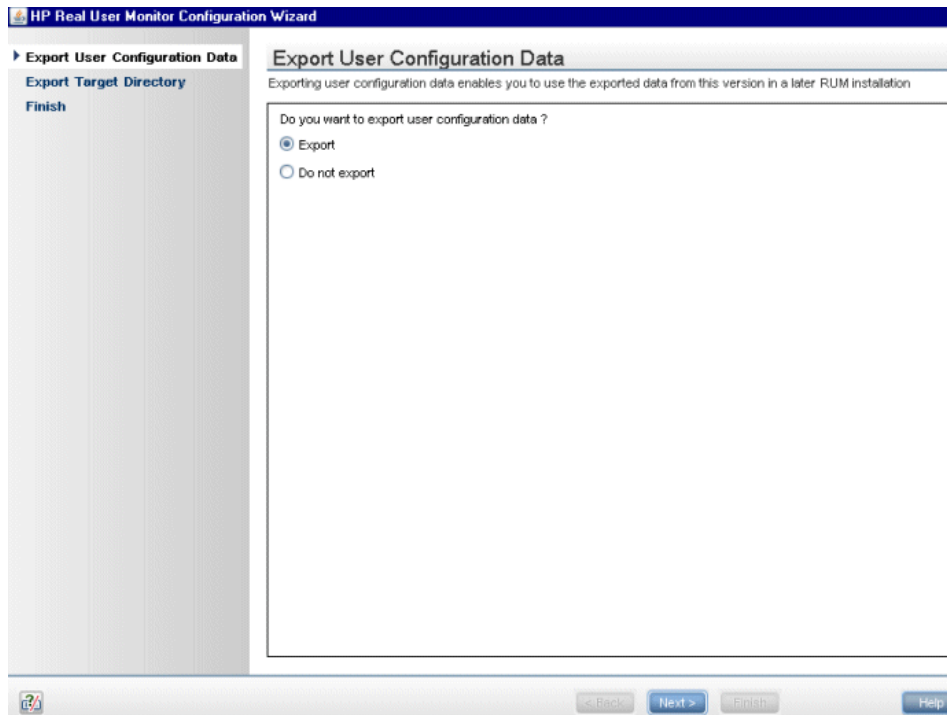
Description	Enables you to select whether you want to export user data settings for use by a future RUM installation.
Important Information	General information about the wizard is available in "Real User Monitor Configuration Wizard" on page 93.
Wizard Map	The Real User Monitor Configuration Wizard contains: **Export User Configuration Data Page** > Export Target Directory Page > Finish Page

The following elements are included:

UI Element	Description
Export	Select this radio button if you want to export user data settings for use when installing a later version of RUM. **Note:** If you are uninstalling RUM as part of an upgrade, you must export the user data settings for importing when you install a later version of RUM.
Do not export	Select this radio button if you do not want to export configuration settings from a previous version of RUM. **Note:** If you select this option, the wizard continues with the "Finish Page" on page 97.

Export Target Directory Page

The following is an example of the Export Target Directory page.

Description	Enables you to select the path to which to export RUM user data settings.
Important Information	General information about the wizard is available in "Real User Monitor Configuration Wizard" on page 93.
Wizard Map	The Real User Monitor Configuration Wizard contains: Export User Configuration Data Page > **Export Target Directory Page** > Finish Page

The following elements are included (unlabeled UI elements are shown in angle brackets):

UI Element	Description
<Target directory>	Enter the target directory to which user configuration data will be exported. You can click **Browse** to locate and select a directory.

Finish Page

The following is an example of the Finish page.

Description	Displays a message showing the status of the Configuration wizard. Click **Finish** to exit and return to the HP Real User Monitor Engine Setup wizard.
Important Information	General information about the wizard is available in "Real User Monitor Configuration Wizard" on page 93.
Wizard Map	The Real User Monitor Configuration Wizard contains: Export User Configuration Data Page > Export Target Directory Page > **Finish Page**

Running a Silent Uninstall

You can use a silent procedure to uninstall the RUM engine. You uninstall the RUM engine silently by running a silent installation, which automatically runs in **uninstall** mode when it detects a similar version of RUM already installed on the machine on which it is running. For details of the silent installation, see "Running a Silent Installation" on page 72.

Uninstalling the HP Real User Monitor Probe

The procedure for uninstalling the Real User Monitor (RUM) probe differs according to the operating system on which it is installed.

This section includes the following topics:

➤ "Uninstalling the RUM Probe on a Windows System" on page 98

➤ "Uninstalling the RUM Probe on a Linux system" on page 98

Uninstalling the RUM Probe on a Windows System

To uninstall the RUM probe:

1 On the machine from which you are uninstalling the RUM probe, select **Start** > **Settings** > **Control Panel**.

2 Select **Add/Remove Programs**.

3 Select **HP RUM Probe.**

4 Click **Change/Remove**.

5 Follow any online instructions.

Uninstalling the RUM Probe on a Linux system

To uninstall the RUM probe on a Linux system, log in as a root user and run the following command:

rpm -e rum_probe-capture

6

Administering the HP Real User Monitor Engine

You administer HP Real User Monitor by using the Windows Start menu and a task bar icon, and use the HP Real User Monitor logs for troubleshooting.

This chapter includes:

➤ Administering HP Real User Monitor on page 99

➤ HP Real User Monitor Logs on page 102

Administering HP Real User Monitor

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

This section includes the following topics:

➤ "HP Real User Monitor Windows Start Menu" on page 100

➤ "HP Real User Monitor Windows Task Bar Icon" on page 101

HP Real User Monitor Windows Start Menu

To access the HP Real User Monitor Start menu that is added to the Windows machine on which the HP Real User Monitor engine is installed, select **Start** > **Programs** > **HP Real User Monitor**. The menu includes the following options:

➤ **Administration**

The Administration menu option includes the following options:

Option	Description
RUM Configuration Tool	Runs the HP Real User Monitor Configuration Tool, which enables you to create a MySQL database schema, and to connect HP Real User Monitor to a MySQL database. For details, see "Creating and Connecting to the MySQL Database" on page 300.
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 HP Real User Monitor	Stops HP Real User Monitor on the specific machine, and disables it from being run automatically whenever the machine is started.
Enable HP Real User Monitor	Starts HP Real User Monitor on the specific machine, and sets it to run automatically whenever the machine is started.

➤ **Open HP Real User Monitor Web Console**

Selecting this option opens the HP Real User Monitor Web console used for administering HP Real User Monitor. For details, see "Using the HP Real User Monitor Web Console" on page 137.

HP Real User Monitor Windows Task Bar Icon

The task bar icon installed with HP Real User Monitor provides a menu with options for the HP Real User Monitor Agent service. The HP Real User Monitor Agent service is responsible for launching HP Real User Monitor and managing the processes used by it. The supervisor process manages and monitors the other processes used by HP Real User Monitor.

When HP Real User Monitor is first enabled, the icon appears with two yellow stars only. When the HP Real User Monitor application server has successfully started, the stars change to grey and a green tick appears above them. If there is an error during startup, or an error with the jboss process after startup, the green tick in the above icon changes to a red X until the problem is rectified.

The menu, which you access by right-clicking the icon, includes the following options:

Option	Description
About	Displays informational data about the HP Real User Monitor Agent service.
View Log	Displays the supervisor log, which includes information about the various processes being used by HP Real User Monitor.
Settings	Displays the processes in use by HP Real User Monitor, and their current settings.
Close	Stops HP Real User Monitor and closes the HP Real User Monitor Agent service.

Note:

➤ Changing any of the process settings can cause HP Real User Monitor to malfunction and should not be done without consulting HP Software Support.

➤ Do not use **Close** to stop HP Real User Monitor. Stop HP Real User Monitor by using the **Disable HP Real User Monitor** option from the **Administration** menu in the HP Real User Monitor Start menu only.

HP Real User Monitor Logs

Real User Monitor logs store messages from Real User Monitor 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 contains the following topics:

➤ Engine Logs

➤ Jboss and Tomcat Logs

➤ Core Logs

Engine Logs

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

➤ **Real User Monitor engine log files.** Log files for modules within the Real User Monitor engine.

➤ **Repository log files.** Log files for modules connecting the Real User Monitor engine and its mySQL database.

There is a log for each module and the Real User Monitor 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 Real User Monitor engine is restarted, it creates a new set of logs.

The name of the Real User Monitor 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 the Real User Monitor 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 HP Real User Monitor engine is installed, and its services.

7

Duplicating Traffic for HP Real User Monitor with VMware

There are various considerations and solutions for duplicating traffic for HP Real User Monitor when the Real User Monitor Probe is installed on a VMware platform.

This chapter includes:

➤ VMware Solutions Overview on page 105

➤ Security on page 106

➤ Configuring Packet Duplication on page 107

➤ References on page 110

VMware Solutions Overview

VMware can use two different kinds of switches—a regular switch, and a DV (distributed) switch which is part of VMware's Enterprise Plus solution (for more information, refer to VMware's vSphere Web page (http://www.vmware.com/vmwarestore/vsphere_purchaseoptions.html).

Working with VMware networks involves defining a virtual switch, which is equivalent to a regular switch. On each virtual machine, you can configure one or more virtual ports, which are equivalent to regular network cards. You then connect each such network card to the virtual switch. For more information, refer to the VMware Virtual Networking Concepts guide (http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf).

There are four basic options for configuring port mirroring for a Real User Monitor Probe with VMware ESX. For details, see "Configuring Packet Duplication" on page 107.

Security

When you configure the promiscuous mode for a VMware machine, it enables other machines to listen to the traffic. For better security, it is recommended that you only allow specifically required machines to receive traffic duplication. For more information, refer to the VMware knowledge base (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1000880).

Configuring Packet Duplication

There are four basic options for configuring port mirroring for a Real User Monitor Probe with VMware ESX.

This section includes the following topics:

➤ "The Probe is Installed on a Virtual Machine and Needs to Capture Traffic from Other Virtual Machines on the Same ESX" on page 107

➤ "The Probe is Installed on a Virtual Machine and Needs to Capture Traffic from Other Virtual Machines Running on a Different ESX" on page 108

➤ "The Probe is Installed on a Virtual Machine and Needs to Capture Traffic from External Servers and Switches" on page 109

➤ "The Probe is Installed on a Physical Server and Needs to Capture Traffic from Virtual Machines" on page 110

The Probe is Installed on a Virtual Machine and Needs to Capture Traffic from Other Virtual Machines on the Same ESX

There are two entities in VMware—a virtual switch and portgroups. By default, a guest operating a system's virtual network adapter only receives frames specific for that adapter. Placing the guest adapter in promiscuous mode causes it to detect all frames passed through the virtual switch that are allowed under the VLAN policy for the associated portgroup.

To configure a portgroup or virtual switch for promiscuous mode using the Virtual Infrastructure Client:

1 Select the ESX Server host and click the **Configuration** tab.

2 Click **Properties** next to the virtual switch or portgroup.

3 To allow promiscuous mode on the virtual switch or portgroup, select the name of the virtual switch or portgroup and click **Edit**.

4 Click the **Security** tab.

5 From the **Promiscuous Mode** drop-down menu, select **Accept**.

Since there is an option to configure several virtual adapters for each virtual machine, and since each virtual adapter can be connected to another virtual switch, there is an option to configure the probe to get the traffic from any virtual switch on the ESX. This is illustrated for the virtual machine VM2 in the example below:
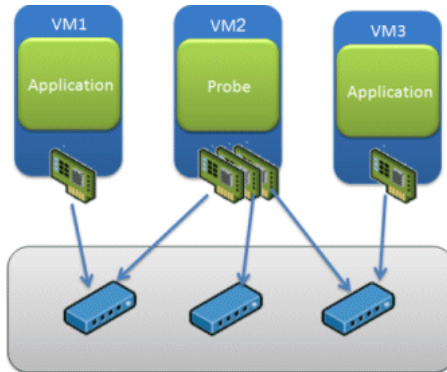
For more information, refer to the VMware knowledge base (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd =displayKC&externalId=1004099).

The Probe is Installed on a Virtual Machine and Needs to Capture Traffic from Other Virtual Machines Running on a Different ESX

You can achieve this option by using the new DV switch. For more information, refer to the relevant VMware white paper (http://www.vmware.com/files/pdf/VMW_09Q1_WP_vSphereNetworking_P8_R1.pdf).

Note: This solution requires a special VMware license.

The Probe is Installed on a Virtual Machine and Needs to Capture Traffic from External Servers and Switches

This option requires the following:

➤ The ESX should have a separate network card (NIC) for the mirrored traffic.

➤ The virtual switch should be configured in promiscuous mode and duplicate the traffic from the NIC to the probe.

➤ There should not be any other virtual machine configured on this virtual switch.

The following example illustrates this option:
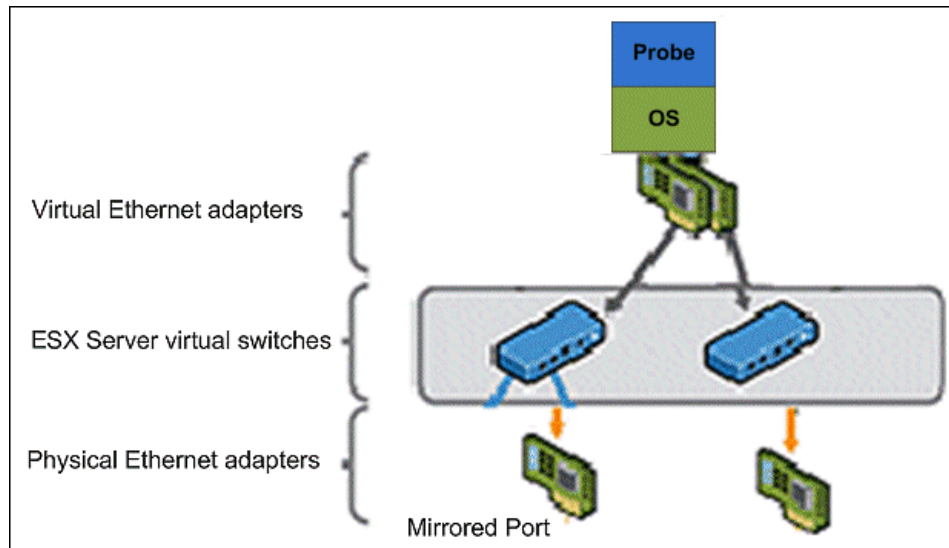
109

The Probe is Installed on a Physical Server and Needs to Capture Traffic from Virtual Machines

You configure this option by integrating Cisco Nexus 1000V Series switches with VMware. This option requires special hardware and is beyond the scope of this document.

References

The following references can provide additional, useful information.

➤ VMware mirroring configuration (http://books.google.co.il/books?id=F_8qs4IPLpwC&pg=PA207&lpg=PA207&dq=vmware+promiscuous+configure&source=bl&ots=GmuIJOwSnv&sig=fle0UCKHHPm4GRmBFj4PsLr4wQY&hl=en&ei=st49TJzMOMe2ngf0s_jdDg&sa=X&oi=book_result&ct=result&resnum=7&ved=0CDEQ6AEwBg#v=onepage&q&f=true)

➤ Defining promiscuous mode in VMware (http://communities.vmware.com/message/371562)

➤ Solution for duplicating traffic from a VMware machine to a non ESX probe (http://www.soleranetworks.com/resources/datasheetV2Ptap_web.pdf)

8

Deploying the RUM SiteMinder Identity Adapter

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:

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.

This section also includes the following topics:

➤ "Prerequisites" on page 112

➤ "System Flow" on page 113

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.
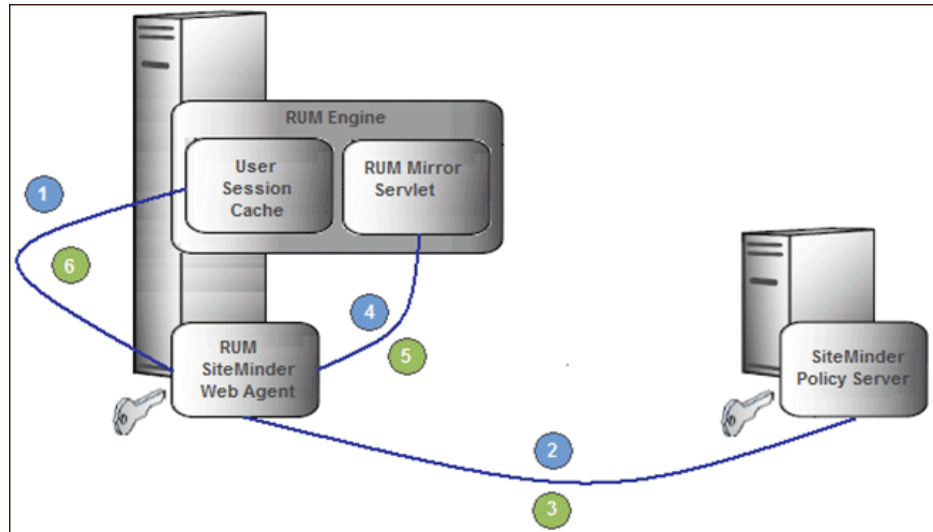
Processing Steps:

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.

113

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" on page 114

➤ "Create the Agent Conf Object" on page 115

➤ "Create the Authentication Scheme" on page 115

➤ "Configure the Domain" on page 116

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 130.

---

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 **AgentContObjects**.

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 Paramater 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" on page 116

➤ "Create the Response" on page 117

➤ "Create the Rules" on page 118

➤ "Configure the Policy" on page 118

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 Adminstration 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 Authetication Schema** created previously.

9 For the Default Resource Portection, 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 Adminstration 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 Adminstration 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 Adminstration 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 Adminstration 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 R**UM 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 insall and configure the SiteMinder Web Agent
and includes the following topics:

➤ "Prerequisites" on page 120

➤ "Installing the SiteMinder Web Agent" on page 120

➤ "Configuring the SiteMinder Web Agent" on page 121

Prerequisites

Ensure the following prequisites 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 in "Configuring the SiteMinder Policy Server" on page 114.)

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" on page 122

➤ "Configuring IIS to Work with the SiteMinder Web Agent" on page 127

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-1.2.32-windows-i386-iis.zip

➤ Win64 x86

http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/windows/tomcat-connectors-1.2.32-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\johndoe\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 130.

---

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:

➤ Select **All Unknown CGI Extensions**.

➤ Click **Allow**.

➤ Select **All Unknown ISAPI Extension**s.

➤ 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 114.

  ➤ 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 115.

➤ **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 122.

➤ **RUM Engine:** Change the **http_settings > por**t 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

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**.

        ➤ Make sure you use an **isapi_redirect.dll** that is compatible with for the host's operating system.

        ➤ 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	➤ Make sure the virtual directory created is called **jakarta**. ➤ Make sure that the **extension_uri** setting is correct. ➤ 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 117.

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 131.

3 Test and troubleshooting the SiteMinder Web Agent. For details, see "SiteMinder Web Agent" on page 132.

Part III

Configuring and Administering HP Real User Monitor

9

Using the HP Real User Monitor Web Console

Once the HP Real User Monitor engine has been installed and started, you can use the HP Real User Monitor Engine Web console to view and configure the connection between HP Real User Monitor and HP Business Service Management, view other HP Real User Monitor engine settings, monitor the health of HP Real User Monitor components, and use HP Real User Monitor diagnostic tools.

This chapter includes:

➤ Accessing the HP Real User Monitor Engine Web Console on page 138

➤ Monitoring the Health of HP Real User Monitor Components on page 143

➤ HP Real User Monitor Configuration and Settings on page 185

➤ BSM Connection Settings on page 185

➤ Probe Management on page 190

➤ TransactionVision Connection Settings on page 219

➤ Advanced Settings on page 221

➤ System Info on page 222

➤ HP Real User Monitor Diagnostic Tools on page 223

Accessing the HP Real User Monitor Engine Web Console

Use the HP Real User Monitor Engine Web console to monitor the health of HP Real User Monitor components. You can also use a number of configuration tools to configure the HP Real User Monitor engine, as well as view and configure the connection parameters between HP Real User Monitor and HP Business Service Management. In addition, the HP Real User Monitor Web console includes diagnostic tools that you can use in resolving HP Real User Monitor problems.

When you start the HP Real User Monitor engine after installation, you can access the HP Real User Monitor Engine Web console by launching a Web browser and entering the following URL:

http://<HP Real User Monitor 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 HP Real User Monitor engine is installed, you can also access the HP Real User Monitor 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" on page 138
➤ "Logging Out" on page 139
➤ "Changing Login Parameters" on page 140
➤ "Changing the Language of the Real User Monitor Web Console User Interface" on page 141

Logging In

When you access the HP Real User Monitor Engine Web console, the login page opens.

Enter the login parameters (login name and password) of a user defined in HP Real User Monitor, 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**. It is recommended that the system superuser change this password immediately to prevent unauthorized entry. For details on changing the password, see "Changing Login Parameters" on page 140.

The HP Real User Monitor 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 <**HP Real User Monitor root directory>\conf\rumwebconsole\rumwebconsole.xml** file. We recommended that you limit access to this file.

Logging Out

When you complete your session, it is recommended 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 HP Real User Monitor Web console after twenty minutes of inactivity.

Changing Login Parameters

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

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

Note: It is recommended that the system superuser limit access to the
<HP Real User Monitor root directory>\conf\rumwebconsole\users.xml
file.

To add an HP Real User Monitor user:

1 Open the **<HP Real User Monitor 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 **encryptedPassword**
parameter is blank.

4 Save the file.

To change an HP Real User Monitor user:

1 Open the **<HP Real User Monitor 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 **encryptedPassword** parameter is blank.

4 Save the file.

To delete an HP Real User Monitor user:

1 Open the **HPRUM\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 HP Real User Monitor Web console.

➤ Changes to the **HPRUM\conf\rumwebconsole\users.xml** file only take effect when the HP Real User Monitor engine is restarted. When the HP Real User Monitor engine is started, user passwords in the **password** parameter are encrypted and removed, and the encrypted passwords are stored in the **encryptedPassword** parameter.

Changing the Language of the Real User Monitor Web Console User Interface

In Real User Monitor 8.00 and later, the Real User Monitor 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]
Japanese	Japanese [ja]
Korean	Korean [ko]

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

To view the Real User Monitor 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 Real User Monitor Web console.

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**.

3 Click **Move Up** to move the selected language to the first row.

4 Click **OK** to save the settings.

5 Refresh the page: the Real User Monitor Web console user interface is displayed in the selected language.

Note:

➤ Starting from Real User Monitor version 7.0, there is no language pack installation. All translated languages are integrated into the Real User Monitor Multilingual User Interface.

➤ Data stays in the language it was entered in, 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 Real User Monitor definitions and configurations.

➤ If a user selects a language not supported by the Real User Monitor Multilingual User Interface, the Real User Monitor Web console user interface appears in English.

Monitoring the Health of HP Real User Monitor Components

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

This section includes the following topics:

➤ "System Status" on page 143

➤ "Capture Log Files" on page 184

System Status

You use the **System Status** menu option to display the status of the main HP Real User Monitor components. When you select this option, the System Health page opens. You can refresh the data displayed on the System Health page by clicking the **Refresh** button at the top, right hand side of the page.

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 HP Real User Monitor 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 handled), 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 might be displayed in brackets, which is the accumulated value of the entity since the HP Real User Monitor engine was last started.

Note: Entities using ratios have no status until the System Health page has been automatically updated twice by the HP Real User Monitor 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 Business Service Management Server" on page 145

➤ "Database" on page 146

Configuration Retrieval From Business Service Management Server

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Connection to Business Service Management 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
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 data type <type name> from BSM server

Database

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
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.
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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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

Real User Monitor Probe

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
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)
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
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)
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
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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
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
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
Lost SSL Requests	The percentage of SSL requests for which the decryption failed.	N/A	N/A	N/A
Missing Mirrored Data	Click **Missing Mirrored Data** to see the entities that comprise the Missing Mirrored Data component.			

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Network Captures Retriever Queue Size	The queue size of the probe's network capture files.	N/A	N/A	N/A
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
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
Packets Lost	The total number of packets that the RUM probe has recognized as missing	The network is stable and packets are being processed normally	Possible network problems which could lead to data loss	The network is bad and the RUM probe might loose some data

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Packets with bad checksum	The percentage of packets with bad checksums	N/A	N/A	N/A
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
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
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
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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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 synchronizati on 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 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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
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)
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
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
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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
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
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)
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
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
Probe Connections Published	The number of connections recorded by the RUM probe	N/A	N/A	N/A
Probe Connections Processed by Engine	The number of connections that the RUM engine has started to process	N/A	N/A	N/A

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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 of probe utilization of the probe process	Probe utilization is normal	Probe utilization is nearing the limit for a single RUM probe	N/A
Probe Process Memory	The total amount of non-swapped, physical memory used by the RUM probe, in kilobytes	Always	N/A	N/A

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
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
Probe Storage ccomps Status	The current status of the database for components	Database status is normal	N/A	Database status is bad

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
Probe Storage pcapnetwork Number of Total Records	The total number of records for network captures in the database	N/A	N/A	N/A

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
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
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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
SSL Transactions Dropped	The percentage of SSL transactions that could be decrypted	N/A	N/A	N/A
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 Engine

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Aggregation Manager	Click **Aggregation Manager** to see the entities that comprise the Aggregation Manager component.			
Application Session Count	The total number of open application sessions	Always	N/A	N/A
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.			
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)
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 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
BBRetriever Thrown Objects	The total number of objects thrown by the BBRetriever	N/A	N/A	N/A
BBRetriever Total Actions Handled	The number of actions being handled by the BBRetriever in the RUM engine	The number of actions being handled is normal	The number of actions being handled is above average	The number of actions being handled is high

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
BBRetriever Total Connections Handled	The number of connections being handled by the BBRetriever in the RUM engine	The number of connections being handled is normal	The number of connections being handled is above average	The number of connections being handled is high
BBRetriever Total Pages Handled	The number of pages being handled by the BBRetriever in the RUM engine	The number of pages being handled is normal	The number of pages being handled is above average	The number of pages being handled is high
BBRetriever Total Poor Requests Handled	The number of Poor requests handled by the BBRetriever in the RUM engine	N/A	N/A	N/A
Classification	Click **Classification** to see the entities that comprise the Classification component.			
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)
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
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
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				
JMS Topology Topic size				

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
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>
Publisher Chunks in Memory	The number of sample chunks (not yet sent to BSM) stored in memory	N/A	N/A	N/A
Poor Request Network Captures Retrieved	The number of Poor request capture files retrieved by the RUM engine	N/A	N/A	N/A

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Poor Request Network Captures Thrown	The number of Poor request capture files thrown by the RUM engine	N/A	N/A	N/A
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 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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
Snapshot Jobs Submit Denials	The total number of submit requests for snapshot failures	Always	N/A	N/A
Snapshot Relevant Events	The total number of events that should trigger snapshot creation	Always	N/A	N/A
Snapshot 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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
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.			

Samples to Business Service Management Server

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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 HP Business Service Management	N/A	RUM has failed in sending data to HP Business Service Management
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 HP Business Service Management. No samples are delayed	N/A	RUM is delaying samples so as not to overload HP Business Service Management
Publisher Samples Created for <entity>	The number of <entity> samples created since the last RUM engine restart	N/A	N/A	N/A
Publisher Samples Thrown	The total number of samples thrown	Always	N/A	N/A

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Publisher Total Samples Created	The total number of samples created (for all <entities>) since the last RUM engine restart	N/A	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	N/A	N/A	N/A

Aggregation Manager

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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
AverageDuration for aggregation	The average execution time for each task	N/A	N/A	N/A
AvgAffectedRows for aggregation	The average number of affected rows for aggregations done since the last RUM engine restart	N/A	N/A	N/A
LastDuration for aggregation	The last execution time for each task	N/A	N/A	N/A
MaxAffectedRows for aggregation	The maximum number of affected rows for aggregations done since the last RUM engine restart	N/A	N/A	N/A
MaxDuration for aggregation	The maximum execution time for each task	N/A	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

Classification

To access, click **Classification** in RUM Engine monitors.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Classification Size Limit Exceeds	The size of all the classifications exceeds an internal, default limit	OK (does not exceed)	N/A	Exceeds
Classification Total Classification Ids Number	The total number of classification IDs	N/A	N/A	N/A
Classification Total Clusters Number	The total number of classification clusters	N/A	N/A	N/A
Classification Total Nodes Number	The total number of classification nodes	N/A	N/A	N/A
Classification Total Stable Clusters	The total number of stable classification clusters	N/A	N/A	N/A
Is Classification Module Stable	The status of the classification module	Stable	N/A	Unstable

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/AS	The Data Access Layer is not active

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
Number of <entity> objects sent	The number of <entity> objects sent to the database since startup	N/A	N/A	N/A

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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\> lookup table in the memory cache	N/A	N/A	N/A

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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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	Partition Manager task performance is normal	Partition Manager task performance has exceeded the warning threshold	Partition Manager task performance has exceeded the error threshold and might cause locks in the database during execution

Topology Engine

To access, click **Topology Engine** in RUM Engine monitors.

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Auto discovered pages accumulator size	The number of pages created by RUM, waiting to be sent to BSM	<= 500	N/A	> 500
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)
Connection status to CMDB	Status of the connection to the Run-time Service Model (RTSM)	Connection OK	N/A	No connection
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
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
Number of accumulated IP ranges	The accumulated data structure size of discovered IP ranges	N/A	N/A	N/A

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
Reporters connection to BSM status	The status of the connection to BSM	Connection OK	N/A	No connection
Resolved Hosts cache size	The number of hosts to be reported to BSM for CI creation	<= 10,000	N/A	> 10,000
Resolved Software Elements - Application links cache size	The number of application and software element links reported to BSM	<= 10,000	N/A	> 10,000
Resolved Software Elements cache size	The number of software elements reported to BSM	<= 10,000	N/A	> 10,000

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
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
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
Unresolved Software Elements cache size	The number of software elements 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 the HP Real User Monitor for support purposes.

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

HP Real User Monitor Configuration and Settings

The **Configuration** drop-down menu on the HP Real User Monitor Engine Web console menu bar includes the following options:

➤ **BSM Connection Settings.** Used to view and configure the connection parameters between HP Real User Monitor and HP Business Service Management. For details, see "BSM Connection Settings" on page 185.

➤ **Probe Management.** Used to configure communication settings with the HP Real User Monitor probe. For details, see "Probe Management" on page 190.

➤ **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 "Real User Monitor Transaction Flow Monitoring" on page 249.

➤ **TV Connection Settings.** Used to view and configure the connection parameters between HP Real User Monitor and TransactionVision. For details, see "TransactionVision Connection Settings" on page 219.

➤ **Advanced Settings.** Provides links to specific areas of the HP Real User Monitor JMX console for configuring parameters and settings for individual HP Real User Monitor modules. For details, see "Advanced Settings" on page 221.

➤ **System Info.** Provides general system information about the HP Real User Monitor. For details, see "System Info" on page 222.

BSM Connection Settings

This page displays the current connection settings for the communication channel between HP Real User Monitor and HP Business Service Management, which you can update.

Note: If you change the configuration, click the **Save Configuration** button to save the configuration and update the HP Real User Monitor engine.

➤ "RUM General Settings Pane" on page 186

➤ "Connection to Business Service Management Pane" on page 187

➤ "Authentication Pane" on page 187

➤ "Proxy Pane" on page 188

➤ "SSL Pane" on page 189

RUM General Settings Pane

Field	Description
Real User Monitor engine name	Configure a name for the Real User Monitor engine. This name is registered in Business Service Management and is used to identify the engine in Real User Monitor Administration.
RTSM-RUM integration user password	Set the password for the default RTSM-RUM integration user.
	The Real User Monitor Engine sends created CIs to the Run-time Service Model (RTSM), via the Business Service Management Gateway Server. To enable the connection to the RTSM, a default user name (rum_integration_user) and password is used. If you change the password in the RTSM (for details, refer to your database administrator), you must also change it in the Real User Monitor Engine.
	Note: If the correct password is not configured (that is, the password configured in the Real User Monitor Engine is different to the password configured in the RTSM), RUM related topology is not updated in the RTSM and you will not see all RUM data in End User Management reports.

Connection to Business Service Management Pane

Field	Description
Business Service Management Gateway Server host name	The IP address or host name of the machine on which the Business Service Management Gateway Server is installed.
Port	The port number used to connect to the host machine on which the Business Service Management Gateway Server is installed.
Protocol	The protocol used to connect to the host machine on which the Business Service Management 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 hostname 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 Business Service Management 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 HP Business Service Management, see "Using Basic Authentication in BSM" in the *HP Business Service Management Hardening Guide* PDF.

Proxy Pane

Field	Description
Use proxy	Select the check box if the Real User Monitor engine connects to the Business Service Management Gateway Server machine via a proxy server.
Proxy host	If the Real User Monitor engine connects to the Business Service Management Gateway Server machine via a proxy server, enter the IP address or host name of the proxy server.
Proxy port	If you connect to the Business Service Management 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 HP Business Service Management, see "Using a Reverse Proxy in BSM" in the *HP Business Service Management Hardening Guide* PDF.

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 Business Service Management 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 the HP Real User Monitor and HP Business Service Management to work with SSL, see "Using SSL in BSM" in the *HP Business Service Management Hardening Guide* PDF.

Probe Management

You use the Probe Management configuration option to create and administer the HP Real User Monitor 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 Real User Monitor traffic. **Note:** Not all the configuration options are enabled for disabled probes.
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 page 193
	Edit Probe Configuration. Opens the Edit Probe Configuration dialog box, where you configure an existing probe for the engine.	"Probe Configuration Dialog Box" on page 193
	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 196
	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

Icon	Description	For details, see ...
	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 203
	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 206
	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 208
	SSH Console. Connects to a probe's console using Secure Shell. **Note:** This button is enabled only for Linux installations of the Real User Monitor probe.	"SSH Console" on page 211
	Probe Traffic Capture. Opens the Probe Traffic Capture page where you instruct a Real User Monitor probe to save the traffic it monitors to a file.	"Probe Traffic Capture" on page 212

Icon	Description	For details, see ...
S⊞	**Session ID Detection.** Opens the Session ID Detection page, where you instruct a HP Real User Monitor probe to detect Session IDs in the traffic it monitors.	"Session ID Detection" on page 213
↻	**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 Real User Monitor 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 Real User Monitor traffic.
Name	The probe name. **Note:** This field is mandatory. **Syntax exceptions:** Cannot exceed 255 characters.
Description	A free text description of the probe. **Syntax exceptions:** Cannot exceed 255 characters.

193

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:** ➤ 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 Real User Monitor engine connects to the probe machine via a proxy server.
Proxy host	If the Real User Monitor engine connects to the probe machine via a proxy server, enter the IP address or host name of the proxy server.
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.

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 Probe 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.

Probe Traffic Discovery

You use the Probe Traffic Discovery tool to instruct the HP Real User Monitor 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 "How to Set up Real User Monitors" in *Using End User Management*.

➤ 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: The Probe Traffic Discovery tool can run concurrently with regular probe monitoring.

This section includes the following topics:

Common Elements

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

UI Element	Description
🕘	**Reset Discovery Statistics.** Resets and initializes probe traffic discovery statistics.
	Note: This button is available only when probe traffic discovery is running.
🔄	**Refresh.** Refreshes the data displayed on the Probe Traffic Discovery page with the most up to date statistics.
	Note: This button is available only when probe traffic discovery is running.
Server Type	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.
	Default value: Both

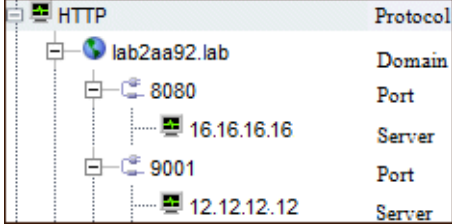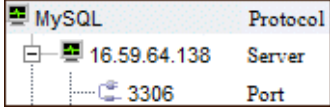| UI Element	Description
<General statistics>	**Discovery start time.** The start time of a currently running traffic discovery.
	Sample period. The date and time that the displayed statistics were retrieved are displayed. For statistics loaded from a saved file, **Saved Results** is displayed next to the date and time.
	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.
	Peak pages/sec. The peak number of pages per second for all the domains or servers included in the page, for the http protocol.
Start Discovery	Click the **Start Discovery** button to start probe traffic discovery for the probe. Starting discovery automatically deletes any previously saved data.
	Note: The **Start Discovery** and **Stop Discovery** buttons are not enabled simultaneously. When one is enabled, the other is disabled.
Stop Discovery	Click the **Stop Discovery** button to stop probe traffic discovery for the probe and save the current data.
	Note:
	➤ 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
Search	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.
	Note:
	➤ When using the search feature in the **Domain View** tab, you can enter alpha-numeric 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 only enter valid IP addresses in the search field. The search filters server IP addresses that exactly match the search string.

UI Element	Description
<Domain View protocol tree>	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: **Note:** This is the default view when you drill down from the Summary View pie chart for the http protocol.
<Server View protocol tree>	For each discovered protocol, the statistics are grouped by server IP addresses and for each server, by port. For example: **Note:** This is the default view when you drill down from the Summary View pie chart for protocols other than http.
% 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.

UI Element	Description
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 HP Real User Monitor 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 Real User Monitor 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 Real User Monitor probe cannot decrypt traffic that uses Diffe 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 205) it is recommended that you configure the Web server of the monitored server not to support the Diffe Helman protocol.

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.
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.

Note: 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 Real User Monitor 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 Real User Monitor 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 Real User Monitor 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. 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.

UI Element	Description
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 Real User Monitor 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 HP Real User Monitor probe to listen to all available devices automatically.

Note: This differs from selecting all the devices manually, as the HP Real User Monitor 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 HP Real User Monitor 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 HP Real User Monitor 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 analyze.

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

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

The HP Real User Monitor 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 HP Real User Monitor 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: ➤ **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: ➤ **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 "Add a new filter" on page 210 for an explanation of the filter's fields.

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

SSH Console

Note: This section applies to Linux installations of the Real User Monitor probe only.

You use SSH Console to connect to the HP Real User Monitor probe's console using Secure Shell, which provides strong authentication and secure communications over insecure channels. To access SSH Console, click the **SSH Console** button on the Probe Management page.

The first time you access SSH Console, a wizard installs some required files on your machine. Accept the default settings, or change them as required. Each time you access SSH Console, accept the certificate displayed, and in the console window, enter the user and password you configured for the HP Real User Monitor probe. You are now connected to the HP Real User Monitor probe's console. (For information on configuring the probe, see "Probe Configuration Dialog Box" on page 193.)

In the HP Real User Monitor probe console, you use regular Linux commands on the command line. There is also a menu providing assorted utilities for working in SSH Console. To access the menu, right-click the mouse while holding down the CTRL key. One of the utilities is a convenient graphical user interface for SFTP, which you use to transfer files to and from the HP Real User Monitor probe machine via secured FTP. To access the SFTP tool from the menu, select **Plugins** > **SFTP File Transfer**.

Probe Traffic Capture

You use the Probe Traffic Capture feature to instruct a Real User Monitor 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)	Enter the maximum capture file size in megabytes. You can configure a file size of up to 100 MB. **Note:** Capturing is automatically stopped when either the configured file size or the configured time is reached.
Capture duration (seconds)	Enter the maximum time (in seconds) for capturing to run. You can configure a time of up to 3600 seconds. **Note:** Capturing is automatically stopped when either the configured file size or the configured time is reached.
Use client IP filter	Select this check box if you want to capture traffic for a specific range of clients.

Element	Description
Client IP filter from...to	If you select the **Use client IP filter** check box, enter the IP range for the clients whose traffic you want to capture.
Start Capture	Click the **Start Capture** button to start the probe traffic capture. The following elements are displayed: ➤ **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. **Note:** The **Time left** and **Current file size** data is refreshed automatically every ten seconds when capturing is running.

Session ID Detection

Use session ID detection to instruct the HP Real User Monitor 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 *Using End User Management*.

This section includes the following topics:

➤ "Configuring Applications in End User Management Administration Using Traffic Discovery and Session ID Detection" on page 214

➤ "Session ID Detection Page" on page 214

➤ "Session ID Detection Report" on page 215

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	Select this check box to instruct Real User Monitor to detect session IDs for a single IP address that it monitors, and enter the IP address in the adjacent field.
Last successful detection time	Shows the last date and time that the Session ID Detection tool was successfully run.
Status	The status of the session ID detection. Valid statuses are: ➤ **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.

UI Element	Description
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" on page 215. **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 "Real User Monitor Application Configuration Wizard" in *Using End User Management*.
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.

UI Element	Description
Application Connections	The total number of connections to the application.
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 "Real User Monitor Application Configuration Wizard" in *Using End User Management*.
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 HP Real User Monitor 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 HP Real User Monitor 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.

UI Element	Description
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 HP Real User Monitor 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 HP Real User Monitor and TransactionVision, which you can update. For details on viewing TransactionVision data from Real User Monitor reports, see "Viewing TransactionVision Data From End User Management Reports" in *Using End User Management*.

The TransactionVision Connection Settings page contains the following panes:

➤ "Events to TransactionVision Analyzer" on page 219

➤ "Connection to TransactionVision Analyzer" on page 219

➤ "Authentication Pane" on page 220

➤ "SSL Pane" on page 220

Events to TransactionVision Analyzer

Select the check box in this pane to configure Real User Monitor to send Real User Monitor 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.

Field	Description
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 HP Real User Monitor modules and provides direct links to specific pages in the HP Real User Monitor 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 HP Real User Monitor module retrieved from HP Business Service Management.

> ➤ **Settings Page.** Links to settings for the configuration of the HP Real User Monitor module in the HP Real User Monitor engine.

For details on working with the JMX console, see "Using the JMX Console to Configure the HP Real User Monitor Engine" on page 235.

System Info

This option shows general system information about the HP Real User Monitor, which is displayed in the following panes:

> ➤ **Real User Monitor Server - General.** Includes the host name, host IP address, total memory, and the number of available processors for the HP Real User Monitor server.

> ➤ **Real User Monitor Server - OS.** Includes the name and version of the operating system of the HP Real User Monitor server.

> ➤ **Real User Monitor Database - General.** Includes the host name and port number of the HP Real User Monitor database, as well as the name of the database schema.

HP Real User Monitor Diagnostic Tools

The **Tools** drop-down menu on the HP Real User Monitor 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 HP Real User Monitor in End User Management Administration. For details, see "Monitoring Configuration Information" on page 223.

➤ **JMX Console.** Provides a link to the HP Real User Monitor JMX console for configuring HP Real User Monitor parameters, such as URL correlation parameters. For details, see "JMX Console" on page 232. (For details on URL correlation, see "Correlating Collected Data with Configured Pages" in *Using End User Management*.)

➤ **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 232.

➤ **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 233.

➤ **Page Name Cache.** Used to manage the Page Name cache of meaningful page names and to delete such names that are no longer relevant. For details, see "Page Name Cache" on page 233.

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 HP Real User Monitor in End User Management Administration.

Click the **Sync All Configuration** button, located at the top of the Engine Configuration page, to force the HP Real User Monitor engine to reload the HP Real User Monitor configuration from HP Business Service Management.

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

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 HP Business Service Management.
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 "Real User Monitor Application Configuration Wizard" in *Using End User Management*.

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 HP Business Service Management.
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 Real User Monitor Configuration Dialog Box" in *Using End User Management*.

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 HP Business Service Management.
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.
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.

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

For information on configuring events for monitoring, see "Real User Monitor Administration User Interface" in *Using End User Management*.

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 HP Business Service Management.
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.
Availability Threshold	The availability threshold, in percent, configured for the page in End User Management Administration.

Column	Description
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 *Using End User Management.*

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 HP Business Service Management.
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 the HP Real User Monitor Probe" on page 77.

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 HP Business Service Management.
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.

Column	Description
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 Real User Monitor Configuration Page" in *Using End User Management*.

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 HP Business Service Management profile ID.

Column	Description
Profile Name	Internal HP Business Service Management profile name.
Engine ID	Internal HP Business Service Management 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 HP Business Service Management 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 HP Business Service Management application ID.
Snapshot mode on	True or False – as configured in End User Management Administration.

JMX Console

This option provides a link to the HP Real User Monitor JMX console, which you use to view and configure HP Real User Monitor parameters, for example, URL correlation parameters. For details on configuring URL correlation parameters, see "Correlating Collected Data with Configured Pages" in *Using End User Management*. For details on working with the JMX console, see "Using the JMX Console to Configure the HP Real User Monitor Engine" on page 235.

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 HP Real User Monitor data samples.

➤ **Unsigned integer.** An internal, unsigned number used in HP Real User Monitor 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 HP Real User Monitor 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 HP Real User Monitor engine.

➤ Time in Greenwich Mean Time.

➤ Time in the time zone set for the HP Real User Monitor 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 meaningful page names that have been created for pages included in the application. You can delete meaningful page names that are no longer relevant (for example, if you have changed the meaningful page name rules for an application so that new and different meaningful page names are created) and thereby reduce the amount of data stored in the Real User Monitor database. For details on configuring meaningful names, see "Configuring Meaningful Page Names" on page 263.

This section includes the following topics:

➤ "Application Selection Page" on page 234

➤ "Application Cached Page Names Page" on page 234

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 HP Real User Monitor engine in End User Management Administration. For information on configuring applications in End User Management Administration, see "Real User Monitor Application Configuration Wizard" in *Using End User Management*.

For each application, you can perform the following actions:

➤ Click the **Delete** button to delete all the meaningful 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" on page 234) on which you can see all the meaningful page names for the application and delete them selectively.

Note: The buttons are disabled for applications that do not have any meaningful 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 meaningful 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.

10

Using the JMX Console to Configure the HP Real User Monitor Engine

You configure HP Real User Monitor 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 HP Real User Monitor Web Console" on page 137.

This chapter includes:

➤ Using the HP Real User Monitor JMX Console on page 235

➤ URL Correlation Parameters on page 242

Using the HP Real User Monitor JMX Console

You use the HP Real User Monitor Engine JMX Console to view and configure HP Real User Monitor settings.

This section includes the following topics:

➤ "Accessing the JMX Console" on page 236

➤ "Setting URL Correlation Parameters" on page 237

➤ "Configuring HP Real User Monitor Aggregation" on page 237

➤ "Configuring HP Real User Monitor Reporting" on page 240

➤ "Configuring the Samples Rate" on page 241

➤ "Configuring the Amount of Unsent Sample Data to Store in Real User Monitor" on page 241

Accessing the JMX Console

Via the JMX console, you can view and configure HP Real User Monitor parameters, view statistics for HP Real User Monitor modules and services, and view and configure jboss components.

Once you start the HP Real User Monitor engine after installation, you can access the HP Real User Monitor Engine JMX Console by launching the HP Real User Monitor Engine Web console and choosing **JMX Console** from the **Configuration** drop-down menu. To access a specific area of the JMX Console for an individual HP Real User Monitor module, select **Advanced Settings** from the **Configuration** drop-down menu in the HP Real User Monitor Engine Web console and then click the links for the module you want to view. For details on the HP Real User Monitor Engine Web console, see "Using the HP Real User Monitor Web Console" on page 137.

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 HP Real User Monitor 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 HP Real User Monitor to malfunction. It is recommended not to change any of these settings.

Setting URL Correlation Parameters

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

Some of the URL correlation parameters are set using the HP Real User Monitor JMX console. For details on changing URL correlation parameters via the HP Real User Monitor JMX console, see "Setting URL Correlation Parameters Via the JMX Console" on page 243.

Configuring HP Real User Monitor Aggregation

HP Real User Monitor pre-aggregates a number of the data samples it sends to HP Business Service Management. For details on HP Business Service Management aggregation, see "Data Aggregation" in *Reports*. For details on HP Real User Monitor pre-aggregation, see "Aggregating Real User Monitor Data" in *Using End User Management*.

You can change the HP Real User Monitor default aggregation periods via the JMX console.

This section includes the following topics:

➤ "Pre-aggregated Data Sample Types" on page 238

➤ "Changing Default Aggregation Periods" on page 239

Pre-aggregated Data Sample Types

The following table shows the data sample types that are pre-aggregated by HP Real User Monitor, 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	StatisticsMgr Conf	Properties	aggregator.actions.interval	300,000
Slow End User			aggregator.domains.interval	300,000
Missing Component			aggregator.Missing Components.interval	300,000
Slow Action			aggregator.SlowActions. interval	300,000
Slow Location			aggregator.slowlocations.int erval	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.actionerror event.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 HP Real User Monitor default aggregation periods via the JMX console:

1 Access the JMX console by choosing **JMX Console** from the Configuration drop-down menu in the HP Real User Monitor 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 HP Real User Monitor to BSM. It is recommended not to change the default aggregation periods.

Configuring HP Real User Monitor Reporting

By default, HP Real User Monitor reports data to HP Business Service Management for all end users, both those configured in end-user groups in End User Management Administration and those who are not configured. (For details on configuring end users in End User Management Administration, see "Add End User Group with Real User Monitor Configuration Dialog Box" in *Using End User Management*.) You can configure HP Real User Monitor to report data only for configured end users.

Note: HP Business Service Management includes a list of predefined end-user names and domains to give meaningful names to end users in HP Real User Monitor reports. If you configure HP Real User Monitor to report data only for configured end users, data for end users in the predefined list are not reported to HP Business Service Management. For details of HP Real User Monitor reports, see "End User Management Reports" in *Using End User Management*.

To configure HP Real User Monitor to report data for configured end users only:

1 Access the JMX console by choosing **JMX Console** from the Configuration drop-down menu in the HP Real User Monitor 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=StatisticsMgrConf**.

3 In the **ShouldReportUndefinedDomains** parameter, change the value to **false**.

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

5 Click the **Invoke** button for the **deployConfiguration** operation to activate the change.

Configuring the Samples Rate

The maximum burst rate controls the number of samples per second that the HP Real User Monitor engine can send to HP Business Service Management. The default setting is 150. You can increase the maximum burst rate to allow more samples to be sent per second, provided that HP Business Service Management is capable of handling the increased number. You can see the state of the flow of samples between HP Real User Monitor and HP Business Service Management by looking at the **Publisher burst state** in Real User Monitor system health. For details on Real User Monitor system health, see "Monitoring the Health of HP Real User Monitor Components" on page 143.

To configure the maximum burst rate:

1 Access the JMX console by choosing **JMX Console** from the Configuration drop-down menu in the HP Real User Monitor 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 Real User Monitor

By default, 1000 chunks of samples data are stored in HP Real User Monitor for sending to HP Business Service Management. You can increase the number of chunks of data stored (providing you have sufficient disk space) to avoid data loss when HP Business Service Management cannot receive data from HP Real User Monitor. For example, you might want to increase the amount of data stored by HP Real User Monitor during a planned

downtime in HP Business Service Management. Bear in mind that when a lot of data has been stored in HP Real User Monitor, it can take a long time for all of it to be sent to HP Business Service Management, 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 HP Business Service Management 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 Configuration drop-down menu in the HP Real User Monitor 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.

URL Correlation Parameters

After the HP Real User Monitor engine has been installed and started, you can configure a number of parameters to determine how the HP Real User Monitor 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 page 243
➤ "Correlating Session ID Parameters" on page 245

Setting URL Correlation Parameters Via the JMX Console

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

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

➤ **adaptIndexurl.** By default, HP Real User Monitor 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 HP Real User Monitor 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 <u>/;/index.html;</u> is configured in the urlIndexStrings parameter then <u>http://www.hp.com/</u> and <u>http://www.hp.com/index.html</u> are considered as being identical, <u>http://www.hp-int.com/</u> and <u>http://www.hp-int.com/</u> <u>index.html</u> are considered as being identical, and so forth.

➤ Changing the **urlIndexStrings** parameter requires the HP Real User Monitor Engine Resolver to be restarted. For details, see "To restart the HP Real User Monitor Engine Resolver:" on page 245.

➤ **adaptCaseSensitive.** By default, HP Real User Monitor URL correlation is case-insensitive, so that a recorded URL such as <u>http://www.hp.com/</u> <u>rumEnginePage.html</u> is correlated with the configured URL <u>http://www.hp.com/rumenginepage.html</u>. To instruct HP Real User Monitor 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, HP Real User Monitor ignores basic authentication when performing URL correlation. For example, the recorded URL <u>http://bob:my_password@www.hp.com</u> is correlated with the configured URL <u>http://www.hp.com</u>. To instruct the HP Real User Monitor 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 Configuration drop-down menu in the HP Real User Monitor 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 HP Real User Monitor Engine Resolver:

1 Access the JMX console by choosing **JMX Console** from the Configuration drop-down menu in the HP Real User Monitor 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 HP Real User Monitor 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 *Using End User Management*. For details on configuring URLs for monitoring, see "Real User Monitor Application Configuration Wizard" in *Using End User Management*.

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

http://www.hp.com/~anand/Ticket_Confirm.jsp?BV_SessionID=@@@@181205 7630.1043567934@@@@&BV_EngineID=cccdadchgidfmlmcefecehidfhfdffk.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 HP Real User Monitor to ignore during correlation. Parameters are entered in the format <parameter>parameter_name, where parameter_name is the name of the parameter. For example, for a parameter called BV_EngineID, the entry is.

  <parameter>BV_EngineID

 4 If you want HP Real User Monitor 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.

11

Real User Monitor Transaction Flow Monitoring

You use Real User Monitor (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:

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 (EUM) 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 Real User Monitor Configuration Page" in *Using End User Management*.

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 page 251. 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 HP Real User Monitor Engine Web Console" on page 138.

The data discovered by RUM transaction flow monitoring is sent to Business Service Management, 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 Topologies" in *Using Transaction Management*.

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 HP Real User Monitor Engine Web Console" on page 138.

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 EUM 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" on page 252.

➤ **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 "Component Properties/Graph Overview Pane" on page 253.

➤ **Topology View.** Displays the topology flow map or table for a selected transaction. For user interface details, see "Topology View Pane" on page 254.

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	The time frame settings for which data is displayed in the Main View pane. Configure the following settings:
	
	➤ **Fixed time frame:**
	   ➤ **From.** Select the starting date and time
	   ➤ **To.** Select the ending date and time
	➤ **Variable time frame:**
	   ➤ **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.
	
	Note: The starting and ending dates and times are updated and displayed according to the selections you make.

Component 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.
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).
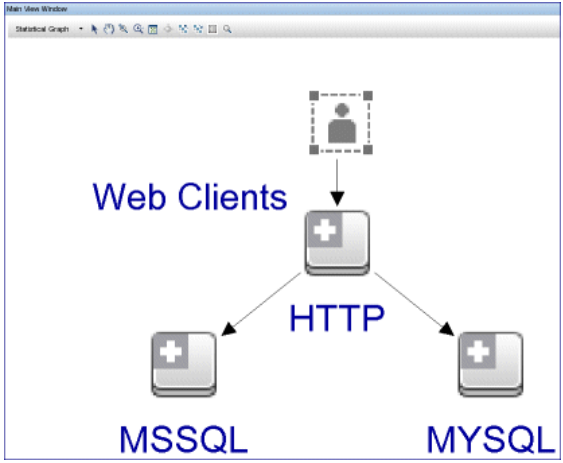
Topology Map - Statistical Graph
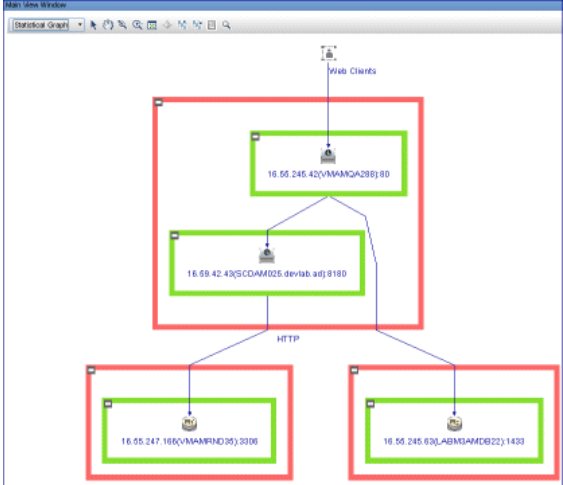
This tab displays a selected transaction's topology flow map as a graph.

User interface elements are described below:

UI Element	Description
▸	**Select.** Enables selecting a component in the topology flow map. N**ote:** 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.

UI Element	Description
	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.
	Marquee Zoom. Zooms on a selected area of the topology flow map.
	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.
	Fit Screen. Fits all the flow map components into the visible area.
	Navigate Communication Channel. Enables navigating between components of the topology flow map.
	You click the Navigation Communication Channel button and then click a line connecting two components or subcomponents. The cursor navigates to the endpoint component.

UI Element	Description
	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. **Note:** This is the default setting when you enter the topology flow map. **Example:**

UI Element	Description
	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. **Example:**
	Properties Dialog. Opens the Graph Properties dialog box, where you can configure the default layout properties for the graph.

UI Element	Description
<Display mode>	Select a display mode from the following options: ➤ **Statistical Graph.** Displays the topology flow map as a graph. **Note:** This is the default display mode. ➤ **Pattern Tree.** Displays the topology flow map as a table. For user interface details, see "Topology Map - Pattern Tree" on page 259.
<Topology flow map>	In the topology flow map, you can do the following: ➤ 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 254. ➤ 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 260. ➤ 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 page 261.
✖	**Remove Transaction Pattern Element.** Deletes a selected pattern rule from the selected topology.
<Display mode>	Select a display mode from the following options: ➤ **Statistical Graph.** Displays the topology flow map as a graph. For user interface details, see "Topology Map - Statistical Graph" on page 254. **Note:** This is the default display mode. ➤ **Pattern Tree.** Displays the topology flow map as a table.
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.

UI Element	Description
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 page 260.
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.

12

Real User Monitor Engine File Configuration

Some of the settings used by the Real User Monitor engine are made in various files that you can edit.

This chapter includes:

➤ Configuring Meaningful Page Names on page 263

➤ Unifying Frames on page 289

Configuring Meaningful Page Names

You can configure HP Real User Monitor to change the URLs of recorded pages that are not configured in End User Management Administration to more meaningful names for use in HP Real User Monitor reports. For information on configuring pages for monitoring, see "<Action> Dialog Box" in *Using End User Management*. For information on HP Real User Monitor reports, see "End User Management Reports" in *Using End User Management*.

This section includes the following topics:

➤ "About Meaningful Page Names" on page 264

➤ "Formatting Tags" on page 265

➤ "Rules Tags" on page 275

➤ "Sample XML File" on page 279

➤ "Validating Meaningful Name XML Files" on page 285

➤ "Adding and Deleting Meaningful Name XML Files" on page 286

➤ "Changing Meaningful Name XML Files" on page 287

➤ "Viewing Meaningful Page Statistics" on page 287

About Meaningful 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 recorded 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 "Real User Monitor Application Configuration Wizard" in *Using End User Management*. For information on configuring pages for monitoring, see "<Action> Dialog Box" in *Using End User Management*.

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 recorded 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 HP Real User Monitor reports. 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 HP Real User Monitor reports. For information on HP Real User Monitor reports, see "End User Management Reports" in *Using End User Management*.

The XML file must be created in the \<**HP Real User Monitor root directory**>**conf****resolver****meaningful_pages** directory on the HP Real User Monitor engine machine. For convenience, it is recommended 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: HP Real User Monitor 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: It is recommended to 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 HP Real User Monitor 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 285), the tags must appear in the XML file in the order in which they are listed below:

URLDecoder

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	<Rename Name="RenameToABC123" String="HP" When the **RenameToABC123** formatting command is referenced in a rule, the entire source string is renamed to **HP**.

Substring

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

Syntax	<SubString Name="**Command_Name**" BeginIndex="**Start_Char_Index**" Count="**Length**"/>
Explanation	**Command_Name.** The name of the Substring formatting tag that can be used in Rule tags. **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. **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.
Example	<Substring Name="ExtractTenToTwelve" BeginIndex="10" Count="3"/> When the **ExtractTenToTwelve** formatting command is referenced in a rule, the tenth, eleventh, and twelfth characters of the source string are extracted.

ExtractStrToStr

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

Syntax	<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**"/>

Explanation	**Command_Name.** The name of the ExtractStrToStr formatting tag that can be used in Rule tags. **Start_String.** The starting string from which the required string is to be extracted. **Include_Start_String.** Whether to include the starting string as part of the extracted string. Valid options are: ➤ **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. **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**. **End_String.** The ending string up to which the required string is to be extracted. **Include_End_String.** Whether to include the ending string as part of the extracted string. Valid options are: ➤ **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. **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**.
Example	<ExtractStrToStr Name="ExtractBetweenABCandXYZ" fromString="ABC" fromInclude="true" fromOccurrences="2" toString="XYZ" toInclude="false" toOccurrences="1"/> 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.

ExtractIndexToStr

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

Syntax	<ExtractIndexToStr Name="**Command_Name**" fromIndex="**Start_Char_Index**" toString="**End_String**" toInclude="**Include_End_String**" toOccurrences="**Occurrences_End_String**"/>
Explanation	**Command_Name.** The name of the ExtractIndexToStr formatting tag that can be used in Rule tags.
	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.
	End_String. The ending string up to which the required string is to be extracted.
	Include_End_String. Whether to include the ending string as part of the extracted string. Valid options are:
	➤ **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.
	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**.
Example	<ExtractIndexToStr Name="ExtractBetween3andXYZ" fromIndex="3" toString="XYZ" toInclude="false" toOccurrences="1"/>
	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.

ExtractStrIToCount

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

Syntax	<ExtractStrToCount Name="**Command_Name**" fromString="**Start_String**" fromInclude="**Include_Start_String**" fromOccurrences="**Occurrences_Start_String**" count="**Length**" />
Explanation	**Command_Name.** The name of the ExtractStrToCount formatting tag that can be used in Rule tags.
	Start_String. The starting string from which the required string is to be extracted.
	Include_Start_String. Whether to include the starting string as part of the extracted string. Valid options are:
	➤ **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.
	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**.
	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.
Example	<ExtractStrToCount Name="ExtractBetweenABCfor5" fromString="ABC" fromInclude="false" fromOccurrences="1" count="5"/>
	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.

Insert

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

Syntax	<Insert Name="**Command_Name**" String="**Insert_String**" ToIndex="**Start_Char_Index**" CountFromBeginning="**Direction**"/>
Explanation	**Command_Name.** The name of the Insert formatting tag that can be used in Rule tags.
	Insert_String. The string to be inserted in the source string.
	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.
	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:
	➤ **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	<Insert Name="InsertABCAfterOrder" String="ABC" ToIndex="5"/>
	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).

ChangeCase

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

Syntax	<ChangeCase Name="**Command_Name**" Type="**Case_Type**" BeginIndex="**Start_Char_Index**" Count="**Length**"/>
Explanation	**Command_Name.** The name of the ChangeCase formatting tag that can be used in Rule tags.
	Case_Type. The type of conversion to be carried out. The valid options are:
	➤ **UpperCase.** Lower case to upper case. This is the default if no type is specified.
	➤ **LowerCase.** Upper case to lower case.
	➤ **OpposisteCase.** Switches the case of characters.
	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.
	Length. The number of characters from the Start_Char to be converted.
Example	<ChangeCase Name="UpperCaseFirstChar" Type="UpperCase" BeginIndex="0" Count="1"/>
	When the **UpperCaseFirstChar** formatting command is referenced in a rule, the first character of the source string is converted to upper case.
Note	If **Length** is not specified, the ChangeCase conversion is carried out from the **Start_Char** to the end of the source string.

Remove

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

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

RemoveNonAlpha

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

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

Replace

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

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

Alias

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

Syntax	<Alias Name="**Command_Name**"> <Pair Name="**Source_String**" Alias="**Assigned_Alias**"/> </Alias>
Explanation	**Command_Name.** The name of the Alias formatting tag that can be used in Rule tags. **Source_String.** The alphanumeric string to which you are assigning an alias. **Assigned_Alias.** The alias you are assigning to replace the Source_String.
Example	<Alias Name="RelateLettersToCategory"> <Pair Name="fi" Alias="Fish"/> </Alias> When the **RelateLettersToCategory** formatting command is referenced in a rule, all occurrences of the string **fi** are replaced with the alias **Fish**.
Note	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.

Rules 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 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 265). 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 HP Real User Monitor 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

```xml
<?xml version="1.0" ?>
<Meaningful_Pages xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSc
 – <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="UpperCaseEigthLetter" 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" />
```

```xml
      <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 AppendToCartS
        </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>
```

```xml
          <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 AppendFr
        </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 UpperCaseFirst(
      </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 U
      </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 Meangingful Names for URLs

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)
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

URL	Meaningful Name
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:

\<HP Real User Monitor root directory>\conf\resolver\
meaningfulpages.xsd

To validate a meaningful 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 HP Real User Monitor 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).

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 265). 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 HP Real User Monitor to reread the End User Management Administration configuration. For information on configuring applications for monitoring, see "Real User Monitor Application Configuration Wizard" in *Using End User Management*.

To force HP Real User Monitor to reread the End User Management Administration configuration:

1 Access the HP Real User Monitor Web console (for details, see "Accessing the HP Real User Monitor Engine Web Console" on page 138).

2 From the **Configuration** menu, select **Engine Configuration Per Data Type**. The Engine Configuration Page opens.

3 Click the **Sync All Configuration** button to force the HP Real User Monitor engine to reload the HP Real User Monitor configuration from HP Business Service Management.

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 HP Real User Monitor to reload the configuration for the specific application. For information on configuring applications for monitoring, see "Real User Monitor Application Configuration Wizard" in *Using End User Management*.

To force HP Real User Monitor to reload the configuration for an application:

1 Access the JMX console by choosing **JMX Console** from the Configuration drop-down menu in the HP Real User Monitor 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=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 HP Real User Monitor.

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

Viewing Meaningful Page Statistics

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

To view meaningful page statistics:

1 Access the JMX console by choosing **JMX Console** from the Configuration drop-down menu in the HP Real User Monitor 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=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 "Real User Monitor Application Configuration Wizard" in *Using End User Management*.)
Configuration file name	The name of the meaningful page XML file used by the application.
Handled pages	The total number of pages monitored in the application that were submitted to the meaningful pages module.
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 HP Real User Monitor 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.

HP Real User Monitor 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 HP Real User Monitor in the **frame_unification.xml** file on the HP Real User Monitor engine machine.

To change the default settings for frame unification:

1 Edit the **<HP Real User Monitor root directory>\conf\ configurationmanager\frame_unification.xml** file on the HP Real User Monitor 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<**HP Real User Monitor root directory**>**conf\ configurationmanager\frame_unification.xml** file on the HP Real User Monitor 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 HP Real User Monitor 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.

13

Configuring the HP Real User Monitor Probe

You can configure the HP Real User Monitor probe by changing the default settings and adding additional configuration settings.

This chapter includes:

➤ Changing the Protocol for Accessing the HP Real User Monitor Probe on page 293

➤ Limiting WebConsole Resources on page 294

➤ Configuring the HP Real User Monitor Probe for I18N on page 295

➤ Changing the Header in Which to Locate Client IP Addresses on page 296

➤ Creating Default Configuration and Properties Files for a Specific Probe on page 297

➤ Configuring the HP Real User Monitor Probe to Support Multiprotocol Label Switching (MPLS) on page 298

Changing the Protocol for Accessing the HP Real User Monitor Probe

The default protocol used for accessing the Real User Monitor (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 193.

Limiting WebConsole Resources

For security reasons, the WebConsole resources of the HP Real User Monitor probe are limited by default, so that only configuration updates and general statistics are available. You can remove this limitation for troubleshooting so that all resources are available.

Note: It is recommended to reset the limitation after you have finished troubleshooting.

To change the availability of WebConsole resources:

1 Edit the **/etc/rum_probe/rpsecurity.conf** file on the probe machine.

Note: On Windows installations of the probe, the **/etc/rum_probe** directory is located in the HP Real User Monitor probe root directory.

---

2 In the **webconsole** section of the file, change the setting of the **restrict_webconsole** parameter to **true** (to impose the limitation) or **false** (to remove the limitation).

3 Save the file.

4 Restart the HP Real User Monitor probe.

Configuring the HP Real User Monitor Probe for I18N

By default, HP Real User Monitor uses the UTF-8 character set when monitoring data. To enable HP Real User Monitor to support non Unicode encodings, you can configure the HP Real User Monitor probe to use a different character set.

To change the character set used by the HP Real User Monitor probe when monitoring data:

In the **<HP Real User Monitor root directory>\conf\ configurationmanager\Beatbox_Default_Const_Configuration.xml** file on the HP Real User Monitor engine, under the **[global]** section, add the following lines:

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

where:

➤ **<false/true>.** Set to **true** to enable HP Real User Monitor 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 HP Real User Monitor searches for a character set. By default, HP Real User Monitor 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 HP Real User Monitor 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 **<HP Real User Monitor root directory>\conf\ configurationmanager\Beatbox_Default_Const_Configuration.xml** file on the HP Real User Monitor 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, HP Real User Monitor tries to locate client IP addresses using the **X-Foward-For** header. If client IP addresses are located in a different header (for example, in a custom header) you can configure HP Real User Monitor to use that header when trying to locate client IP addresses.

To change the header used by the HP Real User Monitor probe when locating client IP addresses:

1 In the **<HP Real User Monitor root directory>\conf\ configurationmanager\Beatbox_Default_Const_Configuration.xml** file on the HP Real User Monitor 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 Real User Monitor engine Web console, synchronize configuration data by selecting **Tools** > **Monitoring Configuration Data** > **Sync All Configuration**. For details, see "Monitoring Configuration Information" on page 223.

Creating Default Configuration and Properties Files for a Specific Probe

The Real User Monitor 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 Real User Monitor Engine, in the **<HP Real User Monitor 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 Real User Monitor. 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 Real User Monitor Engine, in the **<HP Real User Monitor 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 Real User Monitor. For example:

probe.123.4.5.67.properties

3 Edit the file as required with the properties for the specific probe.

Configuring the HP Real User Monitor Probe to Support Multiprotocol Label Switching (MPLS)

By default, the Real User Monitor Probe does not support MPLS.

To enable MPLS support:

1 Edit the **<HP Real User Monitor root directory>\conf\ configurationmanager\Beatbox_Default_Const_Configuration.xml** file on the HP Real User Monitor 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.

14

Administering the MySQL Database

For HP Real User Monitor to work, it must be connected to a MySQL database that has been created and started.

This chapter includes:

➤ Overview of the MySQL Database on page 299

➤ Creating and Connecting to the MySQL Database on page 300

➤ Starting and Stopping the MySQL Database on page 301

➤ Maintaining the MySQL Database on page 302

Overview of the MySQL Database

The MySQL database is the HP Real User Monitor's data repository. The data that is stored in the MySQL database is data that is either not forwarded at all to HP Business Service Management, or that is only sent on request.

Data that is not forwarded at all to HP Business Service Management is HP Real User Monitor configuration data. Data that is sent to HP Business Service Management on request is open session data and session click-stream data (data and snapshots of pages included in sessions). Click-stream 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 HP Real User Monitor engine or on its own machine. For system requirements for the MySQL database, see "Reviewing System Requirements" on page 37.

Creating and Connecting to the MySQL Database

The HP Real User Monitor engine MySQL database is created during the HP Real User Monitor engine installation process, if that option is selected. When the MySQL database is created during the installation process, the HP Real User Monitor engine is connected to it, and the MySQL database is started automatically. The MySQL database to which the HP Real User Monitor engine is connected must be started for the HP Real User Monitor engine to work.

You can create a new MySQL database schema and connect the HP Real User Monitor engine to it, or connect the HP Real User Monitor engine to a different, existing MySQL database completely, if required.

Note: The HP Real User Monitor engine can only be connected to one MySQL database.

To create schemas and connect to MySQL databases on an HP Real User Monitor Windows installation:

On the machine on which the HP Real User Monitor engine is installed, select **Start** > **Programs** > **HP Real User Monitor** > **Administration** > **RUM Configuration Tool**. The HP Real User Monitor Configuration tool starts. For details on working with the HP Real User Monitor Configuration tool, see "Real User Monitor Configuration Wizard" on page 56.

Starting and Stopping the MySQL Database

When the MySQL database is created during HP Real User Monitor 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 an HP Real User Monitor Windows installation:

On the machine on which the HP Real User Monitor engine is installed, select **Start** > **Programs** > **HP Real User Monitor** > **Administration** > **Database** > **Start Real User Monitor Database**.

To stop the MySQL database on an HP Real User Monitor Windows installation:

On the machine on which the HP Real User Monitor 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/administrator/en/).

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/administrator/en/).

HP Real User Monitor 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 HP Real User Monitor Web console, or by using the following URL in you 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=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 **<HP Real User Monitor root directory>\conf\ partitionmanager\pm_tables_config.xml** file on the HP Real User Monitor engine machine.

2 Change the setting **<archiveDuration units="DAYS" qty="14"/>** from 14 to the required number of days.

3 Save the file.

Note: By increasing the number of days for which session click-stream data is stored, you might significantly increase the size of the database, which might necessitate additional disk capacity.

15

Hardening HP Real User Monitor

You can harden the HP Real User Monitor 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:

➤ Hardening the HP Real User Monitor Probe on page 305

➤ Securing Connections to the HP Real User Monitor Engine on page 311

Note: For details on securing connections between HP Real User Monitor and HP Business Service Management, see the *HP Business Service Management Hardening Guide* PDF.

Hardening the HP Real User Monitor Probe

You can harden the HP Real User Monitor 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" on page 306

➤ "Limiting Access to the Probe" on page 307

➤ "Limiting the SSH Version" on page 307

➤ "Securing the HTTP Connection to the Probe" on page 307

Changing the Probe's User and Password

Note: This section applies to the HP Real User Monitor Probe only when it is installed on a Linux system.

When the HP Real User Monitor 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 Real User Monitor 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 Real User Monitor Engine connects to the Real User Monitor Probe via the probe's Web Console. It is recommended to limit access to the Real User Monitor Probe by disabling access to other, unnecessary services according to you organization's security policies.

Limiting the SSH Version

Note: This section applies to the HP Real User Monitor 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 Real User Monitor 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 HP Real User Monitor version 7.0 and later, the Real User Monitor 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 HP Real User Monitor) it might be necessary to manually configure HP Real User Monitor 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 HP Real User Monitor 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 **\<HP Real User Monitor 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 HP Real User Monitor Web console and selecting **Tools** > **Monitoring Configuration Information** > **Sync All Configuration**. For details on working with the HP Real User Monitor Web console, see "Using the HP Real User Monitor Web Console" on page 137.

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:

\<HP Real User Monitor root directory>\JRE\bin\keytool -import -alias rum_probe_cert -keystore <KEYSTORE_FILE> -file <CERTIFICATE_FILE>

Note: The Real User Monitor engine should be configured to trust the imported certificate.

---

7 Edit the **\<HP Real User Monitor 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 HP Real User Monitor Web console and selecting **Tools** > **Monitoring Configuration Information** > **Sync All Configuration**. For details on working with the HP Real User Monitor Web console, see "Using the HP Real User Monitor Web Console" on page 137.

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:

\<HP Real User Monitor 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 **\<HP Real User Monitor 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 on page 310, edit or add the following line:

connection.http.ssl.keystore.PrivateKeypassword=<KEY PASSWORD>

5 Export the client certificate with the command:

\<HP Real User Monitor 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_CERTITIFICATE_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 HP Real User Monitor Web console and selecting **Tools** > **Monitoring Configuration Information** > **Sync All Configuration**. For details on working with the HP Real User Monitor Web console, see "Using the HP Real User Monitor Web Console" on page 137.

Securing Connections to the HP Real User Monitor Engine

You can access HP Real User Monitor engine by different http access points, for the following purposes:

➤ RUM Web console

➤ RUM JMX console

➤ RUM Gateway/Proxy Server (for HP Business Service Management and the replay applet)

You can secure access to the HP Real User Monitor engine by using authentication and https connections.

This section includes the following topics:

➤ "Using Authentication" on page 312

➤ "Using HTTPS" on page 313

Using Authentication

All http access points on the HP Real User Monitor engine are protected via authentication mechanisms. The two main authentication mechanisms used are:

➤ **User and password protection.** Used for access to the HP Real User Monitor engine Web and JMX consoles.

➤ **Basic authentication.** Used for all other access points to the HP Real User Monitor 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 HP Real User Monitor Web Console" on page 137.

To change the password for a user to access the JMX console:

1 On the engine machine, edit the \<**HP Real User Monitor 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 HP Real User Monitor 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 HP Real User Monitor engine using https. For details on hardening HP Business Service Management, including creating, configuring, and trusting client and server certificates, see the *HP Business Service Management Hardening Guide* PDF.

In HP Business Service Management, when viewing session details in Real User Monitor reports, you can view snapshots of pages and replay a session. By default, the Session Replay applet retrieves data from the Real User Monitor engine via the HP Business Service Management Gateway Server, but can be configured to retrieve data directly from the Real User Monitor engine (for details, see "Determining How the Real User Monitor Snapshot Applet Retrieves Snapshots" in *Using End User Management*). If the Session Replay applet is configured to retrieve data directly from the Real User Monitor engine and the Real User Monitor 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 Real User Monitor engine with the command:

\<HP Real User Monitor 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 HP Business Service Management 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>

   c Restart the browser.

Note: HP recommends to configure the Session Replay applet to retrieve data from the Real User Monitor engine via the HP Business Service Management Gateway Server, when the Real User Monitor engine is configured to require a client certificate.

Part IV

Supporting Specific Protocols

16

Parsing Supported Protocols

Parsing supported protocols are protocols on which Real User Monitor can carry out deep analysis, thus providing detailed data about monitored applications for use in End User Management reports.

Real User Monitor supports the following protocols for parsing:

HTTP Protocols

➤ HTTP/S

➤ SOAP

Database Protocols

➤ IBM DB2

➤ Microsoft SQL Server

➤ MySQL Database Server

➤ Oracle DB (Thin JDBC Client)

Mail Protocols

➤ IMAP (Internet Message Access Protocol)

➤ POP3 (Post Office Protocol)

➤ SMTP (Simple Mail Transfer Protocol)

Generically Supported Protocols

➤ DNS – Generic UDP

➤ Flash/ActionScript AMF – HTTP Based

➤ Microsoft Terminals Services (RDP) – Generic Streaming TCP

➤ RMI Registry – Generic TCP

➤ SAPGUI – Generic TCP

➤ SSH – Generic Streaming TCP

Others

➤ Citrix XenApp

➤ FTP (File Transfer Protocol)

➤ IBM WebSphere MQ

➤ ISO 8583 (financial transaction card originated messages for Visa and Mastercard)

➤ LDAP (Lightweight Directory Access Protocol)

➤ Oracle Forms NCA

17

Monitoring Citrix with Real User Monitor

You can use Real User Monitor's HTTP RUM agent to monitor Citrix traffic.

This chapter includes:

➤ Overview of Citrix Monitoring with Real User Monitor on page 319

➤ Overview of the RUM HTTP Agent on page 322

➤ Installing the RUM HTTP Agent on page 323

➤ Configurations for Working with the RUM HTTP Agent on page 324

➤ Advanced Configuration on page 326

➤ Using the RUM HTTP Agent with Terminal Services on page 327

Overview of Citrix Monitoring with Real User Monitor

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 the following topics:

➤ "Monitoring Traffic Between End Users and a XenApp Server" on page 320

➤ "Monitoring Outgoing Traffic from a XenApp Server" on page 321

Monitoring Traffic Between End Users and a XenApp Server

The following diagram shows typical traffic between end users and a Citrix XenApp server:
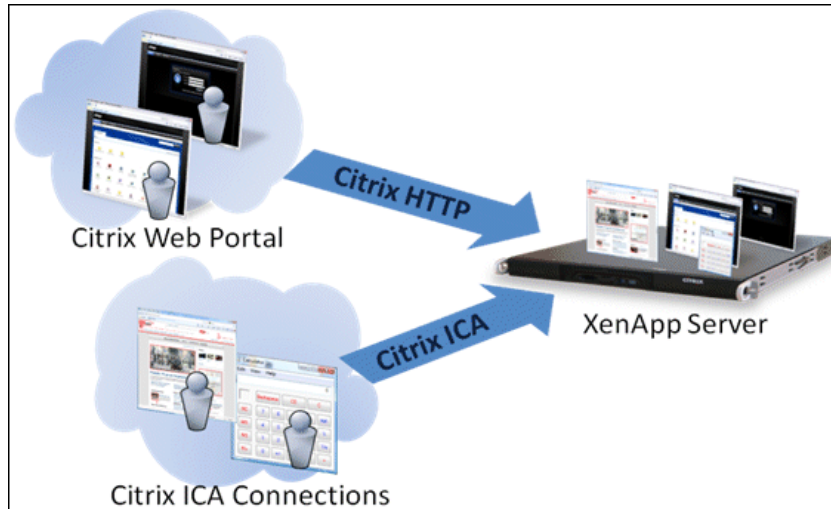
An end user starts by opening a Citrix Web portal and selecting one of the published applications. An ICA session is created, in which the selected application runs on the XenApp server, and the user uses the application remotely.

Alternatively, a user can create an ICA connection directly, without going through a Web portal.

To monitor this traffic with Real User Monitor 9.x or later, no agent installation is required and you just configure the application in Business Service Management using the **Citrix HTTP** and **Citrix ICA** application templates. For user interface details on creating Real User Monitor applications in Business Service Management, see "Real User Monitor Application Configuration Wizard" in *Using End User Management.*

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.

When monitoring the Web server with Real User Monitor, 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 HTTP Agent on the XenApp server.

The following table shows the difference between Real User Monitor reports when the RUM HTTP Agent is, or is not, installed on the XenApp server:

Request URL	Without RUM HTTP Agent		With RUM HTTP 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 HTTP Agent

You use the RUM HTTP Agent to monitor traffic from a XenApp server for the initiating end user.

This section includes the following topics:

➤ "Supported Environments" on page 322

➤ "Supported Applications" on page 322

➤ "How the RUM HTTP Agent Works" on page 323

Supported Environments

The RUM HTTP Agent can be installed on the following environments:

➤ Windows 2003 Server or later (32 and 64 bit versions)

➤ XenApp server 4.5 or later (installed on Windows 2003 Server or later)

Supported Applications

The RUM HTTP Agent monitors traffic for the following applications:

➤ Internet Explorer 6

➤ Internet Explorer 7

➤ Internet Explorer 8

➤ Mozilla Firefox 2

➤ Mozilla Firefox 3

In addition to the above applications, the RUM HTTP Agent can support a wide range of software based on Microsoft's WebBrowser ActiveX component.

How the RUM HTTP Agent Works

The RUM HTTP 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 **UserAgent** HTTP header.

Installing the RUM HTTP Agent

The setup file for installing the RUM HTTP Agent depends on your operating system. The following setup files are available:

➤ HPRumHttpAgent_v-<Version number>_win32.msi—for 32bit systems

➤ HPRumHttpAgent_v-<Version number>_win64.msi—for 64bit systems

To install the RUM HTTP Agent:

1 Click the relevant link on the Business Service Management **Downloads** page (which you access from the Setup and Maintenance tab in Platform Administration) to download the required setup file to the machine on which you want to install the RUM HTTP Agent.

Note: For the RUM HTTP Agent setup files to be available on the Downloads page, they must first be installed to HP Business Service Management. For details on installing HP Business Service Management components setup files, see "Installing Component Setup Files" in the *HP Business Service Management Deployment Guide* PDF.

If you prefer, you can copy the RUM HTTP Agent setup files directly from the Data Collectors and Components directory on the HP Business Service Management DVD, for versions delivered on DVD.

---

2 Run the setup program by double clicking the downloaded file.

3 Follow the online instructions. (During the installation, you are prompted to select the program location.)

Note: The RUM HTTP Agent delivers digitally signed DLL files.

Configurations for Working with the RUM HTTP Agent

You must configure user name detection in the applications you want monitored using the RUM HTTP Agent. Additionally, you can 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.

This section includes the following topics:

➤ "To configure user name detection in applications" on page 324

➤ "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 page 325

To configure user name detection in applications

1 In End User Management Administration in Business Service Management, 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:

Field	Value
Search in	HTTP Header
Header name	User-Agent
Extract text: **Between** **and**	RUM_CLIENT_NAME)

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 Real User Monitor Engine, edit the file:

<HPRUM>\conf\configurationmanager\Beatbox_Default_Const_Configuration .xml

2 Add the following line at the end of the **[Global]** section:

forwarded_for_header User-Agent .*RUM_CLIENT_ADDRESS =IPV4*([^;]*);.* $1

3 Save the file.

4 In the Real User Monitor Engine Web console, synchronize configuration data by selecting **Tools** > **Monitoring Configuration Data** > **Sync All Configuration**. For details, see "Monitoring Configuration Information" on page 223.

Advanced Configuration

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 HTTP Agent is installed.

(For example, C:\Documents and Settings\All Users\Application Data\HP\RumHttpAgent\settings\RumHttpAgent.cfg.)

This section includes the following topics:

To disable the RUM HTTP Agent

In the [**common**] section of the file, change the **disable** parameter value to **true**. The change takes effect for new IE and Firefox browser instances.

To disable the RUM HTTP 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 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 HTTP Agent with Terminal Services

The RUM HTTP 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 HTTP Agent can be used to extract the real client's IP address and user name when monitoring the Web traffic with Real User Monitor.

Index