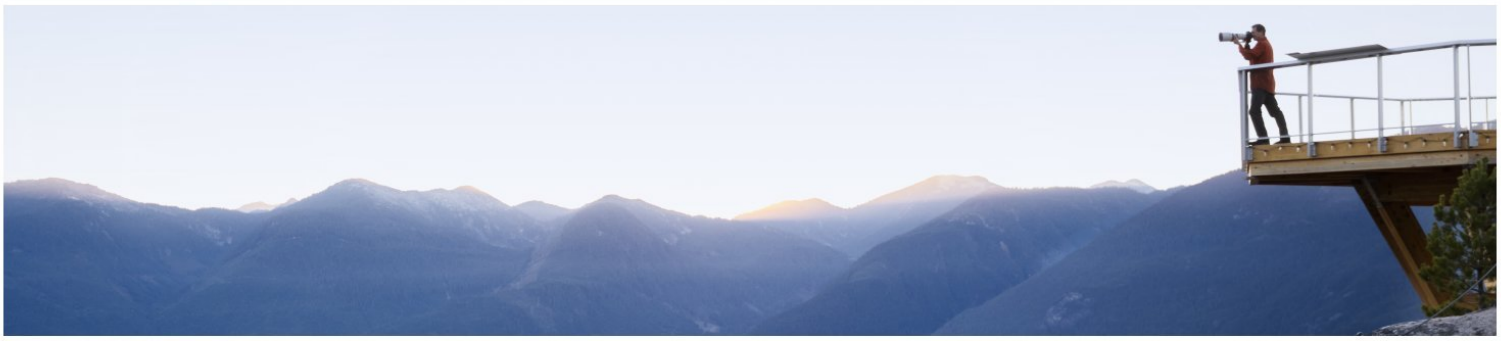
Real User Monitor

Version 9.51, Released November 2018

Real User Monitor Installation and Upgrade Guide

Published November 2018



Legal Notices

Disclaimer

Certain versions of software and/or documents (“Material”) accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus 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

Contains Confidential Information. Except as specifically indicated otherwise, a valid license is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2005 - 2018 Micro Focus or one of its affiliates

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.

Contents

Real User Monitor Installation and Upgrade Overview 5
Part 1: RUM System Requirements and Compatibility 6
Chapter 1: RUM System Requirements 7
Chapter 2: RUM Compatibility Matrixes 15
RUM–APM Compatibility Matrix 15
RUM Probe–RUM Engine Compatibility 15
Part 2: Installing RUM 16
Chapter 3: Installing the RUM Engine 17
The RUM Engine Setup File 17
How to Install the RUM Engine 17
RUM Configuration Wizard 20
Import User Configuration Data Page 20
Import Source Directory Page 22
MySQL Database Properties Page (Import Settings from Previous Distributed Installation) 24
MySQL Database Properties Page 25
Connect to Database Page 26
RUM Database Connection Parameters Page 27
RUM Engine Credentials Page 29
Finish Page 31
Installing RUM on Windows Server 2008 R2 Using Windows Remote Desktop 32
Running a Silent Installation 33
Chapter 4: Installing the RUM Sniffer Probe 37
Physically Connecting the Probe 37
How to Install the RUM Sniffer Probe 38
Running a Silent Installation 41
Stopping and Starting the Probe 42
Connecting the Probe to the RUM Engine 42
Installing an nCipher Card on the RUM Probe 42
Installation of SSL key Agent for Apache web server 44
Prerequisites 44
Configuration of Apache Agent 45
Chapter 5: Installing the RUM Client Monitor Probe 47
The RUM Client Monitor Probe Setup File 47
How to Install the RUM Client Monitor Probe 48
Stopping and Starting the RUM Client Monitor Probe 49
Connecting the RUM Client Monitor Probe to the RUM Engine 49
Installing the JavaScript Snippet 49

Instrumenting Mobile Applications for Android 52
Instrumenting Mobile Applications for iOS 58
Monitoring Hybrid Applications 60
Chapter 6: Installing the RUM Server Collector 61
Chapter 7: Installing the RUM VDI Agent 64
Chapter 8: Uninstalling RUM 65
Uninstalling the RUM Engine on a Windows Platform 65
How to Uninstall the RUM Engine Using the Windows Control Panel 65
RUM Configuration Wizard 66
Export User Configuration Data Page 66
Export Target Directory Page 67
Finish Page 68
Running a Silent Uninstall 69
Uninstalling the RUM Sniffer Probe 69
Uninstalling the RUM Client Monitor Probe 70
Uninstalling the RUM Server Collector 71
Uninstalling the RUM VDI Agent 72
Uninstall SSL Agent for Apache web server 72
Part 3: Upgrading RUM 74
Chapter 9: Workflow for Upgrading RUM 75
Upgrading to Version 9.51 from Versions Previous to 9.2x 75
Chapter 10: Upgrading the RUM Sniffer Probe 77
Chapter 11: Upgrading the RUM Client Monitor Probe 79
Chapter 12: Upgrading the RUM Engine 80
Flow for the RUM Engine Upgrade 80
Upgrading from a Typical Installation to a Distributed Installation 82
Upgrading from RUM Versions 9.2x and Above 82
Upgrading Database Data 83
Troubleshooting 84
Chapter 13: Upgrading the RUM Server Collector 86
Chapter 14: Upgrading the RUM VDI Agent 87
Chapter 15: Upgrading MySQL from version 5.5 to 5.7 88
Coexistence of earlier RUM Engine versions (9.2x or later) with latest RUM Engine 88
Manually Upgrade RUM Engine and MySQL Database – with No Raw Data Upgrade 89
Manually Upgrade RUM Engine and MySQL Database – with Raw Data Upgrade 89
Chapter 16: Upgrading RUM - Notes and Limitations 92
Renaming a MySQL Database Schema 93
Linux Installer Troubleshooting 95
Send Documentation Feedback 96

Real User Monitor Installation and Upgrade Overview

This guide provides detailed instructions on how to install and upgrade the (RUM) data collector.

For details on hardening the RUM Sniffer Probe, RUM Client Monitor Probe, and RUM Engine, see the Real User Monitor Hardening Guide. You can download this document from the Software Support site (https://softwaresupport.softwaregrp.com/).

For details on designing and planning the deployment of the RUM solution, see the Real User Monitor Deployment Planning Guide. You can download this document from the Software Support site (https://softwaresupport.softwaregrp.com/).

For details on administering and working with RUM, see the Real User Monitor Administration Guide.

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

This guide contains the following parts:

- "RUM System Requirements and Compatibility" on page 6

  Describes the system requirements necessary for installing RUM and the compatibility between the different versions of RUM and Application Performance Management.
- "Installing RUM" on page 16

  Explains how to install and uninstall the RUM Engine. Also explains how to install one or more RUM Probes.
- "Upgrading RUM" on page 74

  Describes the procedures for upgrading the RUM Engine and Probe. Also includes upgrade notes and limitations.

Part 1: RUM System Requirements and Compatibility

Chapter 1: RUM System Requirements

This chapter describes the recommended system requirements for running RUM.

Caution: For production systems, you must install the RUM Engine, Probe, and database on separate physical disks or with dedicated low latency (less than 10 milliseconds) network storage systems such as iSCSI.

This chapter includes the following topics:

- "RUM Engine Requirements" below
- "RUM Repository (MySQL Database) Requirements" on the next page
- "Requirements for Installing the RUM Engine and Repository (MySQL Database) on the Same Machine" on the next page
- "Client Requirements for Viewing the RUM Engine Web Console" on page 9
- "RUM Sniffer Probe Requirements" on page 9
- "RUM Client Monitor Probe Requirements" on page 12
- "RUM Server Collector Requirements" on page 12
- "RUM VDI Agent Requirements" on page 13
- "RUM on Virtual Platforms" on page 13

RUM 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:** Microsoft Windows Server 2012 R2 (64 bit) Standard Edition Microsoft Windows Server 2012 (64 bit) Standard Edition Microsoft Windows Server 2008 R2 SP1 (64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (64 bit) Standard and Enterprise Editions	**Windows:** Microsoft Windows Server 2016 (64 bit) Standard Edition and Datacenter Edition
Memory	4 GB	8 GB
Hard Drive	70 GB	70 GB
Network Card	Gigabit network adapter	2 Gigabit network adapters (one for database connectivity and one for probe connectivity)

RUM 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 2012 R2 (64 bit) Standard Edition Microsoft Windows Server 2012 (64 bit) Standard Edition Microsoft Windows Server 2008 R2 SP1 (64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (64 bit) Standard and Enterprise Editions	**Windows:** Microsoft Windows Server 2016 (64 bit) Standard Edition
Memory	4 GB	8 GB
Hard Drive	200 GB fast hard drive	2 TB SCSI disks RAID 0 (RAID 0 + 1 for high availability)
Network Card	Gigabit network adapter	Gigabit network adapter
MySQL Version	5.7.21 (installed by the RUM installation program)	5.7.21 (installed by the RUM installation program)

Requirements for Installing the RUM 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 Server
Operating System	**Windows:** Microsoft Windows Server 2012 R2 (64 bit) Standard Edition Microsoft Windows Server 2012 (64 bit) Standard Edition Microsoft Windows Server 2008 R2 SP1 (64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (64 bit) Standard and Enterprise Editions	**Windows:** Microsoft Windows Server 2016 (64 bit) Standard Edition
Memory	4 GB	8 GB

	Minimum	Recommended
Hard Drive	2 Disks: • 70 GB for the RUM Engine installation • 200 GB fast hard drive for the RUM repository	2 Disks: • 70 GB for the RUM Engine installation • 2 TB SCSI disks RAID 0 (RAID 0 + 1 for high availability) for the RUM repository.
	Note: It is important not to install the RUM Engine on the same disk as the RUM repository. The RUM repository is configured in the MySQL data path in the Configuration wizard during the RUM Engine installation. For details, see "MySQL Database Properties Page" on page 25.	
Network Card	Gigabit network adapter	Gigabit network adapter
MySQL Version	5.7.13 (installed by the RUM installation program)	5.7.13 (installed by the RUM installation program)

Client Requirements for Viewing the RUM Engine Web Console

	Minimum	Recommended
Supported Browsers	Microsoft Internet Explorer (IE) 11.0 Mozilla Firefox 52.x ESR 64 bit Google Chrome 65.0.3325.181	Microsoft Internet Explorer (IE) 11.0 Mozilla Firefox 52.x ESR 64 bit Google Chrome 65.0.3325.181

Note: The Probe Traffic Discovery feature (**RUM Engine web console > Configuration > Probe Management > [select probe] > Probe Traffic Discovery**) does not work with Firefox.

RUM Sniffer Probe Requirements

- ### Hardware and Operating System Requirements

	Minimum	Recommended
Computer/Processor	Dual-CPU Xeon 3.0 GHz Server	32 CPU Intel® Xeon® CPU E5-2630 V3 @ 2.40GHz

	Minimum	Recommended
Operating System	**Linux:** Red Hat Enterprise Linux (64 bit version): • RHEL 6.x • RHEL 7.0-7.5	
	Windows: Microsoft Windows Server 2012 R2 (64 Bit) Standard Edition Microsoft Windows Server 2008 R2 SP1 (64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (64 bit) Standard and Enterprise Editions	**Windows:** Microsoft Windows Server 2016 (64 bit) Standard Edition
Memory	8 GB	32 GB
Hard Drive	70 GB IDE/SATA	300 GB

	Minimum	Recommended
Network Card	**For connecting port mirrored cable:** 1 standard network card of either 1 or 10 GB. **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 standard network cards • 1 G to connect to the probe • 10 GB to monitor the traffic **Caution:** Two network cards are required if the TAP to which the RUM 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, provided that bandwidth restrictions are not exceeded.
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 • Python (an interpreted, interactive, object-oriented programming language)
rum_probe user	A user called **rum_probe** is automatically created during installation, but you must manually configure a password for this user.
Linux and Windows installation:	
Probe console port	Port 2020 is the default port used for accessing the Real User Monitor probe console. By default, HTTPS with client certificate is used.

RUM Client Monitor Probe 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 2012 R2 (64 bit) Standard Edition Microsoft Windows Server 2012 (64 bit) Standard Edition Microsoft Windows Server 2008 R2 SP1 (64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (64 bit) Standard and Enterprise Editions	**Windows:** Microsoft Windows Server 2016 (64 Bit) Standard Edition
Memory	4 GB	8 GB
Hard Drive	50 GB	70 GB
Network Card	Gigabit network adapter	2 Gigabit network adapters (one for RUM Engine connectivity and one for client data connectivity)
Supported Browser for RUM Browser Solution	Best optimized for Internet Explorer 11.0, as well as Firefox and Chrome	Microsoft Internet Explorer (IE) 11.0 Mozilla Firefox 52.x ESR 64 bit Google Chrome 65.0.3325.181

RUM Server Collector Requirements

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

	Minimum	Recommended
Computer/Processor	Dual-CPU Xeon 3.0 GHz Server	Dual-CPU Xeon 3.0 GHz Server

	Minimum	Recommended
Operating System	**Linux:** Red Hat Enterprise Linux (64 bit version): • RHEL 6.x • RHEL 7.0-7.5	
	Windows: Microsoft Windows Server 2012 R2 (64 bit) Standard Edition Microsoft Windows Server 2012 (64 bit) Standard Edition Microsoft Windows Server 2008 R2 SP1 (64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (64 bit) Standard and Enterprise Editions	**Windows:** Microsoft Windows Server 2016 (64 Bit) Standard Edition
Memory	4 GB	16 GB
Hard Drive	10 GB	10 GB
Network Card	Sharing the same NIC with App/Web Server	Dedicated NIC with the same bandwidth as the main NIC(s) + 25% overhead

RUM VDI Agent Requirements

	Minimum	Recommended
Computer/Processor	XenApp server 4.5 or later (installed on Windows 2008 R2 Server or later)	XenApp server 4.5 or later (installed on Windows 2008 R2 Server or later)
Operating System	**Windows:** Microsoft Windows Server 2008 R2 SP1 (64 bit) Standard and Enterprise Editions Microsoft Windows Server 2008 R2 (64 bit) Standard and Enterprise Editions	**Windows:** Microsoft Windows Server 2012 R2 (64 bit) Standard Edition Microsoft Windows Server 2012 (64 bit) Standard Edition
Hard Drive	20 MB	20 MB

Supported Browsers for HTTP Traffic

The RUM VDI Agent monitors HTTP traffic for Internet Explorer 11.0.

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

RUM on Virtual Platforms

We recommend installing RUM on physical servers when possible. However, when necessary, you can

install both the RUM Engine and Probe on a virtual platform. The following virtualization platforms are supported:

- VMware ESX 6.0
- VMware ESX 5.x
- VMware ESXi 5.0

For details on duplicating traffic for a RUM Probe on a virtual machine, see "Duplicating Traffic for RUM with VMware" in the Real User Monitor Administration Guide.

Note:

- For production systems, you must install the RUM Engine, Probe, and database on separate physical disks, or on any high performance storage system.
- For the RUM database, the default VMware disk performance is usually not sufficient as one physical disk is shared between several virtual machines.
- RUM installed on VMware with NAS (Network-attached storage) has been tested with a Netapp iSCSI connection with a latency of less than 10 milliseconds.
- The virtual machine should not have shared resources (disk space, CPU, RAM).

Chapter 2: RUM Compatibility Matrixes

This section includes the following information:

- "RUM–APM Compatibility Matrix" below
- "RUM Probe–RUM Engine Compatibility" below

RUM-APM Compatibility Matrix

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

Note: Most RUM features require that the APM and RUM versions are aligned.

Compatibility Matrix	APM 9.50	APM 9.40	APM 9.30	BSM 9.26	BSM 9.25
RUM 9.51	✓	✓	✓	✓	✓
RUM 9.50	✓	✓	✓	✓	✓
RUM 9.40	X	✓	✓	✓	✓
RUM 9.30	X	X	✓	✓	✓
RUM 9.26	X	X	X	✓	✓
RUM 9.25	X	X	X	X	✓

RUM Probe–RUM Engine Compatibility

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

Part 2: Installing RUM

Chapter 3: Installing the RUM Engine

To monitor real user activity, you must first install the RUM Engine on a Windows platform.

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 Release Notes PDF (rum_readme_<version number>.pdf) for any last minute notes and limitations, as well as for upgrade and service pack install instructions.

This section includes:

- "The RUM Engine Setup File" below
- "How to Install the RUM Engine" below
- "RUM Configuration Wizard" on page 20
- "Installing RUM on Windows Server 2008 R2 Using Windows Remote Desktop" on page 32
- "Running a Silent Installation" on page 33

The RUM Engine Setup File

The RUM Engine setup file can be accessed from one of the following locations:

- The RUM installation package.
- The Software Support Online web site (https://softwaresupport.softwaregrp.com/). Sign in using your Passport user name and password. Click **Manuals**. Under Document Type, select **Patches**. In the Search field, enter **RUM Engine Setup File**.
- The Downloads page in APM Platform Administration. For details, see the APM Platform Administration Guide.

  Note: There may be more recent versions of RUM than the version included in the APM Downloads page. For details, check the Software Support Online web site (https://softwaresupport.softwaregrp.com/).

How to Install the RUM Engine

For details on the system requirements for installing the RUM Engine, see "RUM System Requirements" on page 7.

Note:

- For production systems, you must install the RUM Engine, Probe, and database on separate physical disks.
- For better performance, we recommend installing the RUM Engine and the RUM Probe on the same local area network (LAN).

- Before installing the RUM Engine on Windows Server 2008 R2 using Windows Remote Desktop, refer to "Installing RUM on Windows Server 2008 R2 Using Windows Remote Desktop" on page 32.
- RUM MySQL installation is supported only on Windows and only using the RUM MySQL installation according to the hardware matrix ("RUM System Requirements" on page 7). Only the RUM MySQL installation is supported for use with the RUM Engine; all other MySQL installations are not supported.

  For best performance, we recommend installing the RUM Engine and MySQL on a single machine but on different physical drives.

To install the RUM Engine:

1. Save the RUM setup folder for Windows on the machine on which you are installing RUM. For more details on the location of the RUM setup file, see "The RUM Engine Setup File" on the previous page.
2. On this machine, navigate to the downloaded file and double-click **RUMEngine_<version number>_setup.exe**.
3. When prompted, select the installation language (default English) and click **OK**. The RUM 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 below 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:
   - **RUM - Core.** Installs the RUM Engine.
   - **RUM - DB.** Installs the MySQL database.
   - **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.)
8. Click **Next**.

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

9. Select the path of the folder in which you want to install the RUM Engine. Either accept the default path (**C:\RUM**), 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.
10. 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).

Note: When you go back and make the necessary corrections, the **Next** button may appear disabled. However, you can click it and continue with the installation.

11. 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.
12. 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 RUM Configuration wizard is automatically started. The wizard includes the following pages:

Page	Enables you to ...	For user interface details, see ...
Import User Configuration Data	Select whether you want to import user data settings from a previous RUM installation.	"Import User Configuration Data Page" on the next page
Import Source Directory	Select the path from which to import user data settings from a previous RUM installation.	"Import Source Directory Page" on page 22
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 25
Connect to Database	Configure whether to connect the RUM Engine to a MySQL database.	"Connect to Database Page" on page 26
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 27
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 29
Finish	View the status of the Configuration wizard.	"Finish Page" on page 31

13. When the RUM Configuration wizard has finished, the status of the RUM 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.
14. 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 APM.

To start RUM and configure connection settings:

1. Start RUM by executing **Enable Real User Monitor** from the computer's Start menu.

   Note: You can stop RUM by executing **Disable Real User Monitor** on the computer's Start menu.

   For additional information on starting and stopping RUM, see "Administering Real User Monitor" in the Real User Monitor Administration Guide.

2. Configure the connection settings to APM in the RUM web console. For details, see "APM Connection Settings" in the Real User Monitor Administration Guide.

RUM Configuration Wizard

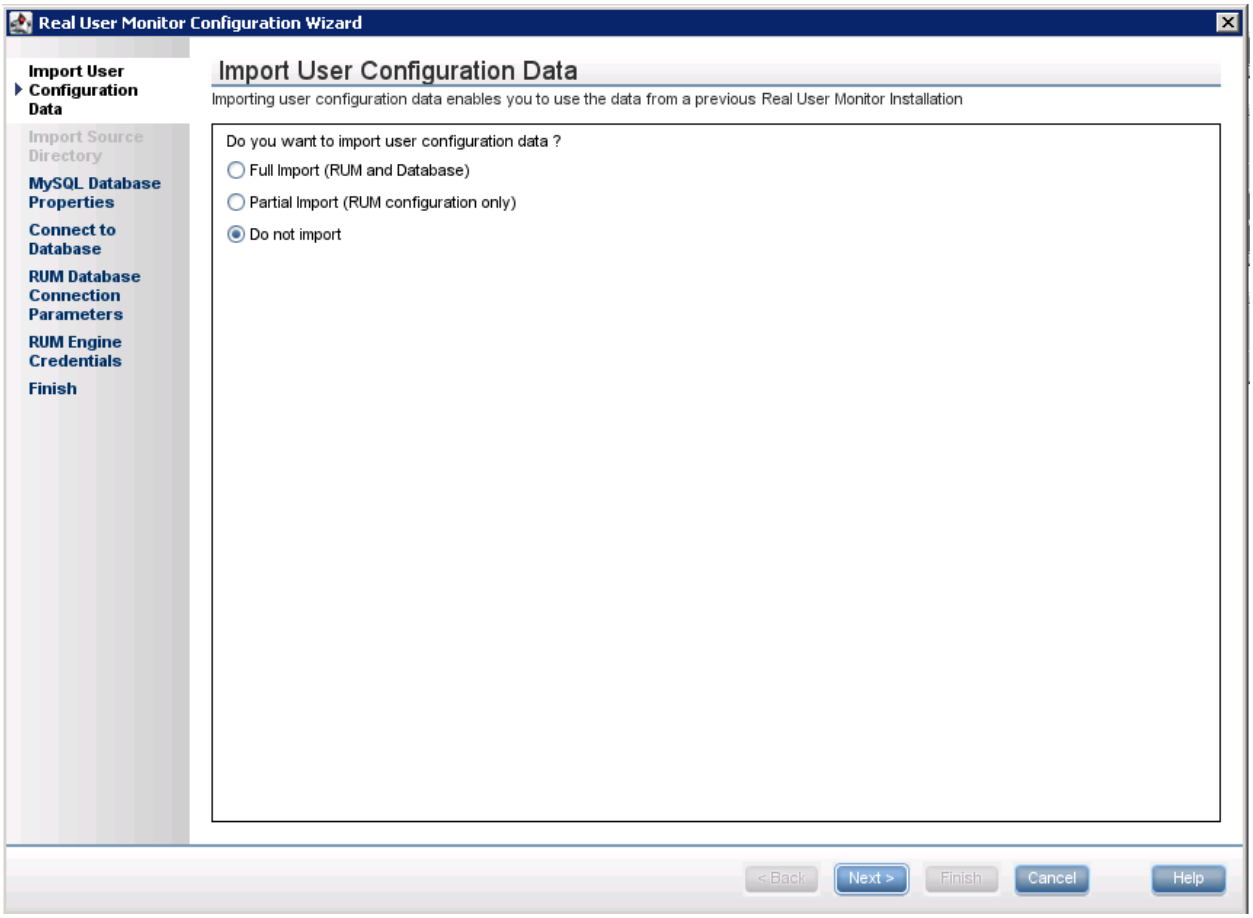
This wizard enables you to import configuration data from a previous installation, as well as to configure various connection parameters.

To access	The RUM Configuration wizard is automatically launched during a RUM installation, after the setup program has installed the RUM application.
Wizard Map	The RUM Configuration wizard contains: "Import User Configuration Data Page" below > "Import Source Directory Page" on page 22 > "MySQL Database Properties Page (Import Settings from Previous Distributed Installation)" on page 24 > "MySQL Database Properties Page" on page 25 > "Connect to Database Page" on page 26 > "RUM Database Connection Parameters Page" on page 27 > "RUM Engine Credentials Page" on page 29 > "Finish Page" on page 31
Useful Links	"Installing the RUM Engine" on page 17

Import User Configuration Data Page

This page enables you to select whether you want to import user data settings from a previous installation. This is part of the RUM Configuration wizard; refer to "RUM Configuration Wizard" above for general information.

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



The following elements are included:

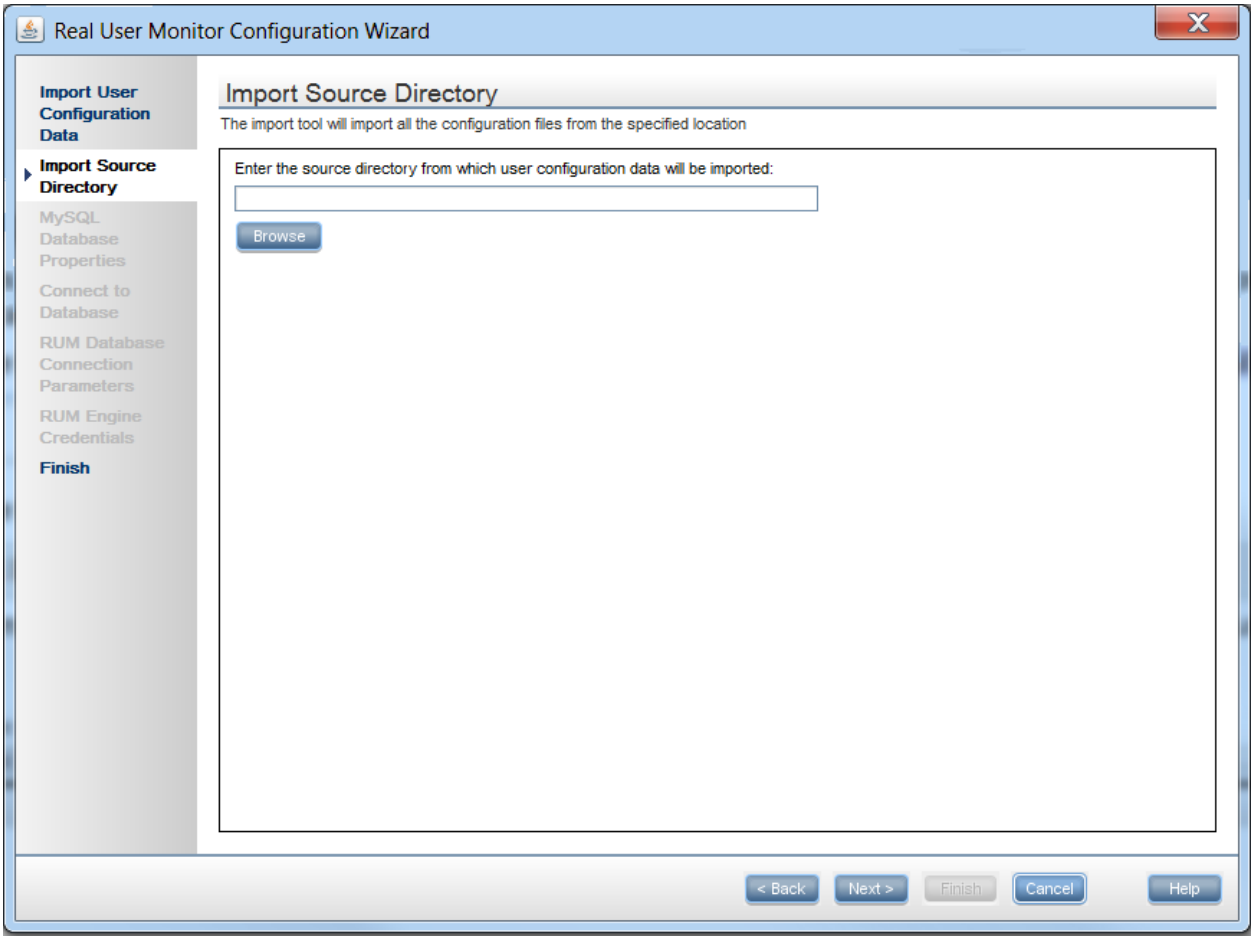
UI Element	Description
Full Import	Select this radio button if you want to import both your RUM user configuration and RUM database that you exported when uninstalling a previous version of RUM. **Note:** • If you want to include settings from an earlier version as part of a RUM upgrade, you must import the user data settings you saved when uninstalling the previous version. • The <MySQL data path> must be located in the same path in which it was located in the RUM installation from which you are importing. • If you import user data settings from a previous installation of RUM, the RUM Engine Credentials page is not accessed in the wizard.

UI Element	Description
Partial Import	Select this radio button if you want to import only your RUM user configuration that you exported when uninstalling a previous version of RUM. After your RUM user configuration is imported, the MySQL Database properties page appears (see "MySQL Database Properties Page" on page 25) which will enable you to install a new instance of MySQL. Enter the name and path of a new <RUM_DATA> folder or delete the contents of the C:\RUM_DATA post uninstall. If you delete the contents of <RUM_DATA>, you will lose all your old data. **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. • If you select this option, you will not be able to connect to an existing database.
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 "MySQL Database Properties Page" on page 25.

Import Source Directory Page

This page enables you to select the path from which to import user data settings from a previous RUM installation. This is part of the RUM Configuration wizard; refer to "RUM Configuration Wizard" on page 20 for general information.

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



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

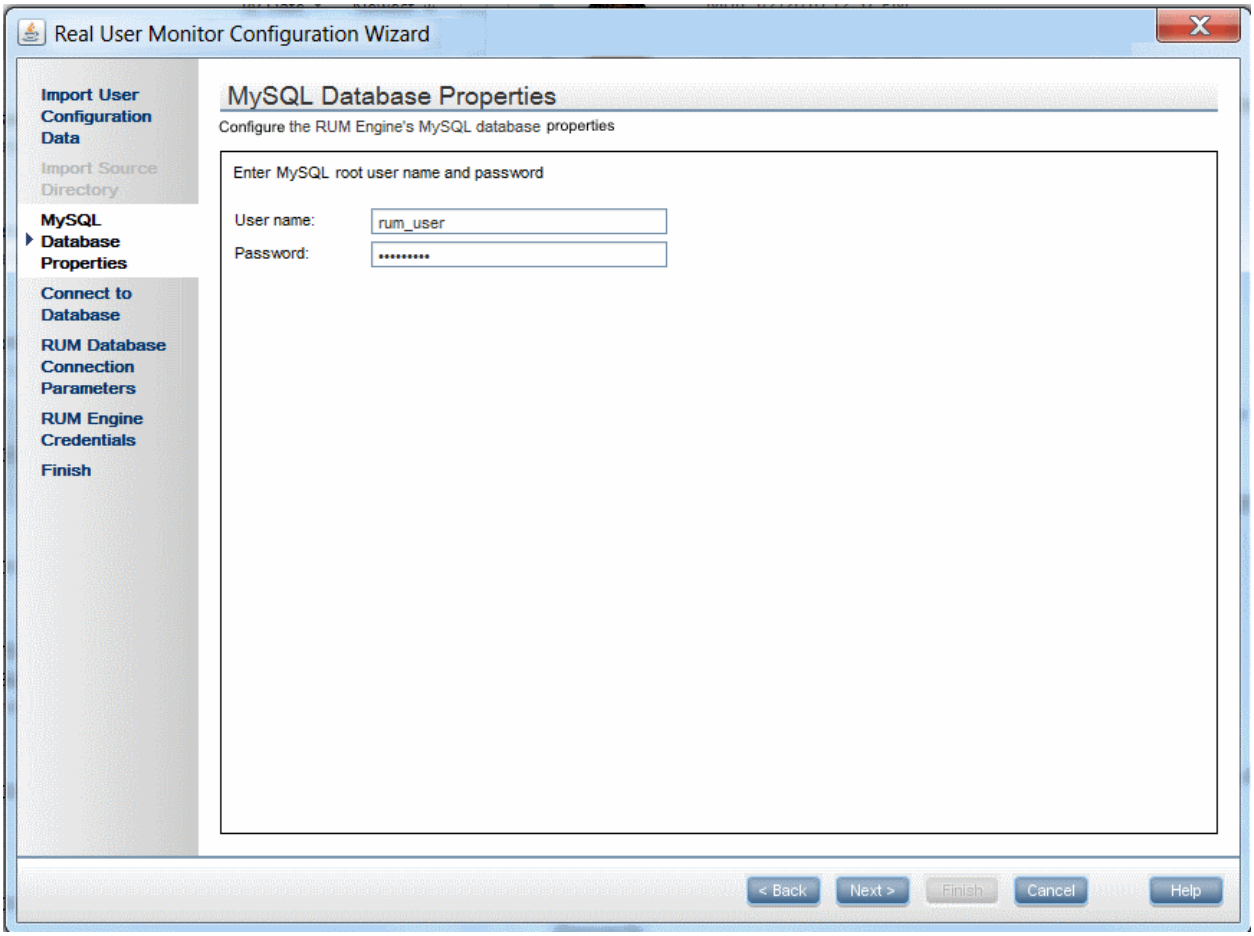
UI Element	Description
<Source directory>	Enter the source directory from which user configuration data will be imported. You can click **Browse** to locate and select a directory. **Note:** Importing data from an earlier version of RUM as part of an upgrade only changes the database structure, but does not copy old data. New, empty tables with the new database structure are created and the old tables are renamed by appending **_old** to their name. A warning about this is displayed when relevant. For details on copying the data from the old tables to the new ones, see "Upgrading Database Data" on page 83.

If you are installing the MySQL database in a distributed installation (that is, a system in which the engine and database are installed on separate machines), the Configuration Wizard continues with the next step. Otherwise, it continues with the Finish page (for details, see "Finish Page" on page 31).

MySQL Database Properties Page (Import Settings from Previous Distributed Installation)

This page enables you to configure the user name and password for accessing the database, if you import user data settings from a previous RUM installation when installing the MySQL database in a distributed installation (that is, a system in which the engine and the database are installed on separate machines). This is part of the RUM Configuration wizard; refer to "RUM Configuration Wizard" on page 20 for general information.

The following is an example of the MySQL Database Properties page, if you import user data settings from a previous RUM installation when installing the MySQL database in a distributed installation (that is, a system in which the engine and the database are installed on separate machines).



The following elements are included:

UI Element	Description
User name	The user name for accessing the MySQL database.
Password	The password for accessing the MySQL database.

Note: Enter the same user name and password that was used when the database was created. This enables APM to connect to the database after importing data from version 9.x to the latest version.

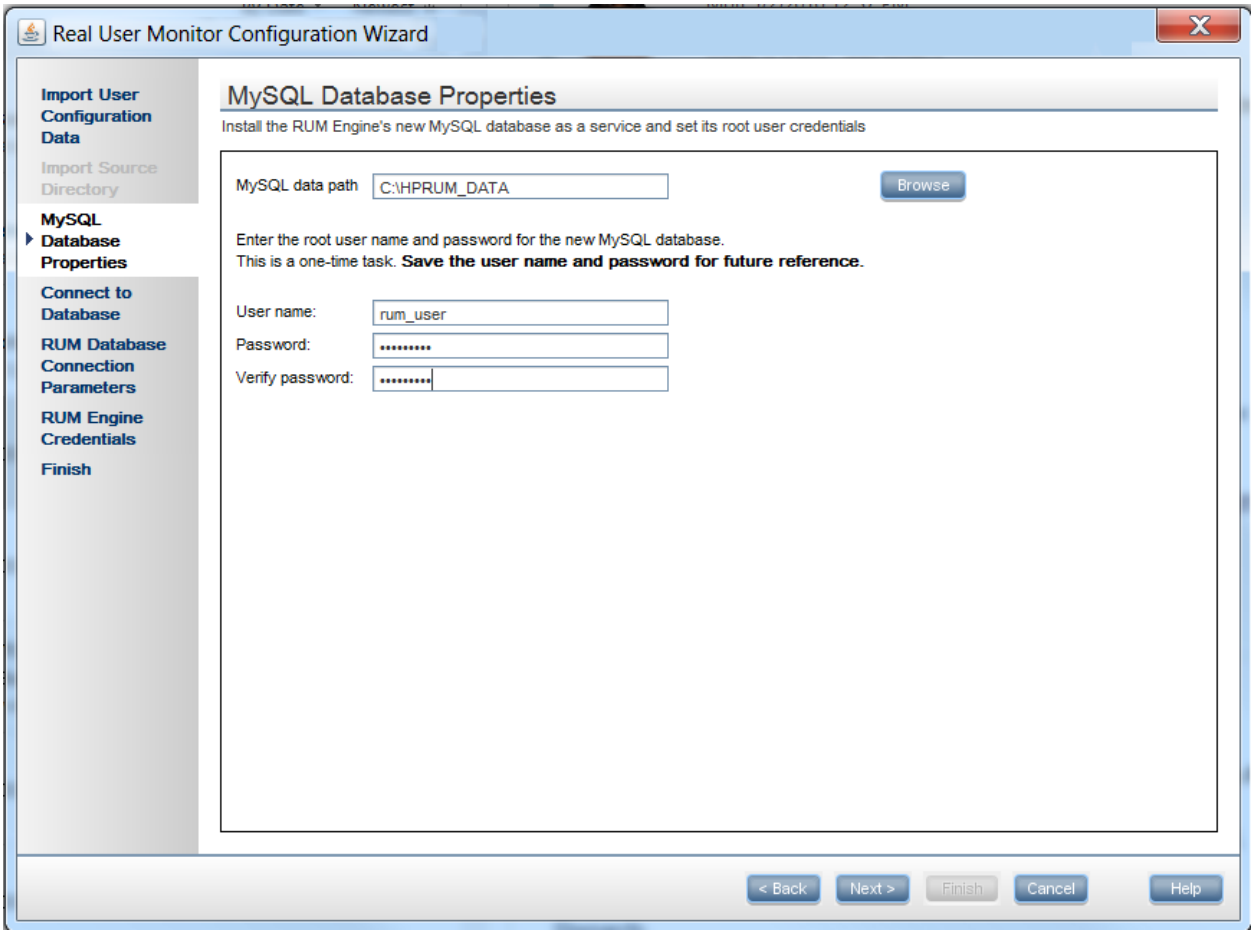
The Configuration Wizard continues with the Finish page. For details, see "Finish Page" on page 31.

MySQL Database Properties Page

This page enables you to configure the path in which the MySQL database data files are placed, as well as the user name and password for accessing the database. This is part of the RUM Configuration wizard; refer to "RUM Configuration Wizard" on page 20 for general information.

Important Information	• 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.

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



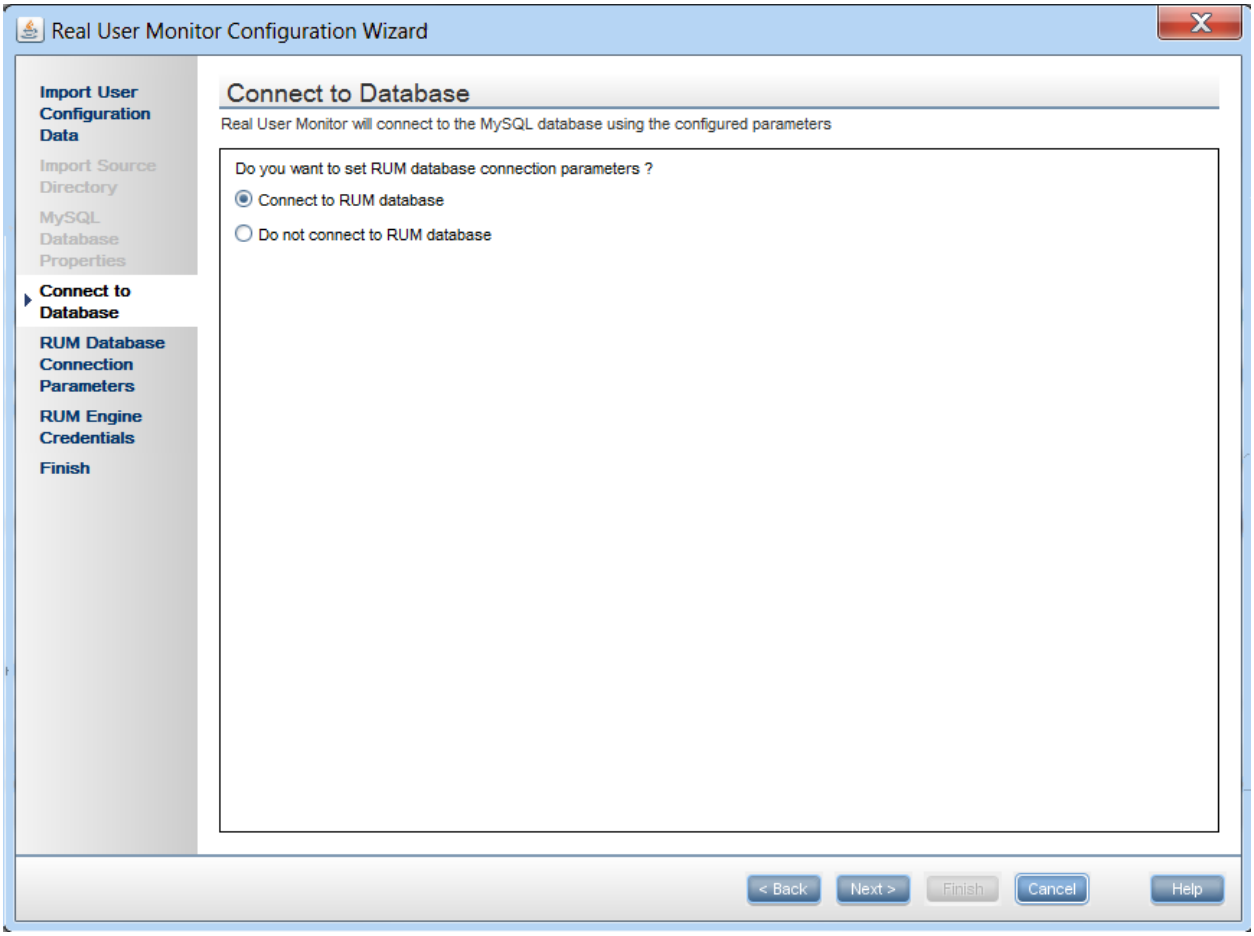
The following elements are included:

UI Element	Description
MySQL data 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. • If you enter an existing path, RUM uses the data in this directory and does not construct a new schema. • We recommend that you exclude this directory from anti-virus software scanning.
User name	The user name for accessing the MySQL database.
Password	The password for accessing the MySQL database.
Verify password	Retype the password for verification.

Connect to Database Page

This page enables you to configure whether to connect the RUM Engine to a MySQL database. This is part of the RUM Configuration wizard; refer to "RUM Configuration Wizard" on page 20 for general information.

The following is an example of the Connect to Database page:



The following elements are included:

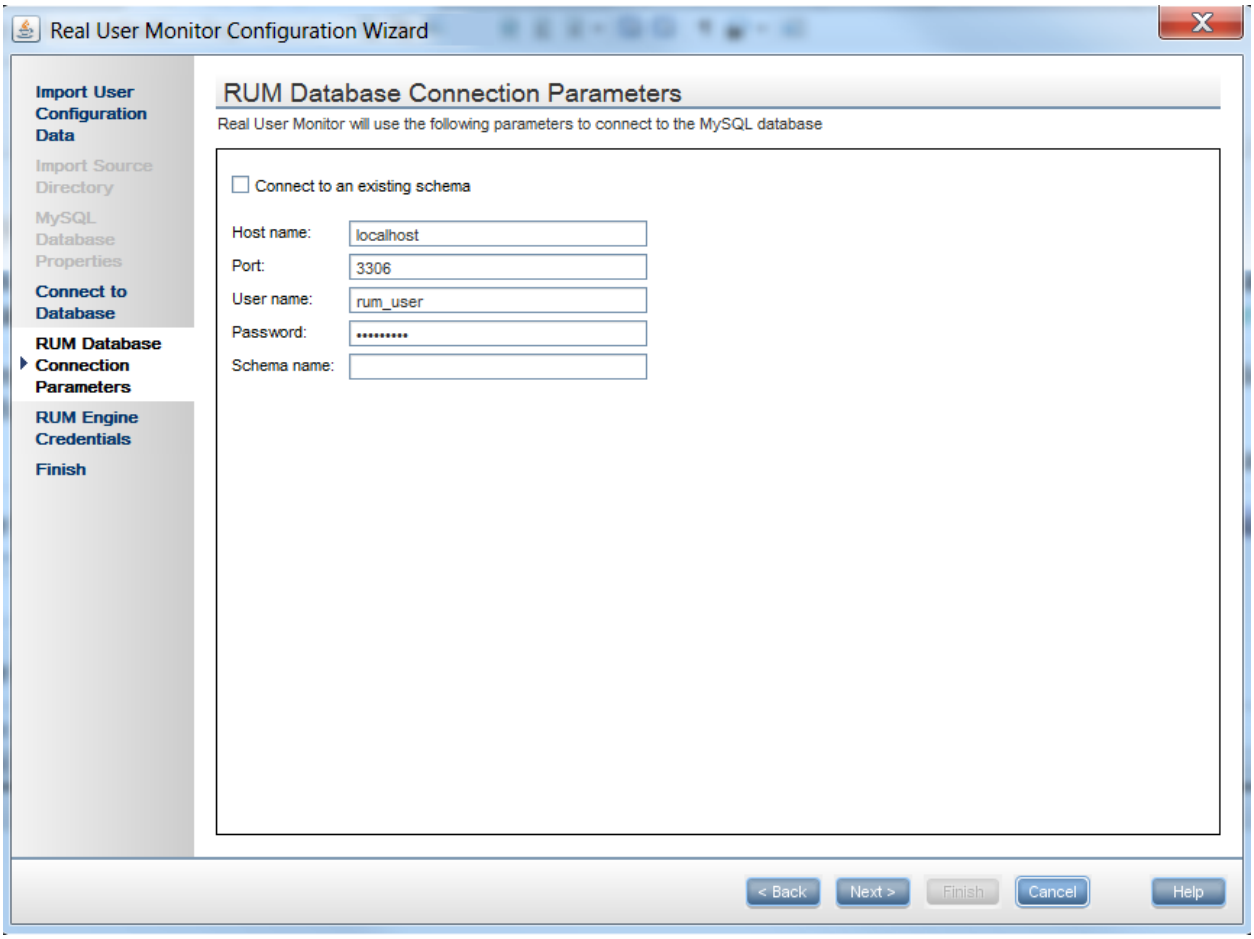
UI Element	Description
Connect to RUM database	Select this radio button to configure connection parameters and connect the RUM Engine to a MySQL database.
Do not connect to RUM database	Select this radio button if you do not want to connect the RUM Engine to a MySQL database. **Note:** • If you select this option, the wizard continues with the "RUM Engine Credentials Page" on page 29. • You can connect to a MySQL database, or change an existing connection, after installing RUM, by running the RUM Configuration wizard (open **Configuration Tool** on the computer's Start menu).

RUM Database Connection Parameters Page

This page enables you to configure the parameters used by the RUM Engine to connect to its MySQL database. This is part of the RUM Configuration wizard; refer to "RUM Configuration Wizard" on page 20 for

general information.

The following is an example of the RUM Database Connection Parameters 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. • If you connect to a schema from an earlier RUM version, RUM automatically upgrades the schema so that it is compatible with the current version.
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

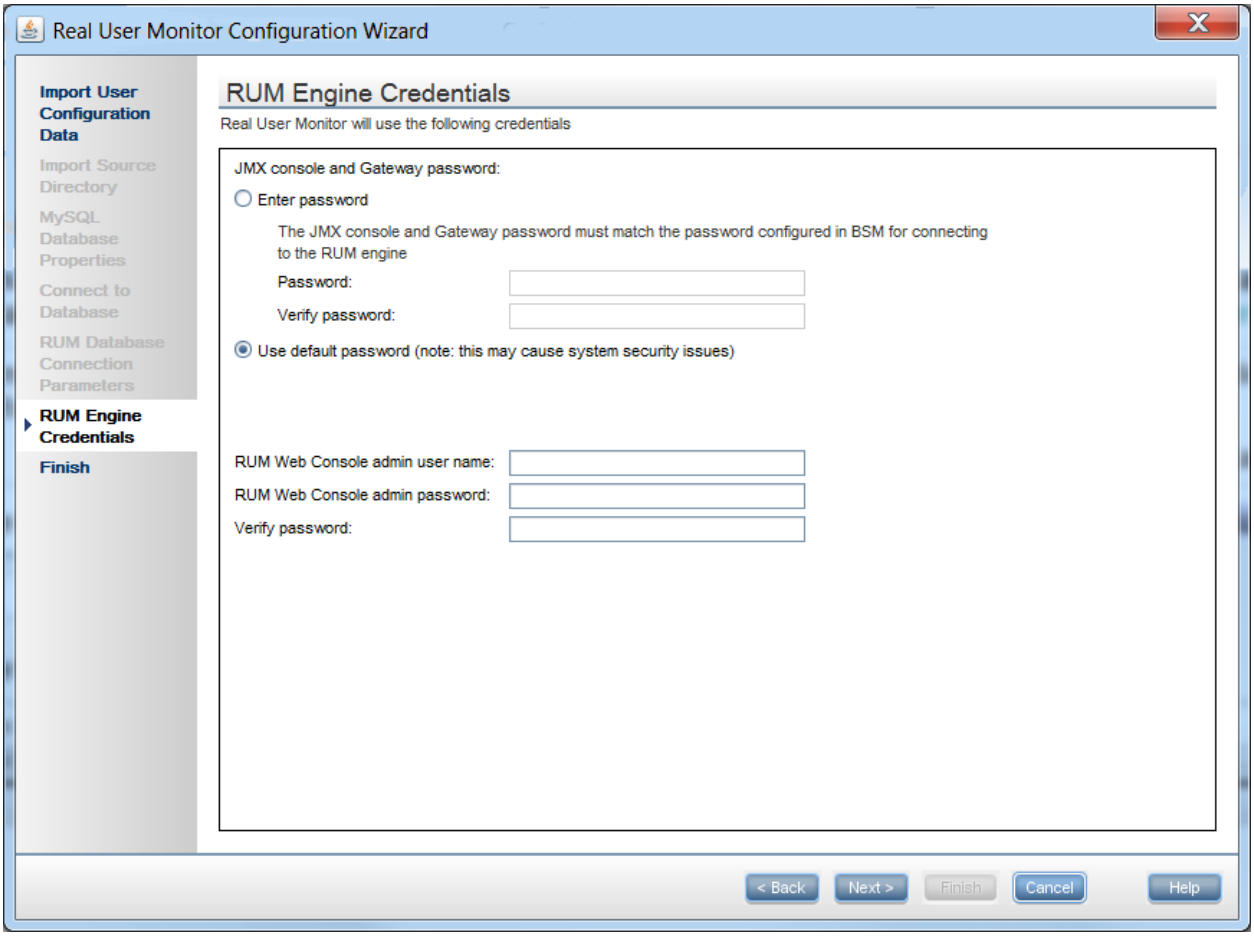
UI Element	Description
User name	The configured user name for connecting to the MySQL database. This must match the user name that you configured as part of the database parameters in the "MySQL Database Properties Page" on page 25.
Password	The configured password for connecting to the MySQL database. This must match the password that you configured as part of the database parameters in the "MySQL Database Properties Page" on page 25.
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 only valid special character is an underscore (_). • The name cannot end with a space.

RUM Engine Credentials Page

This page enables you to configure the credentials for the RUM JMX interface and the RUM web console. This is part of the RUM Configuration wizard; refer to "RUM Configuration Wizard" on page 20 for general information.

Note: If you imported user data settings from a previous RUM installation, this wizard page is not accessed.

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



The following elements are included:

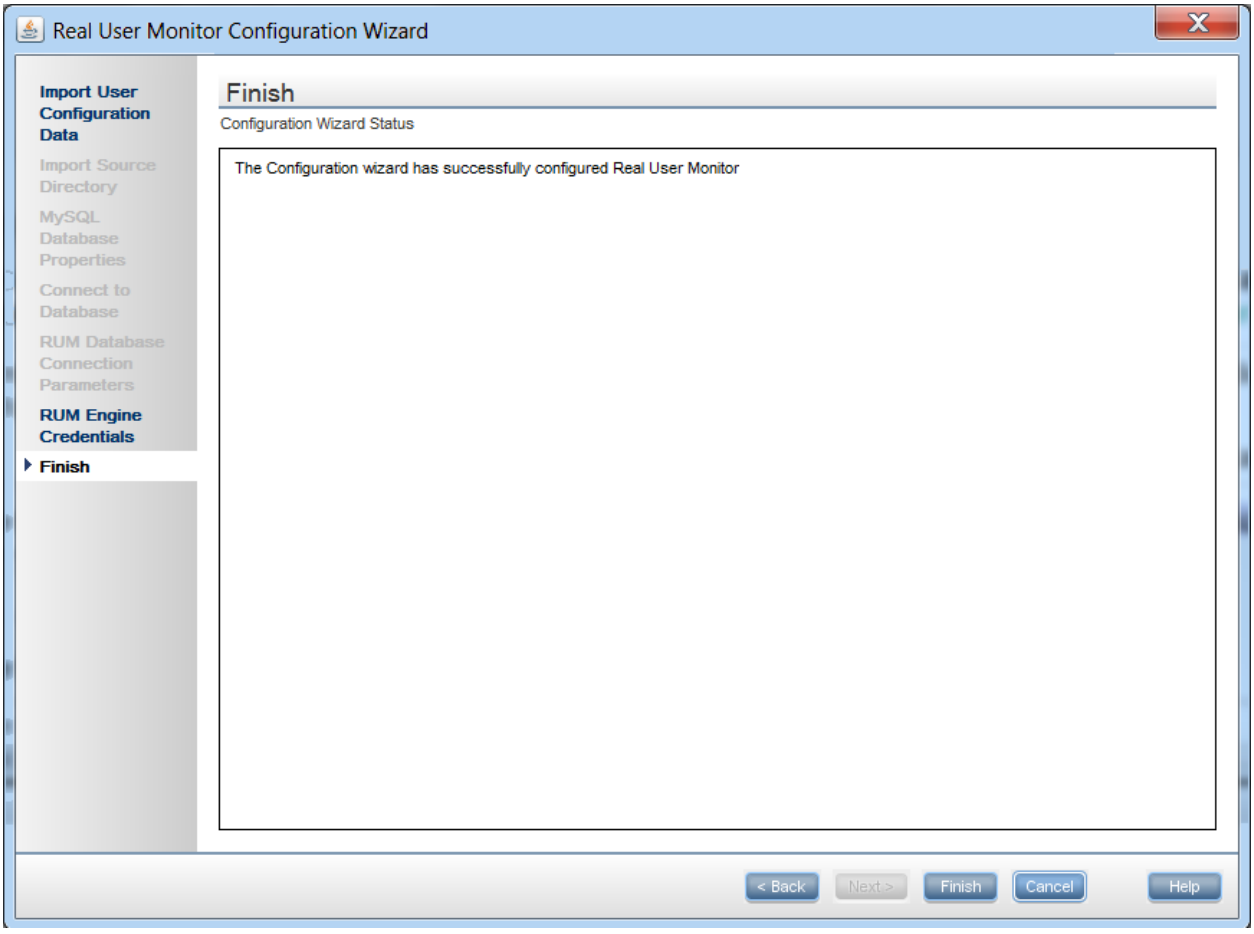
UI Element	Description
JMX console and Gateway Password	The password for the JMX console and APM Gateway user. • **Enter password:** Select this radio button to enter a password of choice. • **Use default password:** Select this radio button to use the default password (admin). **Note:** The JMX console and Gateway password must match the password configured for the RUM Engine connection settings in End User Management Administration in APM. If they do not match, APM 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 the APM Application Administration Guide.
RUM Web Console admin user name	The user name you use for accessing the RUM web console.

UI Element	Description
RUM Web Console admin password	The password for the RUM web console user.
Verify password	Retype the password (JMX console and Gateway user password, or RUM web console password) for verification.

Finish Page

This page displays a message showing the status of the Configuration wizard. Click **Finish** to exit and return to the RUM Setup wizard. This is part of the RUM Configuration wizard; refer to "RUM Configuration Wizard" on page 20 for general information.

The following is an example of the Finish page:



Installing RUM on Windows Server 2008 R2 Using Windows Remote Desktop

If you try to install the RUM Engine and/or MySQL database on Windows Server 2008 R2 using Windows Remote Desktop, the installation may not run and an error message is displayed. In such cases, you must first install Terminal Server Role Service on the remote machine on which you want to install engine or database and then carry out the installation using the Terminal Server.

This section includes the following topics:

- "To install the Terminal Server Role Service" below
- "To install RUM using Terminal Server" on the next page

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**.

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 **Server 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 RUM using Terminal Server

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

Follow the installation process as described in "How to Install the RUM Engine" on page 17.

Running a Silent Installation

You can use a silent installation procedure to run the 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" below
- "Prerequisites" on the next page
- "Silent Installation for Windows" on the next page
- "Configuring the RUMInstallationDefaults.properties File" on the next page

How a Silent Installation Assigns Values

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

- **<temp directory>\ovinstallparams.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.
- **<temp directory>\RUMInstallationDefaults.properties.** This file contains the parameter values used by the RUM Configuration wizard (for details, see "RUM Configuration Wizard" on page 20).

The installation process copies this file to the **<RUM installation directory>\bin directory**. (The default RUM installation directory is **C:\RUM**.) 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" below.

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 RUM" on page 65.
- 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 machine's temp directory or the **<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" below.

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 RUM Engine" on page 17.
2. When the Real User Monitor Configuration wizard opens, click **Cancel** and then quit the RUM installation.
3. Copy the **\RUM\bin\RUMInstallationDefaults.properties** file to the location of your choice.
4. Uninstall RUM. For details, see "Uninstalling RUM" on page 65.
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:

   ```
   Rum_<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 RUM 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 the previous page.

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.	
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.	
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.	
webConsolePassword	The password for the RUM web console user.	

Parameter	Description	Default Value
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, APM 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 the APM Application Administration Guide.	
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.	

Chapter 4: Installing the RUM Sniffer Probe

After installing the RUM Engine, you must install at least one RUM Probe. You must then set up the probe to collect real-user data and report this data to the engine.

This section describes the installation of the RUM Sniffer Probe. For details on installing a RUM Client Monitor Probe, see "Installing the RUM Client Monitor Probe" on page 47.

Note:

- Before beginning the installation, review the information in the RUM Release Notes PDF (rum_readme_<version number>.pdf) for any last minute notes and limitations, as well as for upgrade and service pack install instructions.
- For production systems, you must install the RUM Engine, Probe, and database on separate physical disks.
- For details on installing and working with a probe on a VMware platform, see "Duplicating Traffic for Real User Monitor with VMware" in the Real User Monitor Administration Guide.
- Before installing RUM Probe on a Linux machine, either disable it or make sure that SELinux will not block it.

  To disable SELinux:

  a. Open the **/etc/selinux/config** file

  b. Set **SELINUX=disabled**.

  c. Reboot the machine.

This section includes:

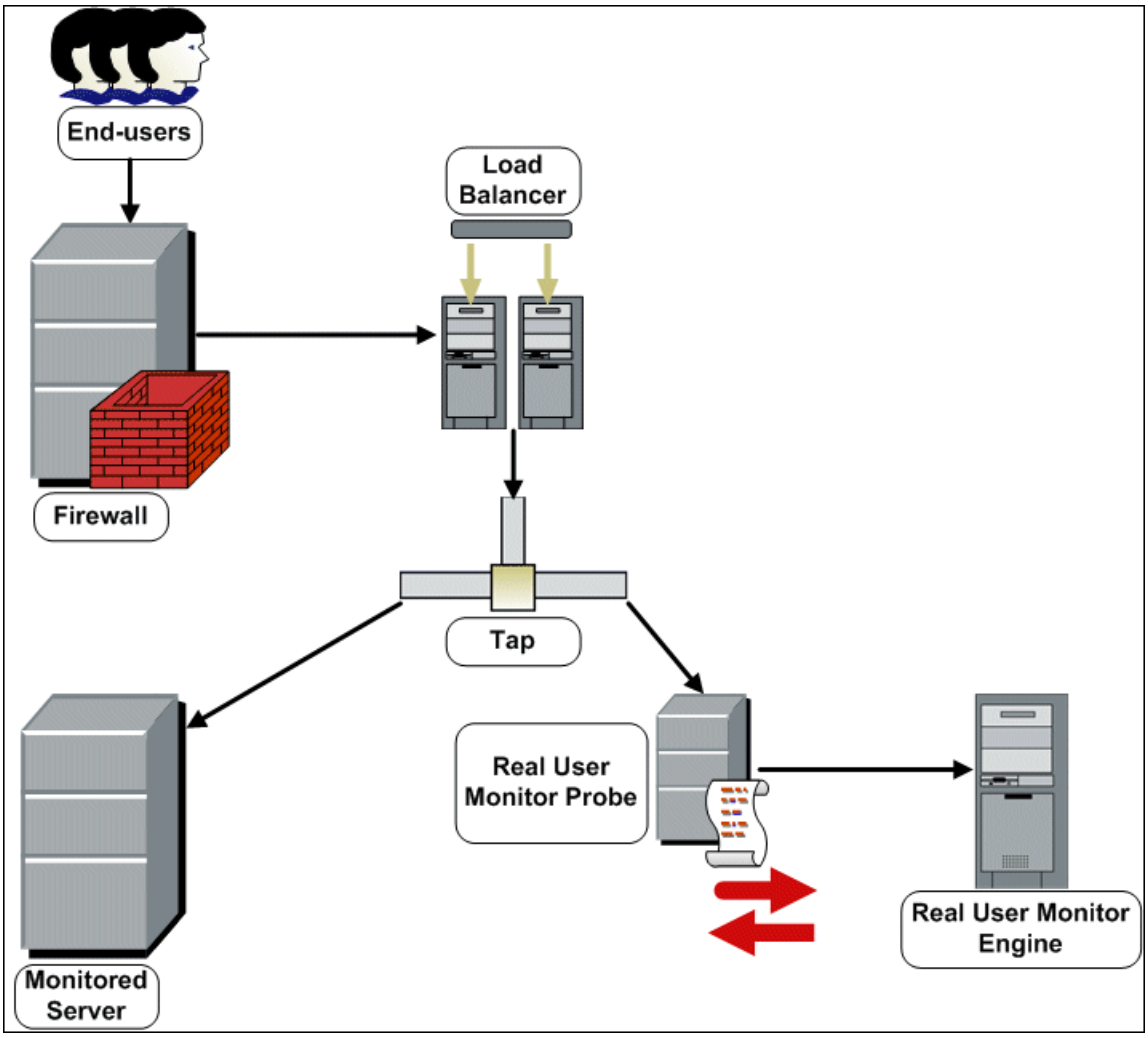
- "Physically Connecting the Probe" below
- "How to Install the RUM Sniffer Probe" on the next page
- "Running a Silent Installation" on page 41
- "Stopping and Starting the Probe" on page 42
- "Connecting the Probe to the RUM Engine" on page 42
- "Installing an nCipher Card on the RUM Probe" on page 42

Physically Connecting the Probe

This section describes how to physically connect the RUM Probe to the network.

The RUM 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 RUM Engine uses to connect to the probe machine). It is recommended that the network interface used for sniffing should not have an IP address assigned to it. IP addresses are usually used for sending and receiving data and therefore it can lead to confusion between sniffed traffic and the IP address traffic. For details on the system requirements for the RUM Probe, see "RUM Sniffer Probe Requirements" on page 9.

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-forwarded-for** header to preserve end-user IP addresses for use by RUM.
- For small installations with a low amount of network traffic, instead of using a network tap, an Ethernet port of the RUM Probe can be connected to a switch that is configured for port mirroring for the monitored server.

How to Install the RUM Sniffer Probe

This section describes how to install the probe.

The RUM Probe is installed on a machine running either the Linux or Windows operating system. For details on the system requirements for the RUM Probe, see "RUM Sniffer Probe Requirements" on page 9.

Tip: For better performance, it is recommended to install the RUM Engine and the RUM Probe on the same local area network (LAN).

This section includes the following topics:

- "The RUM Probe Setup File" below
- "Installing the RUM Probe on a Linux System" below
- "Installing the RUM Probe on a Windows System" on the next page

The RUM Probe Setup File

The RUM Probe setup file can be accessed from one of the following locations:

- The RUM installation package.
- The Software Support Online web site (https://softwaresupport.softwaregrp.com/). Sign in using your Passport user name and password. Click **Manuals**. Under Document Type, select **Patches**. In the Search field, enter **RUM Probe Setup File**.
- The Downloads page in APM Platform Administration. For details, see the APM Platform Administration Guide.

  Note: There may be more recent versions of RUM than the version included in the APM Downloads page. For details, check the Software Support Online web site (https://softwaresupport.softwaregrp.com/).

There are different versions of the RUM Probe setup file for Windows and Linux. The name of the setup file reflects the applicable operating system.

Examples:

- **HPRUMProbe_<version number>_linux64.bin** is the Probe setup file for a Linux 64 bit operating system.
- **HPRUMProbe_<version number>_win64_setup.exe** is the Probe setup file for a Windows 64 bit operating system.

Installing the RUM Probe on a Linux System

Note: The RUM Probe installation must be carried out as the root user.

To install the RUM Probe:

1. Save the RUM Probe setup folder for Linux to the **/var/tmp** directory on the machine on which you want to install the probe. Note that if you cannot save this file directly on the Linux machine on which you are installing the probe, make sure that you save it on a machine from which you can later FTP (in binary mode) the file to the Linux machine. For details on the location of the setup file, see "The RUM Probe Setup File" above.
2. Run the installation script with the following commands:
   - **cd /var/tmp**
   - **chmod 777 <Probe setup file name>**
     For example: **chmod 777 HPRUMProbe_v<version number>_linux64.bin**
   - **<Probe setup file name>**
     For example: **HPRUMProbe_v<version number>_linux64.bin**

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

<Probe setup file name> --prefix=/<full path name>/

3. Start the RUM Probe with the command
   /etc/init.d/rum_probe-capture start.
4. Verify that the RUM 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 RUM Probe on a Windows System

Note:

- The RUM Probe installation must be carried out as an administrator.
- The Windows local system must be enabled to run services. (By default, it is enabled.)
- SSL keystore files from previous probe installations that are located in **<Real User Monitor probe root directory>\etc\rum_probe\keystore**, are retained.

For details on the system requirements for installing the RUM Probe, see "RUM Sniffer Probe Requirements" on page 9.

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 probe:

1. Save the RUM Probe setup folder for Windows on the machine on which you are installing the RUM Probe. For details on the location of the RUM Probe setup file, see"The RUM Probe Setup File" on the previous page.
2. On this machine, navigate to the downloaded file and double click **HPRUMProbe_<version number>_win64_setup.exe**.
3. When prompted, select the installation language (default English) and click **OK**. The RUM Probe 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 the path of the folder in which you want to install the RUM probe. Either accept the default path (**C:\HPRumProbe**), 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.
   - If you have saved SSL keystore files from a previous installation, select the same path as the previous installation.

7. The Setup wizard verifies that you have enough free disk space for the installation. If this check fails, go back and free up more disk space before continuing with the installation.
8. 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.

9. The installation begins and its progress is displayed. You can choose whether to view summary or detailed progress data, by clicking the appropriate tab.
10. The status of the RUM Probe 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.
11. Click **Done** to exit the Setup wizard.
12. Start the RUM Probe.
13. If you are installing the RUM Probe on Windows Server 2008 R2:
    a. Open **Windows Services** (In My Computer, right-click Manage and select Configuration > Services)
    b. Edit the properties of **RUM Probe Service**
    c. In the **Log on** tab select **This account**
    d. Set an administrator user
    e. Apply the changes

Running a Silent Installation

You can use a silent installation procedure to run the RUM Probe setup for Windows. A silent installation is an installation that is performed automatically, without the need for user interaction. Instead, all configuration parameters are allocated predetermined, default values.

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.

Prerequisites

- The RUM Probe installation must be carried out as an administrator.
- The Windows local system must be enabled to run services. (By default, it is enabled.)
- **%temp%** must be a valid directory on the machine on which you are running the silent installation.
- For details on the system requirements for installing the RUM Probe, see "RUM Sniffer Probe Requirements" on page 9.

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

Silent Installation for Windows

Caution: If a previous installation of the RUM Probe already exists on the machine, the silent installation automatically runs in **uninstall** mode and removes the previous installation.

To run a silent installation:

1. Save the RUM Probe setup folder for Windows on the machine on which you are installing the RUM Probe. For details on the location of the RUM Probe Setup file, see "The RUM Probe Setup File" on page 39.
2. On this machine, run the following command:

```
start /wait <the RUM probe setup.exe file as downloaded in step 1>
-DSKIPALL=true -i silent
```

Stopping and Starting the Probe

The RUM Probe is started automatically each time the machine on which it is installed is started. You can also manually start and stop the RUM Probe.

To start the RUM Probe manually on a Linux machine:

1. Log on to the RUM Probe machine as the root user.
2. Start the RUM Probe with the command **/etc/init.d/rum_probe-capture start**.

To start the RUM Probe manually on a Windows machine:

Execute **Enable RUMProbe** on the computer's Start menu.

To stop the RUM Probe manually on a Linux machine:

1. Log on to the RUM Probe machine as the root user.
2. Stop the RUM Probe with the command **/etc/init.d/rum_probe-capture stop**.

To stop the RUM Probe manually on a Windows machine:

Execute **Disable RUMProbe** on the computer's Start menu.

Connecting the Probe to the RUM Engine

After you have installed and started the RUM Probe, you must connect it to a RUM Engine. You configure the connection using **Probe Management** in the RUM Engine web console. For details, see "Probe Management" in the Real User Monitor Administration Guide.

Installing an nCipher Card on the RUM Probe

Note: This section applies to the RUM Probe only when it is installed on a Linux system.

You can install an nCipher card on the RUM 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:

- "Recommendations for Uploading Keys to an nCipher Probe" below
- "Customizing RUM" below
- "Troubleshooting" on page 44

Recommendations for Uploading Keys to an nCipher Probe

It is recommended to load the application server keys to the nCipher module (the PCI card) without a password.

The keys must be loaded with application embed (openSSL option in kSafe).

Customizing RUM

To customize RUM to work with the nCipher card, you must configure both the RUM Engine and Probe machines and send the updated engine configuration to the probe.

To configure the RUM Engine machine:

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

   In the **static_global_params** section, under the global heading, 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>
   ```

2. Add the PEM file created by nCipher to the keystore. For details see, "SSL Keystore Management" in the Real User Monitor Administration Guide.

To configure the RUM Probe machine:

1. Edit the **/usr/bin/rp_run_probe.sh** file.

   Change the environment variable definition for **NFAST_HOME** to:

   export NFAST_HOME=/opt/nfast

   Note: /opt/nfast is the default location of the nCipher installation. If you install nCipher in a different path, use the relevant path in the export command.

2. If application server keys were not previously loaded to the nCipher module (the PCI card), edit the **/usr/bin/rp_run_probe.sh** file and modify the following line:

   From: `${BEATBOX_ROOT}/bin/HPRUMProbe -D`

   To: `${NFAST_HOME}/bin/preload <nCipher parameters>`
   `${BEATBOX_ROOT}/bin/HPRUMProbe -D`

   Note:

   - If the preload command requires you to enter a password, the RUM Probe cannot run as a service. Running the RUM Probe not as a service is not supported.
   - Consult your nCipher administrator for the parameters to add to the preload command.

3. Restart the probe with the following command:

   /etc/init.d/rum_probe-capture restart

To send the updated RUM Engine configuration to the RUM Probe:

Force an update of the RUM Probe configuration by accessing the RUM Engine web console and selecting **Tools > Monitoring Configuration Information > Sync All Configuration**. For details on working with the RUM Engine web console, see "Using the Real User Monitor Web Console" in the Real User Monitor Administration Guide.

Troubleshooting

The probe is unable to decrypt traffic

If the probe is unable to decrypt traffic, verify if the problem is in the probe by installing the Apache Web Server and trying to connect it to the nCipher card. (The Apache Web Server connects to the nCipher card in the same way as the probe.) For details on integrating the nCipher components with the Apache Web Server installation on the RUM Probe, refer to the Integration Guide for Apache HTTP Server on the **nCipher** web site.

Check security world status

You can use the following commands to check the security world status:

- Check the status of the nCipher module (the PCI card): **/opt/nfast/bin/enquiry**
- Check if there are nCipher cards in the security world: **/opt/nfast/bin/nfkminfo –c**
- Check which keys are loaded in the security world: **/opt/nfast/bin/nfkminfo –l**

Installation of SSL key Agent for Apache web server

Prerequisites

- Perl must be installed with the following libraries:
  - LWP::UserAgent
  - URI::URL
- Python (an interpreted, interactive, object-oriented programming language)
- gcc

The RPM file for the SSL Key agent for Apache is included in **rp_sslKeyPlugin.tgz.** This can be accessed from the RUM installation package.

Run the following command to extract the file : **tar -xvf rp_sslkeyPlugin.tgz**

```
[root          depot]# tar -xvf rp_sslKeyPlugin.tgz
rp_sslKeyPlugin/
rp_sslKeyPlugin/rp_ssl_agent_plugin-9.51-0113.x86_64.rpm
[root          depot]#
```

By default installation of the agent goes under the (/) directory. Alternatively, you can install in the custom path:

rpm -ivh --prefix=/opt/ rp_ssl_agent_plugin-9.51-0082.x86_64.rpm

The above step will install a plug-in in **/opt/** directory.

```
[root          install]# cd rp_sslKeyPlugin
[root          rp_sslKeyPlugin]# rpm -ivh --prefix=/opt rp_ssl_agent_plugin-9.51-0114.x86_64.rpm
Preparing...                ########################################### [100%]
   1:rp_ssl_agent_plugin    ########################################### [100%]
[root          rp_sslKeyPlugin]#
```

Configuration of Apache Agent

Perform the below steps to configure the agent plug-in:

1. Locate the plug in install directory. In this case it is under **/opt.**
2. Execute the following command: **./rp_sslKeyLoggerConfig.sh –install**
   You will be prompted with questions to confirm the port number and Apache agent as shown below:

```
[root        rp_sslKeyPlugin]# cd /opt/rp_sslKeyPlugin/plugin/config/
[root        config]# ./rp_sslKeyLoggerConfig.sh --install
HTTPD_ROOT=/etc/httpd
In Plugin generation.....
LIB_SSL_PATH=/usr/lib64/libssl.so.10
is_api=
ssl_ver=libssl_so_1_0_1e
ssl_ver=libssl_so_1_0_1
sslKeyLoggerGenerator.....

Found the plugin at /opt/rp_sslKeyPlugin/plugin/modules

By default RUM-Plugin shares SSL keys with the Rum-Agent over tcp port 3003. Do you want to provide a custom port [Y/N]?N

The script will now update/create the configuration file with environmenmt variables required to invoke the plugin.
The file /etc/sysconfig/httpd will be updated so that plugin.conf will get sourced when the httpd service is started next time.
The file ssl.conf will be updated so that RUM wrapper for httpd's mod_ssl.so gets loaded when the httpd service is started next time.
This will enable sharing of SSL session keys with the RumProbe Agent.
A copy of the original version of the files /etc/sysconfig/httpd and ssl.conf will be saved at /opt/rp_sslKeyPlugin/plugin/config/backup

Do you want to continue [Y/N]?Y
The httpd service must be restarted for the Plugin to get loaded. Do you want to restart now [Y/N]?Y
setenforce: SELinux is disabled
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
[root        config]#
```

3. Modify the **agent.conf** file for providing the IP address of the probe server.

```
[root        config]# cd /opt/rp_sslKeyPlugin/agent/etc/rum_agent/
[roo         rum_agent]# vi agent.conf
```

```
[general]
# Address the daemon has to bind to
# Default: it binds to 127.0.0.1.
address=127.0.0.1

# Port the daemon has to bind to. Default: 3003.
port=3003
session_key_buf_size=8192

#probe=IP/FQDN port

#ssl_probe=IP/FQDN port
ssl_probe=192.168.5.11 2020

[security]
# Use SSL manage/data connections. If set - this will violate backward
#use_ssl=FALSE|true
use_ssl=false

# optional client authentication
ssl_ca_file=/etc/rum_agent/rum-probe-ca.crt

# mandatory server key/certificate.
# the certificate must be signed by a CA to pass optional server authentication on client
ssl_key=/etc/rum_agent/rum-probe-server.key
ssl_cert=/etc/rum_agent/rum-probe-server.crt
```

4. After modifying the **agent.conf**, run the following command to start the agent:

./etc/init.d/rum_ssl-agent start

Chapter 5: Installing the RUM Client Monitor Probe

After installing the RUM Engine, you must install at least one RUM Probe. You must then set up the probe to collect real-user data and report this data to the engine.

This section describes the installation of the RUM Client Monitor Probe. For details on installing a RUM Sniffer Probe, see "Installing the RUM Sniffer Probe" on page 37.

Note:

- For production systems, you must install the RUM Engine, Probe, and database on separate physical disks.
- Before beginning the installation, review the information in the RUM Release Notes for any last minute notes and limitations, as well as for upgrade and service pack install instructions.

The RUM Client Monitor Probe is installed on a machine running the Windows operating system. For details on the system requirements for the RUM Client Monitor Probe, see "RUM Client Monitor Probe Requirements" on page 12.

Tip: For better performance, it is recommended to install the RUM Engine and the RUM Client Monitor Probe on the same local area network (LAN).

This section includes:

- "The RUM Client Monitor Probe Setup File" below
- "How to Install the RUM Client Monitor Probe" on the next page
- "Stopping and Starting the Probe" on page 42
- "The RUM Client Monitor Probe Setup File" below
- "Installing the JavaScript Snippet" on page 49
- "Instrumenting Mobile Applications for Android" on page 52
- "Instrumenting Mobile Applications for iOS" on page 58
- "Monitoring Hybrid Applications" on page 60

The RUM Client Monitor Probe Setup File

The RUM Client Monitor Probe setup file can be accessed from one of the following locations:

- The RUM installation package.
- The Software Support Online web site (https://softwaresupport.softwaregrp.com/). Sign in using your Passport user name and password. Click **Manuals**. Under Document Type, select **Patches**. In the Search field, enter **RUM Client Monitor Setup File**.
- The Downloads page in APM Platform Administration. For details, see the APM Platform Administration Guide.

  Note: There may be more recent versions of RUM than the version included in the APM Downloads

page. For details, check the Software Support Online web site (https://softwaresupport.softwaregrp.com/).

How to Install the RUM Client Monitor Probe

Note:

- The RUM Client Monitor Probe installation must be carried out by an administrator.
- The Windows local system must be enabled to run services. (By default, it is enabled.)

For details on the system requirements for installing the RUM Client Monitor Probe, see "RUM Client Monitor Probe Requirements" on page 12.

Tip: For better performance, we recommend installing the RUM Engine and the RUM Client Monitor Probe on the same local area network (LAN).

To install the RUM Client Monitor Probe:

1. Save the RUM Client Monitor Probe setup folder for Windows on the machine on which you are installing the probe. For details on the location of the RUM Client Monitor Probe setup file, see "The RUM Client Monitor Probe Setup File" on the previous page.
2. On this machine, navigate to the downloaded setup file (**RUMClientMonitorProbe<version number>_setup.exe**) and double-click it.
3. When prompted, select the installation language (default English) and click **OK**. The RUM Client Monitor Probe Setup wizard begins.
4. When the Introduction page is displayed, click **Next**.
5. Accept the terms of the license agreement and click **Next**.
6. The features to be installed are displayed (by default, all features are selected). Click **Next**.
7. Select the path of the folder in which you want to install the RUM Client Monitor Probe. Either accept the default path (C:\RUMClientMonitorProbe), 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 installation path.

8. The Setup wizard performs a number of system checks (free disk space, previous installations, and port availability). If any of these checks fails, go back and make the necessary changes before continuing with the installation.
9. 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.
10. The installation begins and its progress is displayed. You can choose whether to view summary or detailed progress data, by clicking the appropriate tab.
11. The status of the RUM Client Monitor Probe 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.
12. Click **Done** to exit the Setup wizard.

    The RUM Client Monitor Probe starts automatically when the installation is completed.

After installing the RUM Client Monitor Probe and opening it to the network to be accessed by the end user mobile devices and browsers in order to send data, try to access the probe's data URLs: `http://<cm_probe_`

server>:<cm_probe_port>/hpmobilemon/data/ and http://<cm_probe_server>:<cm_probe_port>/hpclientmon/data/ (for example: **http://clientmonitor.mycompany.com:8080/hpmobilemon/data/**). If you get a 405 error, it indicates that end user devices can correctly access the probe to send it data.

Stopping and Starting the RUM Client Monitor Probe

The RUM Client Monitor Probe is started automatically each time the machine on which it is installed is started. You can also manually start and stop the RUM Client Monitor Probe.

- **To start the RUM Client Monitor Probe manually on a Windows machine:**
  Open **Start RUM Client Monitor** from the computer's Start menu.
- **To stop the RUM Client Monitor Probe manually on a Windows machine:**
  Open **Stop RUM Client Monitor** from the computer's Start menu.

Connecting the RUM Client Monitor Probe to the RUM Engine

After you have installed and started the RUM Client Monitor Probe, you must connect it to a RUM Engine. You configure the connection using **Probe Management** in the RUM Engine web console. For details, see "Probe Management" in the Real User Monitor Administration Guide.

When you configure the connection between the RUM Engine and the RUM Client Monitor Probe, by default, the RUM Client Monitor Probe's port 2020 is used for the connection. If you change this port number when configuring the connection in the RUM Engine web console, you must update the new port number in the following files on the RUM Client Monitor Probe machine:

- **RUMClientMonitorProbe\apache-tomcat\conf\server.xml** (change port 2020 to the new port number)
- **C:\RUMClientMonitorProbe\conf\cm.properties** (change the value of the **enginePort** parameter to the new port number)

Installing the JavaScript Snippet

You use the RUM client monitor solution to enable the RUM Client Monitor Probe to acquire web application data through Internet browsers. This requires you to install a small JavaScript snippet in each of the specific HTML pages you want to monitor.

Tip: Multiple pages in a web site may share a common component. For example, the header part of pages may derive from the same source. In such instances, it may be possible to find a single location for the snippet that updates all the other pages you want to monitor.

The snippet must be added immediately after the **HEAD** opening tag of the page. The following is an example of the snippet:

```
<html>
    <head>
       <script type="text/javascript" src="/cm-app/clientmon.js"
id="id_cmMonitorJsEl"></script>
```

```
      <script type="text/javascript">
            cm_impl.init({ probeURL: “cm_probe_url“ });
      </script>
       ...
       ...
    </head>
     ...
     ...
</html>
```

The JavaScript snippet comprises two lines:

- The first line imports the RUM Client Monitor JavaScript file (clientmon.js). This file includes the code for performing the monitoring of the pages’s data and its components, and for sending the monitored data to the RUM Client Monitor Probe for processing and analysis.
- The second line sets the parameters (mandatory and optional) used by the JavaScript file. Parameters must be separated by a comma. The following table describes the valid parameters:

Parameter Name	Description	Mandatory/Optional
probeURL	The URL of the RUM Client Monitor Probe to which the monitored client data is sent. The format for the parameter is: **<protocol>://<host>:<port>/clientmon/data** **Note:** The value must be enclosed with quotation marks ("value"). **Example:** "http://probeHostName:8080/clientmon/data"	Mandatory
sProbeURL	The URL of the RUM Client Monitor Probe to which the monitored client data is sent, if using https. The format for the parameter is: **<protocol>://<host>:<port>/clientmon/data** **Note:** The value must be enclosed with quotation marks ("value") **Example:** "https://probeHostName:2021/clientmon/data"	If any of the application pages are (or may be) accessed using https, this parameter is mandatory.
Monitoring Parameters		
enableCbd	If set to **true**, collects component breakdown information for each page.	Optional
cmRespContLen	If specified, this parameter represents the total number of bytes sent in the entire response data, including SSL bytes.	Optional
cmReqContLen	If specified, this parameter represents the total number of bytes sent in the entire request data, including SSL bytes.	Optional
cmCPort	If specified, this parameter represents the port number on the client machine that sent the request.	Optional

Parameter Name	Description	Mandatory/Optional
cmCMethod	If specified, this parameter represents the HTTP request method used (for example: GET, POST, HEAD). **Note:** The value must be enclosed with quotation marks ("value").	Optional
cmUserName	If specified, this parameter represents the user name that activated the page. The user name is used in reports. The application owner should know how to extract the username from the page content. It is available as plain text, attribute, value, etc. In the "Setting a User Name" below example, the username is available inside the element with the ID **loginDataBar**, and is extracted using pattern matching. **Note:** The value must be enclosed with quotation marks ("value").	Optional
cmPageEvents	If specified, this parameter represents specific events that occurred on the page. **Note:** You configure a list of the required event IDs. To locate an event ID, in the RUM web console select **Tools > Monitoring Configuration Information > Events** and use the search box to locate an event by name.	Optional
Integration Parameters		
cmHpCamColor	If specified, this parameter represents the X-HP-CAM-COLOR header that is sent at the request. **Note:** The value must be enclosed with quotation marks ("value").	Optional
cmHpTvColor	If specified, this parameter represents the X-HP-TV-COLOR header that is sent at the request. **Note:** The value must be enclosed with quotation marks ("value").	Optional

You can also set the above parameters dynamically, using the **set_cm_value** method within JavaScript code. While you can do this for any of the parameters, the most common use cases are for dynamically setting user names and events. The following are examples of the scripts for such use cases.

Setting a User Name

```
<script>
    var username =  '-';
    var match = /Logged user: (.*) -
/g.exec(document.getElementById('loginDataBar').innerHTML);
    if(match.length > 0){
       username = match[1];
```

```
    }
    set_cm_value('cmUserName', username);
</script>
```

Setting an Event

Setting an event without extracting text:

```
<script>
   set_cm_value('cmPageEvents','event_id');
</script>
```

If several events are needed, their IDs must be separated with a comma:

```
<script>
   set_cm_value('cmPageEvents','event_id_1, event_id_2, event_id_3');
</script>
```

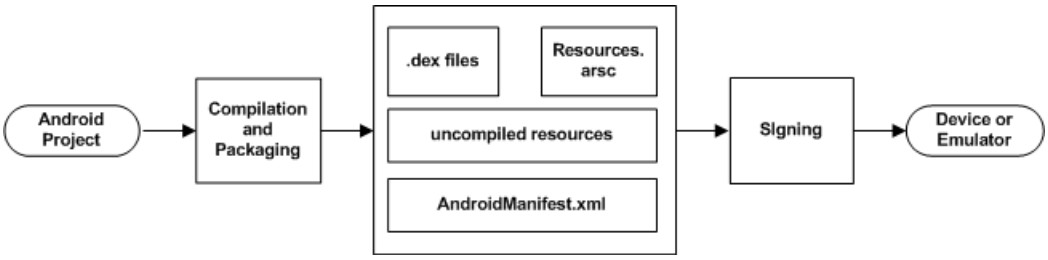
Setting an event extracting text:

```
<script>
    set_cm_value(’cmPageEvents’,’554{39$}’);
</script>
```

Instrumenting Mobile Applications for Android

You use the RUM mobile solution to enable the RUM Client Monitor Probe to acquire mobile application data through mobile devices. This requires you to instrument the mobile applications. This section describe how to instrument Android APKs. For details on instrumenting iOS apps, see "Instrumenting Mobile Applications for iOS" on page 58.

The following diagram shows the development flow of an Android application:



You use the ApkInfuser to instrument an APK. The instrumentation is made to the compiled Java classes in the APK and does not modify any source code, as it is done in the post-build stage.

You can instrument an APK using:

- The RUM web console. For details, see "Mobile Application Instrumentation" in the Real User Monitor Administration Guide.
- The **ApkInfuser.bat** file.

You run the ApkInfuser.bat file from a command line in the following format:

```
<RUM installation directory>\tools\ApkInfuser\ApkInfuser.bat <parameters> <path and name
of the APK  you are instrumenting>
```

You must specify the following parameters:

- **-u <Probe URL>.** The URL of the RUM Client Monitor service on the RUM Client Monitor Probe (for example, https://123.12.1.2:2021/hpmobilemon/data).
- **-h <Probe host>.** The RUM Client Monitor Probe's host name or IP address.

  Note: Either the Probe URL (-u) or Probe host (-h) must be included in the command options.

- **-o <Output file>.** The full path and name of the new APK that is generated.

  Note: The file name must include the file type (**.apk**) or instrumentation will fail.

- **-pans.** Permission AccessNetworkState. Enables the APK to determine and report the type of user connection (WiFi/2G/G3/4G).
- **<Source APK file>.** The full path and name of the source APK you are instrumenting.

  Note:

  - This parameter must be the last one in the command line or instrumentation will fail.
  - The file name must include the file type (**.apk**) or instrumentation will fail.

- **<Signing option>.** For details, see "Signing an APK" on the next page.
- **-ak <Application key>.** An application key is assigned to a mobile application configured in APM. The application key is used by the RUM Client Monitor Probe to associate monitored data of a mobile application to the configured application in APM. For details on configuring an application key in APM, see "Real User Monitor Administration User Interface > Monitoring Settings Page" in the APM Application Administration Guide.
- **-nocrashreport.** Disables crash reporting. (Crash reporting is enabled by default.)

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

- -**overrideacra.** uses a version of the ACRA library to collect data on crashes. If your app already uses ACRA, by default RUM will not show crash data for the app. You can use this flag to add the ACRA library version and override your current ACRA library.

  Note that this will disable your existing ACRA-based reporting mechanism, and you will see crash data in RUM.

- **-hybrid.** Enable hybrid instrumentation for the application. Use this option if the app being monitored is hybrid. For more details, see "Monitoring Hybrid Applications" on page 60.
- **-scf <file name>.** The full path and name of the Static Configuration File located on your local machine. The Static Configuration File of the application is located in **<RUM engine root>\log\configuration\mobileStaticConfigs\<ApplicationName>_ <ApplicationKey>\rumstaticconf.txt**.

  Note: During instrumentation of the APK file from the web console, the RUM Engine will make a copy of the Static Configuration File and save it locally in **<RUM engine root>\tools\ApkInfuser\InfuserDir**. It will use this local copy for instrumentation.

The static configuration file is created when the RUM engine synchronizes the configuration. If this file does not exist, manually synchronize the configuration as follows:

a. Click **Tools > Monitoring configuration information**.

b. Click **Sync all configuration**.

You can also include additional, optional parameters. To display a list of all the valid parameters, run the ApkInfuser.bat file without any parameters.

The following is an example of the command line for running the ApkInfuser.bat file:

```
<RUM installation directory>\tools\ApkInfuser.bat  -u
https://123.12.1.2:2021/hpmobilemon/data -signdebug -ak appkey1234 -o
"c:\MyInstrumentedAPK.apk" "c:\MySourceAPK.apk"
```

Note:

- After instrumenting a mobile app for monitoring by RUM, you must test the instrumented app to ensure that it functions properly before uploading it to the app store.
- You can only instrument an APK once. If you want to make changes to the properties of an already instrumented APK, you must instrument the original source (non-instrumented) APK again.

Signing an APK

When you instrument an APK, you must specify a signing option. You can choose to skip the signing process completely, sign the APK with a a self-signed, debug certificate that is dynamically generated by the ApkInfuser, or fully sign the APK using a Java keystore file containing a private key. Using a self-signed, debug certificate is satisfactory for testing the APK, but to be able to upload the APK to the Google Play store it must be fully signed. You can fully sign the APK later using Java's jarsigner.exe tool (see "Signing an APK using Java's jarsigner.exe Tool" on page 56).

The following table explains the signing parameter options:

Command Line Parameter	Description	Mandatory	Example
You must include one of the following three options in the APKInfuser command line:			

Command Line Parameter	Description	Mandatory	Example
-skipsigning	Do not sign the APK after instrumentation. The user is responsible to sign the APK before uploading it to the Google Play store or installing it on a device.	One of these three options must be included in the APKInfuser command line.	<RUM installation directory>\tools\ApkInfuser\ApkInfuser.bat -u https://123.12.1.2:2021/hpmobilemon/data -**skipsigning** -ak appkey1234 -o "c:\MyInstrumentedAPK.apk" "c:\MySourceAPK.apk"
-signdebug	Sign the APK with a self-signed debug certificate. This is sufficient for testing the APK on a device, but not for uploading it to the Google Play store.		<RUM installation directory>\tools\ApkInfuser\ApkInfuser.bat -u https://123.12.1.2:2021/hpmobilemon/data -**signdebug** -ak appkey1234 -o "c:\MyInstrumentedAPK.apk" "c:\MySourceAPK.apk"
-keystore <Keystore File>	Fully sign the APK using a Java keystore file with a private key. You must include the path and name of the keystore file. **Note:** The keystore file name must include the file type (**.jks**) or instrumentation will fail.		<RUM installation directory>\tools\ApkInfuser\ApkInfuser.bat -u https://123.12.1.2:2021/hpmobilemon/data -**keystore "C:\KeyStores\MyKeyStore.jks" -alias MyAlias -storepass MyKeyStorePassword -keypass MyPrivateKeyPassword** -ak appkey1234 -o "c:\MyInstrumentedAPK.apk" "c:\MySourceAPK.apk"
If you select the -keystore signing option in the APKInfuser command line, the following parameters are applicable: **Note:** When using the -keystore signing option and the mandatory -alias option, we recommend setting passwords for both the keystore and for the private key.			

Command Line Parameter	Description	Mandatory	Example
-alias <Private Key alias>	An alias to the private key entry in the keystore.	Mandatory	<RUM installation directory>\tools\ApkInfuser\ApkInfuser.bat -u https://123.12.1.2:2021/hpmobilemon/data **-keystore "C:\KeyStores\MyKeyStore.jks" -alias MyAlias -storepass MyKeyStorePassword -keypass MyPrivateKeyPassword** -ak appkey1234 -o "c:\MyInstrumentedAPK.apk" "c:\MySourceAPK.apk"
-storepass <Keystore password>	A password for the keystore.	Mandatory when -skipsigning and -signdebug flags are not used.	
-keypass <Private Key password>	A password for the private key entry in the keystore.	Mandatory when -skipsigning and -signdebug flags are not used. **Notes:** • If you set a keystore password (recommended) this option is then mandatory. • If there is no keypass password defined, use the storepass password.	

Note: If you are unable to sign the APK using the ApkInfuser, the **<RUM>\tools\ApkInfuser\log\ApkInfuser.log** file will show the **jarsigner.exe** command line that was executed and the **jarsigner** reported error.

Signing an APK using Java's jarsigner.exe Tool

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

1. From a cmd window, enter:

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

Parameter	Description
KEYSTORE_FILE_FULL_PATH	The path to the keystore file
KEYSTORE_PASSWORD	The password to the keystore

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

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

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

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

Storing URL Request Data

When instrumenting an APK, you can add the **- data** parameter to the ApkInfuser.bat file command line. This option causes the application's URL network data (such as Method, Headers, Post Data, and Response Headers) to be stored to a local file on the mobile device, rather than being sent to the RUM Probe (and subsequently to th RUM Engine and to APM). This is a debug option that enables you to analyze the data to help determine what data to use to extract user names and parameters when configuring an application in APM. (For details on configuring data extraction for an application in APM, see **Real User Monitor Administration User Interface > Search Area** in the APM Application Administration Guide.

When you include the **-data** parameter, the URL request data is saved on the mobile device in **android\data\appliation ID\files\app-network-data.txt**.

Note: If you use the **-data** parameter, the only other parameter you can use in the command line is a signing option. For details, see "Signing an APK" on page 54.

Enabling Users to Opt-In/Opt-Out of Data Reporting

Some apps give each user the ability to avoid sending data from their device, for example using a Settings menu item (opt-out). Other apps ask users to actively approve data collection, for example when the app is first launched (opt-in).

By default, data is automatically sent from mobile apps to Real User Monitor. You can use the -optIn parameter to disable default data reporting; in this case data is only collected from users who opt in. Note that the relevant user interface and interaction within the app are up to the application developer.

To enable or disable reporting from your app to Real User Monitor, change the Boolean value "enabled" in the SharedPreferences "UserMonitoring". The change will take effect the next time the user opens the app.

For example:

```
    private static final String RUM_API_PREFERENCES_NAME = "UserMonitoring";
    private static final String RUM_API_PREFERENCES_ENABLED = "enabled";

    public void disableReporting(View view) {
        SharedPreferences.Editor spe = getSharedPreferences(RUM_API_PREFERENCES_NAME,
```

```
Context.MODE_MULTI_PROCESS).edit();
        spe.putBoolean(RUM_API_PREFERENCES_ENABLED, false).commit();
    }

    public void enableReporting(View view) {
        SharedPreferences.Editor spe = getSharedPreferences(RUM_API_PREFERENCES_NAME,
Context.MODE_MULTI_PROCESS).edit();
        spe.putBoolean(RUM_API_PREFERENCES_ENABLED, true).commit();
    }
```

Notes and Limitations

There are number of known limitations when instrumenting Android applications. For example:

- Using some bytecode obfuscation techniques that employ "junk byte injection" technique will cause APK instrumentation to fail.

Instrumenting Mobile Applications for iOS

You use the RUM mobile solution to enable the RUM Client Monitor Probe to acquire mobile application data through mobile devices. This requires you to instrument the mobile applications. This section describe how to instrument iOS apps. For details on instrumenting Android apps, see "Instrumenting Mobile Applications for Android" on page 52.

To instrument an iOS app, you must make changes to the project Xcode. The changes include adding a number of frameworks to the project, but no code changes are made.

Instrumenting an iOS app

To instrument an iOS app for RUM:

1. From the RUM Engine machine (<RUM engine root>\tools\mobile\ios), copy the following files:
   - RUMService.framework
   - rummonitor.plist

   Note: Alternatively, using CocoaPods you can add the RUMService.framework as a dependency to the project. To do this, edit the Podfile in your project and add **pod 'RumService', '1.2'**.
2. In the Build Phases - Link Binary, add the following native libraries and RUMService.framework to the project:
   - SystemConfiguration.framework
   - CoreTelephony.framework
   - libstdc++.dylib
   - libz.dylib
3. In the build settings, under Other Linker Flags, add the **-ObjC** linker flag.
4. Copy the rummonitor.plist file that you copied in step 1 and add it as a supporting file to the project.

Note: If working with a CocoaPod dependency, create a new rummonitor.plist file in your project.

5. In the rummonitor.plist file, set the following:
   - **Mandatory Parameters**
     - **AppId.** The application key. An application key is assigned to a mobile application configured in APM. The application key is used by the RUM Client Monitor Probe to associate monitored data of a mobile application to the configured application in APM. For details on configuring an application key in APM, see "Real User Monitor Administration User Interface > Monitoring Settings Page" in the APM Application Administration Guide.
     - **cmUrl .** The URL of the RUM Client Monitor Probe to which monitored data is sent. The format is:

       `http://<RUM Client Monitor Probe host name>:8080/<path to the RUM Client Monitor Probe on the host>`

       `For example: http://myhost.com:8080/hpmobilemon/data`

       If you have an https certificate installed on your RUM Client Monitor Probe (see the RUM Hardening Guide), the format is:

       `https://<RUM Client Monitor Probe host name>:2021/<path to the RUM Client Monitor Probe on the host>`

       For example: `https://myhost.com:2021/hpmobilemon/data`

   - **Optional Parameters**
     - **EnableDynamicConfiguration.** Enable the application to use any extracted content (parameter settings, username detection, or allowed POST parameters) configured for it in APM, when the application runs.

       Default value: YES
     - **data.** – Set to YES to test the application offline and collect data locally only. Collected network data is not sent to the probe and is stored locally in the application folder on the mobile device. This data includes the POST content of requests, which can assist you in defining extracted parameters for the application in APM. For details on extracted parameters, see "Parameter Extraction Area" in the Real User Monitor Application General Page in the APM Application Administration Guide.

       Default value: NO

6. Compile the app. The compiled app includes all the necessary components to enable RUM to monitor the mobile application and monitoring is automatically activated when you run the app.
7. Optional. To set up a static configuration, access the file **<RUM engine root>\log\configuration\mobileStaticConfigs\<ApplicationName>_<ApplicationKey>\rumstaticconf.txt** and save this file in the application folder.

   Note: The static configuration file is created when the RUM engine synchronizes the configuration. If this file does not exist, manually synchronize the configuration as follows:

   a. Click **Tools > Monitoring configuration information**.
   b. Click **Sync all configuration**.

Note: After instrumenting a mobile app for monitoring by RUM, you must test the instrumented app to ensure that it functions properly before uploading it to the app store.

Enabling Users to Opt-In/Opt-Out of Data Reporting

Some apps give each user the ability to avoid sending data from their device, for example using a Settings menu item (opt-out). Other apps ask users to actively approve data collection, for example when the app is first launched (opt-in).

By default, data is automatically sent from mobile apps to Real User Monitor. To modify this, in the rummonitor.plist file set the **sendingEnabled** parameter to **NO**. In this case, data is only collected from users who opt in. (The default value is **YES**, which means data is sent unless users opt out.) Note that the relevant user interface and interaction within the app are up to the application developer.

- Include the header file as follows: `#import <RUMService/UserMonitoringSDK.h>`
- To test for the current reporting status: `BOOL b = [UserMonitoringSDK getOptStatus];`

  A value of **YES** means that the device is allowed to report data, **NO** means not allowed.
- To change the value: `[UserMonitoringSDK setOptStatus:YES];`

  Enter **YES** to enable data reporting. The change will take effect the next time the user opens the app.

Monitoring Hybrid Applications

A hybrid application is a cross-platform app that runs inside an embedded WebView and implements web technologies such as JavaScript. Such apps usually include Ajax technology over JavaScript.

When instrumenting a hybrid app, the required operations to monitor every page load and Ajax network operation are automatically included. This means that no manual server-side instrumentation is required.

Note: By default, RUM monitors Ajax operations so that it can report on the network. However, if Java is disabled for an app, Ajax is also disabled so RUM will not be able to monitor the Ajax operations or page loads.

For details on instrumenting apps for Android, see "Instrumenting Mobile Applications for Android" on page 52 and for details on instrumenting apps for iOS, see "Instrumenting Mobile Applications for iOS" on page 58.

Chapter 6: Installing the RUM Server Collector

This section describes how to install the RUM Server Collector on a server running applications that you want to monitor. The RUM Server Collector can be installed on servers running on Windows or Linux operating systems.

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

This section includes the following topics:

- "The RUM Server Collector Setup File" below
- "Installing the RUM Server Collector on a Linux System - Prerequisite" below
- "Installing the RUM Server Collector" on the next page

The RUM Server Collector Setup File

The Software Support Online web site (https://softwaresupport.softwaregrp.com/). Sign in using your Passport user name and password. Click **Manuals**. Under Document Type, select **Patches**. In the Search field, enter **RUM Server Collector Setup File**.

Changing the /tmp Directory for a Linux Installation

In Linux, you can change the installer's working directory (by default /tmp) by running the following commands:

```
export IATEMPDIR=/new/tmp/dir
```

```
export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp/directory
```

where `/new/tmp` directory is the new /tmp directory

Installing the RUM Server Collector on a Linux System - Prerequisite

Before installing the RUM Server Collector on Red Hat Enterprise Linux operating systems for supported 6.x versions, you must install the following RPM packages:

• glibc	• libXext
• glibc-common	• libXtst
• nss-softokn-freebl	• compat-libstdc++-33
• libXau	• libXrender
• libxcb	• libgcc
• libX11	• openssl098e
• compat-expat1	• rpm-devel

To install the RPM packages listed in the upper table, run the RPM installation tool:

<APM_install_folder>/rhel_oel_installation_fix/rpm_installer.sh.

- If the script fails to install any of the RPM packages, the following message appears:

  ```
  !!! ERROR: package <package name> has not been installed successfully

  In this case, refer the problem to your system administrator.
  ```

- If the script detects that an RPM package is already installed, it skips that package and continues with the next package.

  However, you can force the tool to try to re-install any pre-installed packages by adding the **f** parameter to the command:

  <APM_install_folder>/rhel_oel_installation_fix/rpm_installer.sh f

If the Yum Linux upgrade service is not functional on your machine, you will need to download and install the necessary RPM packages manually by running the following command:

yum install -y openssl098e glibc.i686 glibc-common.i686 nss-softokn-freebl.i686 libXau.i686 libxcb.i686 libX11.i686 libXext.i686 libXtst.i686 compat-libstdc++-33.i686 libXrender.i686 libgcc.i686 compat-expat1 rpm-devel

The version of these packages changes from system to system. You can download the packages from any RPM repository site that matches your system specifications. The following RPM search tool can assist you in this task (http://rpm.pbone.net/).

To determine the package version you need to download, execute the following command in a terminal window:

rpm –qa ${PACKAGE_NAME} (ex: rpm -qa glibc)

The command will return the following text:

```
# rpm -qa glibc

glibc-2.12-1.132.el6.x86_64
```

This text indicates the package version required for your machine.

In this case, you would need to download the i686 architecture package with the same version - glibc-2.12-1.132.el6.i686 – and install it manually.

Installing the RUM Server Collector

To install the RUM Server Collector:

1. Save the RUM Server Collector setup folder (for Windows or Linux) on the machine on which you are installing the probe. For details on the location of the RUM Server Collector setup file, see "The RUM Server Collector Setup File" on the previous page.
2. Ensure that the **packages** directory is in the same location as the Server Collector setup file.
3. Run the setup program:
   - **Windows:** Navigate to the downloaded setup file (**RUMSC_<version number>_win64_setup.exe**) and double-click it.
   - **Linux:**
     - Login as the **root** user.
     - Assign full permissions to the setup file: `chmod 777 ./RUMSC_<version number>_linux64_`

`setup.bin`

- Run the setup file:
  - On a machine with X-Server (X11) enabled, run **./RUMSC_<version number>_linux64_setup.bin**
  - On a machine without X11, run **./RUMSC_<version number>_linux64_setup.bin -i silent**

4. Follow the online instructions until the setup has successfully completed.
5. The RUM Server Collector is automatically started after the installation.

Chapter 7: Installing the RUM VDI Agent

The setup file for installing the RUM VDI Agent is **RumVDIAgent_v-<Version number>setup.exe**. The RUM VDI Agent Setup file can be accessed from the RUM installation package.

To install the RUM VDI Agent:

1. Save the RUM VDI Agent setup folder to the machine on which you want to install the RUM VDI Agent.
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.)
4. After the installation completes, close and restart all Internet Explorer and Firefox instances.
5. When restarting Internet Explorer and/or Firefox, enable the **RUMIEAgentBHO** plugin if you are asked to do so.

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

Chapter 8: Uninstalling RUM

This section provides instructions for uninstalling RUM.

Note: To reinstall the RUM engine or probe, wait a least 15 seconds after uninstalling the component.

This section includes:

- "Uninstalling the RUM Engine on a Windows Platform" below
- "Uninstalling the RUM Sniffer Probe" on page 69
- "Uninstalling the RUM Client Monitor Probe" on page 70
- "Uninstalling the RUM Server Collector" on page 71
- "Uninstalling the RUM VDI Agent" on page 72

Uninstalling the RUM Engine on a Windows Platform

You can uninstall the RUM Engine using the Windows Control Panel, or by running a silent installation.

This section includes:

- "How to Uninstall the RUM Engine Using the Windows Control Panel" below
- "RUM Configuration Wizard" on page 20
- "Running a Silent Uninstall" on page 69

How to Uninstall 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. Go to the **Control Panel**
   b. Select the option to add and remove programs
   c. Select **Real User Monitor**
   d. Select the remove option
2. When prompted, select the installation language (default English) and click **OK**. The RUM 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 RUM Configuration wizard is automatically started. For details on the user interface, see "RUM Configuration Wizard" on the next page.

   Note: When uninstalling a MySQL database only, the RUM 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. After 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.

RUM Configuration Wizard

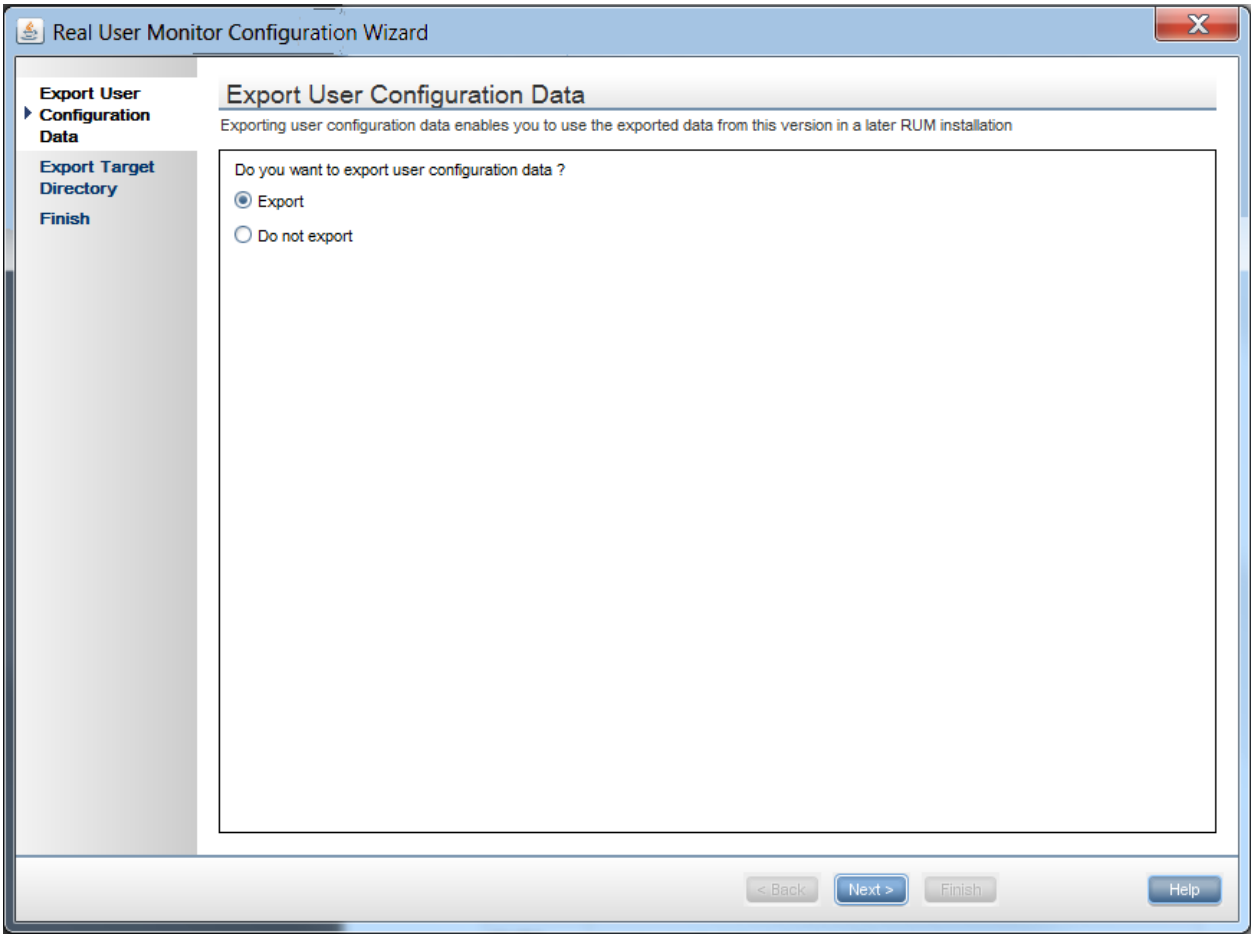
This wizard enables you to export user configuration data for use in a future RUM installation.

To access	The RUM 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 RUM. • If you export user data settings, do not delete the **rum_data** directory or you will lose all the data stored in the database.
Wizard Map	The RUM Configuration wizard contains: "Export User Configuration Data Page" below > "Export Target Directory Page" on the next page > "Finish Page" on page 68
Useful Links	"Installing the RUM Engine" on page 17

Export User Configuration Data Page

This page enables you to select whether you want to export user data settings for use by a future RUM installation. This is part of the RUM Configuration wizard; refer to "RUM Configuration Wizard" above for general information.

The following is an example of the Export User Configuration Data page:



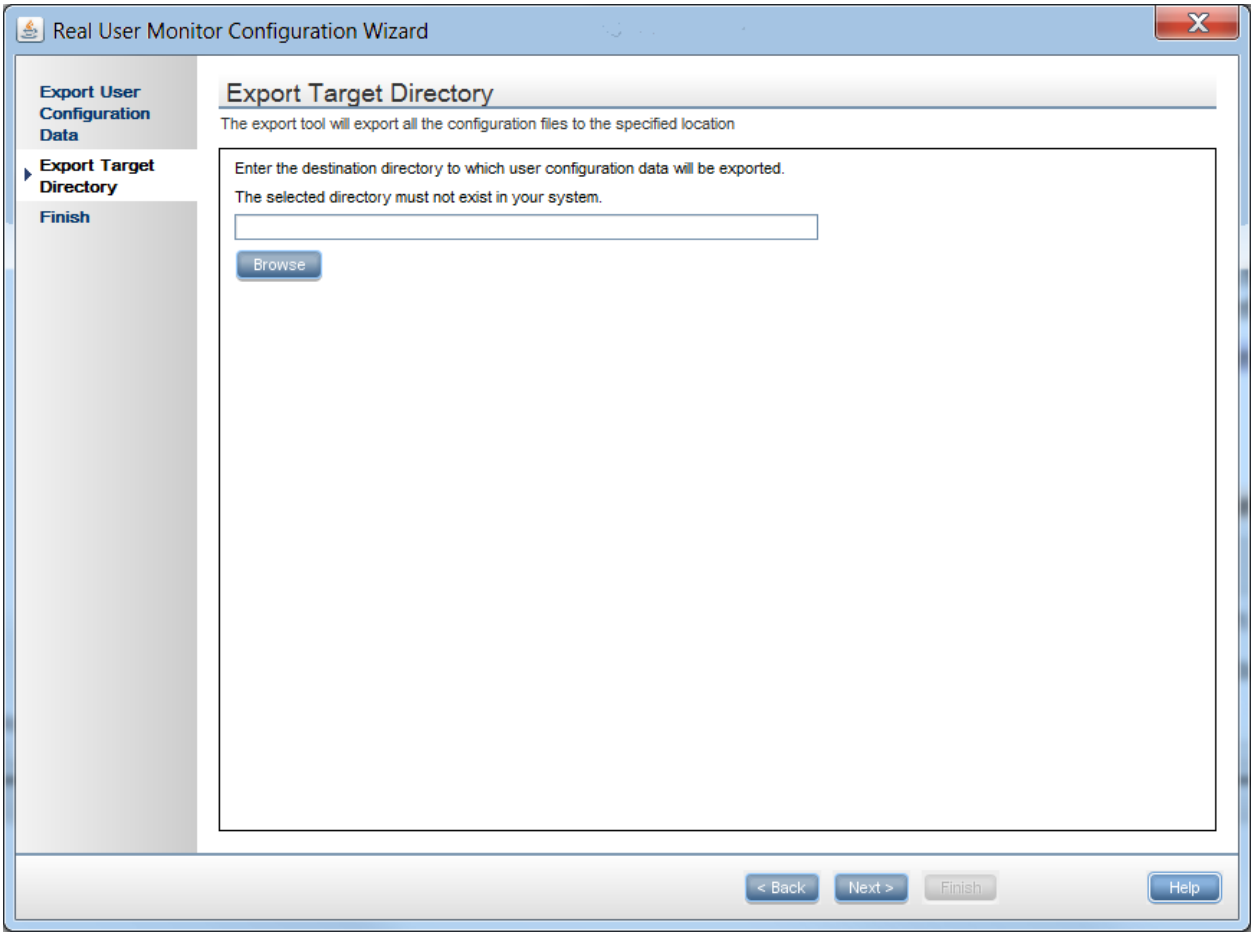
The following elements are included:

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 the next page.

Export Target Directory Page

This page enables you to select the path to which to export user data settings. This is part of the RUM Configuration wizard; refer to "RUM Configuration Wizard" on the previous page for general information.

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



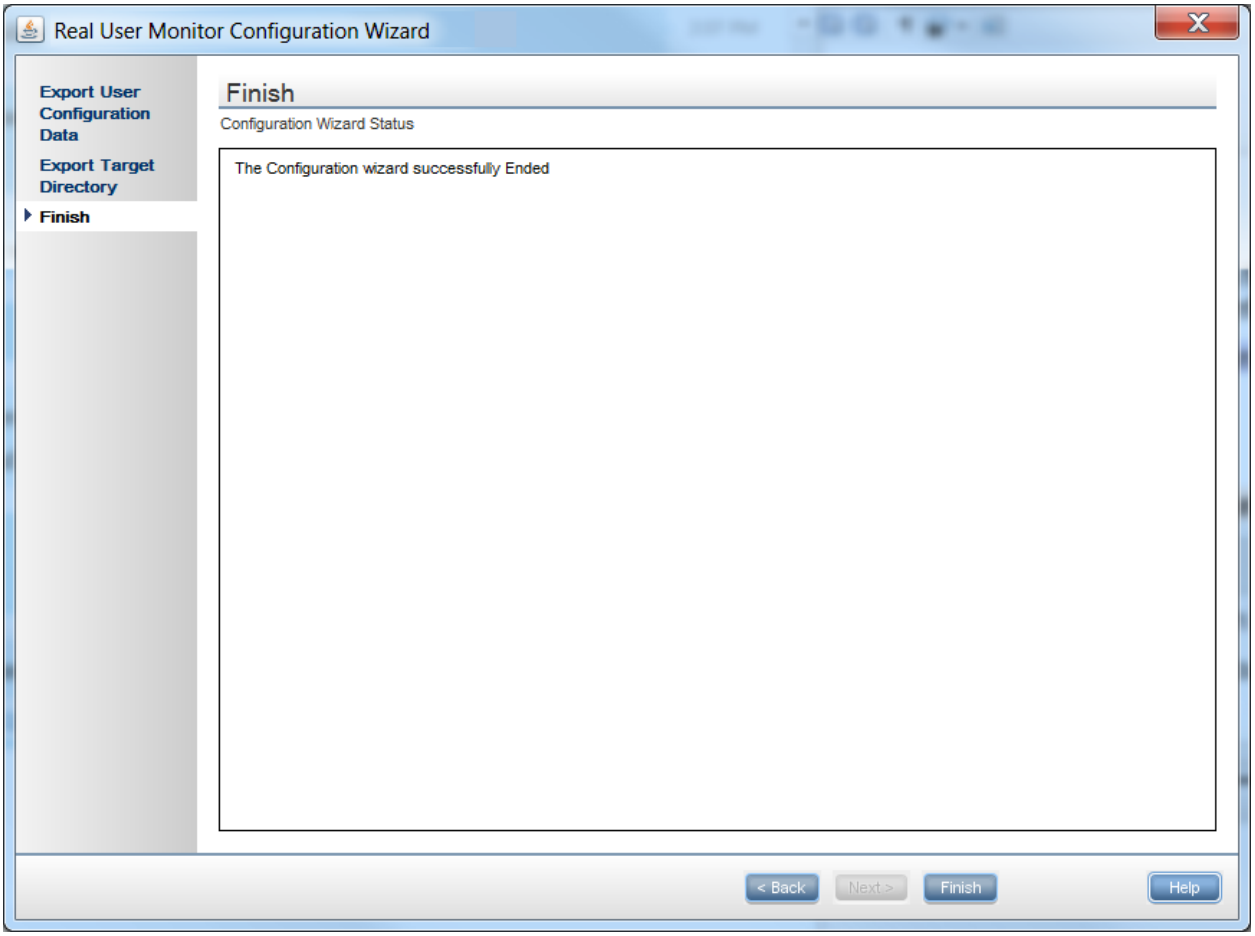
The following elements are included:

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

This page displays a message showing the status of the Configuration wizard. Click **Finish** to exit and return to the RUM Engine Setup wizard. This is part of the RUM Configuration wizard; refer to "RUM Configuration Wizard" on page 66 for general information.

The following is an example of the 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 33.

Uninstalling the RUM Sniffer Probe

The procedure for uninstalling the RUM Sniffer differs according to the operating system on which it is installed.

This section includes:

- "Uninstalling the RUM Probe on a Windows System" on the next page
- "Uninstalling the RUM Probe on a Linux System" on the next page

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:
   a. Go to the **Control Panel**.
   b. Select the option to add and remove programs.
   c. Select **RUM Sniffer Probe**.
   d. Select the remove option.
2. When prompted, select the installation language (default English) and click **OK**. The RUM 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**.
5. 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. After the RUM Probe 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.

Uninstalling the RUM Probe on a Linux System

To uninstall the RUM Probe on a Linux system:

1. Log in as a root user.
2. Stop the RUM Probe using the following command:

   ```
   /etc/init.d/rum_probe-capture stop
   ```

3. Uninstall the Probe:
   a. `rpm -qa | grep -i rum_probe` (This command lists all the installed rum_probe RPMs.)
   b. `rpm -e XXX` (`XXX` is one of the installed rum_probe RPMs that was listed in the previous step. Repeat this instruction for each RPM.)
4. Verify that all related directories are removed.

   ```
   ls /etc/rum_probe
   ```

   Remove any remaining related directories:
   a. `/etc/rum_probe`
   b. `/var/spool/rum_probe/`

   Note: If the RUM Probe was installed in a non-standard directory, rum_probe will be located under that directory. For example, if the RUM Probe was installed under /opt/mydirectory, it will be located in /opt/mydirectory/etc/rum_probe.

Uninstalling the RUM Client Monitor Probe

When you uninstall the RUM Client Monitor Probe you lose any changes you made to the configuration files. If you want to save these changes for when you reinstall the newer RUM Client Monitor Probe version, backup

the configuration files before uninstalling. You can restore these files after reinstalling the new version of the RUM Client Monitor Probe.

Uninstalling the RUM Client Monitor Probe on a Windows System

To uninstall the RUM Client Monitor Probe:

1. On the machine from which you are uninstalling the RUM Client Monitor Probe:
   a. Go to the **Control Panel**
   b. Select the option to add and remove programs
   c. Select **RUM Client Monitor Probe**.
   d. Select the remove option
2. When prompted, select the installation language (default English) and click **OK**. The RUM Engine Setup wizard begins.
3. When the Application Maintenance page is displayed, select **Uninstall**. A message appears warning that the configure changes you made will be lost.
4. Click **OK** to continue uninstalling the Client Monitor Probe.
5. Click **Next**.
6. The pre-uninstall summary information displays the RUM components that will be removed. Click **Uninstall**.
7. 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.
8. After the RUM Client Monitor Probe has been uninstalled, you can view the uninstall log file by clicking the **View log file** link.
9. Click **Done** to exit the uninstall process.

Uninstalling the RUM Server Collector

This section describes how to uninstall the RUM Server Collector.

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

Caution: After uninstalling the RUM Server Collector, the Server Collector configuration file and default security keys and certificates are no longer available.

Uninstalling on Windows

To uninstall the RUM Server Collector from Windows, use one of the following options:

- Invoke the Uninstall wizard - `C:\<RUM Server Collector installation directory>\Uninstall\RUMSC\setup.exe`
- Use standard Windows tools

Uninstalling on Linux

To uninstall the RUM Server Collector from Linux:

1. Stop the RUM Server Collector: `/etc/init.d/rum_server-collector stop`
2. Navigate to the directory containing the uninstall command: `cd /opt/HP/RUMSC/Uninstall/RUMSC`
3. Run the setup file: `sudo ./setup.bin -i silent`

Uninstalling the RUM VDI Agent

This section describes how to uninstall the RUM VDI Agent.

To uninstall the RUM VDI Agent:

1. Click **Start > Control Panel > Add or Remove Programs**.
2. Select **RUM VDI Agent** and click **Remove**.
3. Reboot the computer.

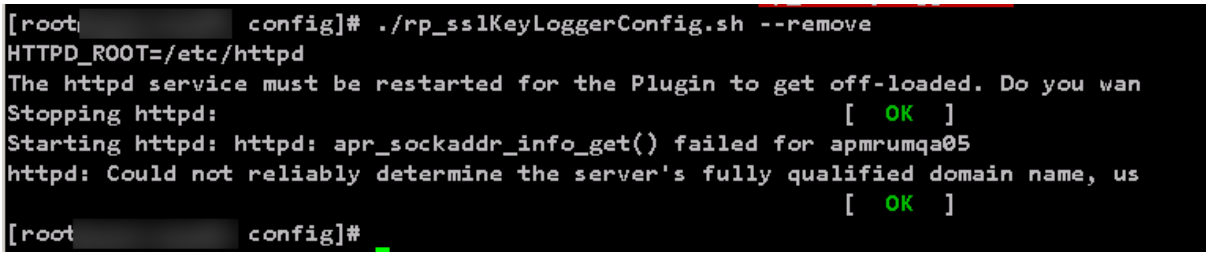
Uninstall SSL Agent for Apache web server

Perform the following steps for uninstalling the SSL agent:

1. Remove the plug-in:

   Change directory to **~/rp_sslKeyPlugin/plugin/config/** and execute the below command

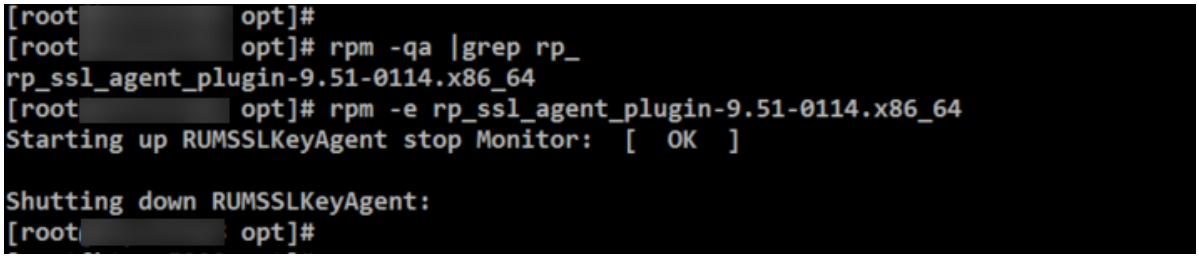
   ./rp_sslKeyLoggerConfig.sh –remove



2. Uninstall the package

   Move to the install dir of the agent. In this case it is /opt

   a. **rpm -qa | grep -i rp_ssl_agent_plugin** (This command lists the installed SSL plugin RPM.)
   b. **rpm -e XXX** . Where XXX is the installed SSL plugin RPM listed in the previous step.


[root opt]#
[root opt]# rpm -qa |grep rp_
rp_ssl_agent_plugin-9.51-0114.x86_64
[root opt]# rpm -e rp_ssl_agent_plugin-9.51-0114.x86_64
Starting up RUMSSLKeyAgent stop Monitor: [OK]
Shutting down RUMSSLKeyAgent:
[root opt]#

Part 3: Upgrading RUM

Chapter 9: Workflow for Upgrading RUM

Note:

- The RUM Sniffer Probe and the RUM Client Monitor Probe version must be the same as the RUM Engine version. However, when upgrading RUM, you first upgrade the Probes and then upgrade the Engine, so the Probe versions will be newer than the RUM Engine until the upgrade is complete. For details about specific versions, see "Upgrading the RUM Sniffer Probe" on page 77 and "Upgrading the RUM Client Monitor Probe" on page 79.
- You must upgrade the RUM Database CORE before upgrading the RUM engine.

To upgrade RUM, upgrade the following components in the order shown:

1. RUM Sniffer Probe (see "Upgrading the RUM Sniffer Probe" on page 77)
2. RUM Client Monitor Probe (see "Upgrading the RUM Client Monitor Probe" on page 79)
3. RUM Server Collector (see "Upgrading the RUM Server Collector" on page 86)
4. RUM Engine (see "Upgrading the RUM Engine" on page 80)
5. APM (see the appropriate APM Upgrade Guide)

   Note: When upgrading APM, RUM persists the data samples to send to APM. Persistency is limited by the amount of unsent sample data and by time. To increase the amount of unsent sample data, see Configuring the Amount of Unsent Sample Data to Store in RUM in the Real User Monitor Administration Guide.

6. After completing this workflow, check the status of the Publisher in the Health report. If the status is not OK, check the publisher log to see if the samples are being sent. If no samples are being sent, restart the RUM Engine and check the status of the Publisher in the Health report again.

Upgrading to Version 9.51 from Versions Previous to 9.2x

The RUM Sniffer Probe version must always be equal to or greater than the RUM Engine version.

Therefore, if the RUM Sniffer Probe and the RUM Engine can be upgraded at the same time (for example, during a downtime), you can upgrade both directly to version 9.51.

However, you must upgrade the RUM Sniffer Probe and RUM Engine to version 9.22 before upgrading to version 9.51. Version 9.22 provides an improvement modification in the communication between the RUM Engine and RUM Sniffer Probe.

For example, if the RUM Sniffer Probe and RUM Engine are both version 9.13 and you want to upgrade them to version 9.51, and you cannot perform the upgrade to both the Probe and Engine on the same day, you need to do the following:

1. Upgrade the RUM Sniffer Probe to version 9.22.
2. Upgrade the RUM Engine to version 9.22.

3. Upgrade the RUM Sniffer Probe to version 9.51.
4. Upgrade the RUM Engine to version 9.51.

Chapter 10: Upgrading the RUM Sniffer Probe

The procedure for upgrading the RUM Sniffer Probe differs according to the platform on which it is installed.

Note: You must upgrade the RUM Sniffer Probe and RUM Engine to version 9.22 before upgrading to version 9.51. Version 9.22 provides an improvement modification in the communication between the RUM Engine and RUM Sniffer Probe.

This section includes:

- "Upgrading the RUM Probe - Linux" below
- "Upgrading the RUM Probe - Windows" below

Upgrading the RUM Probe - Linux

To upgrade Linux installations of the RUM Probe:

1. Stop the RUM Probe:
   - Log in to the RUM probe machine as the root user.
   - Stop the RUM Probe with the following command: **/etc/init.d/rum_probe-capture stop**
2. If you are upgrading the probe from version 9.x, uninstall the old probe as described in "Uninstalling RUM" on page 65.
3. Save the RUM Probe Setup file for Linux to the **/var/tmp** directory on the RUM Probe machine. For details on the location of the RUM Probe setup file, see "The RUM Probe Setup File" on page 39.
4. SSL keystore files from previous probe installations that are located in **<prefix>/etc/rum_probe/keystore**, are retained. If the SSL keystore files are located in any other location, back them up.
5. Run the installation script as described in "Installing the RUM Sniffer Probe" on page 37.

   Note: Install the new probe to the exact path of the old one (default /var/HPRUMProbe).
6. Restore SSL keystore files if you backed them up in step 4.
7. Start the RUM Probe with the following command: **/etc/init.d/rum_probe-capture start**

Note: The above procedure should take less than a minute and therefore results in minimal data loss.

Upgrading the RUM Probe - Windows

To upgrade Windows installations of the RUM Probe:

1. Save the RUM Probe setup file for Windows on the machine on which you are upgrading the probe. For details on the location of the RUM Probe setup file, see "The RUM Probe Setup File" on page 39.
2. Stop the old probe by opening **Disable RUMProbe** on the computer's Start menu.
3. SSL keystore files from previous probe installations that are located in **<Real User Monitor probe root directory>\etc\rum_probe\keystore**, are retained. If the SSL keystore files are located in any other location, back them up.
4. Uninstall the old probe by selecting **Start > Control Panel > Add or Remove Programs > HPRUMProbe**.

5. Install the new Windows probe as described in "Installing the RUM Sniffer Probe" on page 37.

   Note: Install the new probe to the exact path of the old one (default C:\HPRUMProbe).

6. Restore SSL keystore files if you backed them up in step 3.
7. Start the new probe by executing **Enable RUMProbe** on the computer's Start menu.

Chapter 11: Upgrading the RUM Client Monitor Probe

When upgrading the RUM Client Monitor Probe to version 9.51, the RUM Engine version must be at least 9.23. If necessary, upgrade the RUM Engine to version 9.23 before upgrading the RUM Client Monitor Probe to version 9.51.

Note: If when installing the RUM Client Monitor Probe, you made any changes to the configuration files, you will need to back up these files before upgrading and reapply the changes in the new configuration files.

This section describes how to upgrade the RUM Client Monitor Probe.

To upgrade the RUM Client Monitor Probe:

1. Back up the RUM Client Monitor Probe configuration files if any changes were made. RUM Client Monitor Probe configuration files include (but are not limited to):
   - <RUMClientMonitorProbe>\conf\cm.properties
   - Files within the <RUMClientMonitorProbe>\conf\ssl folder
   - <RUMClientMonitorProbe>\apache-tomcat\conf\server.xml
   - <RUMClientMonitorProbe>\apache-tomcat\webapps\ROOT\WEB-INF\web.xml
2. Uninstall the old RUM Client Monitor Probe.
3. Install the new RUM Client Monitor Probe as described in "Installing the RUM Client Monitor Probe" on page 47.
4. Reapply the configuration changes in the corresponding new files.

   Note: Do not replace the entire file.

Chapter 12: Upgrading the RUM Engine

Upgrading the RUM Engine is a two part procedure. You must upgrade the RUM Engine configuration and then upgrade the database data.

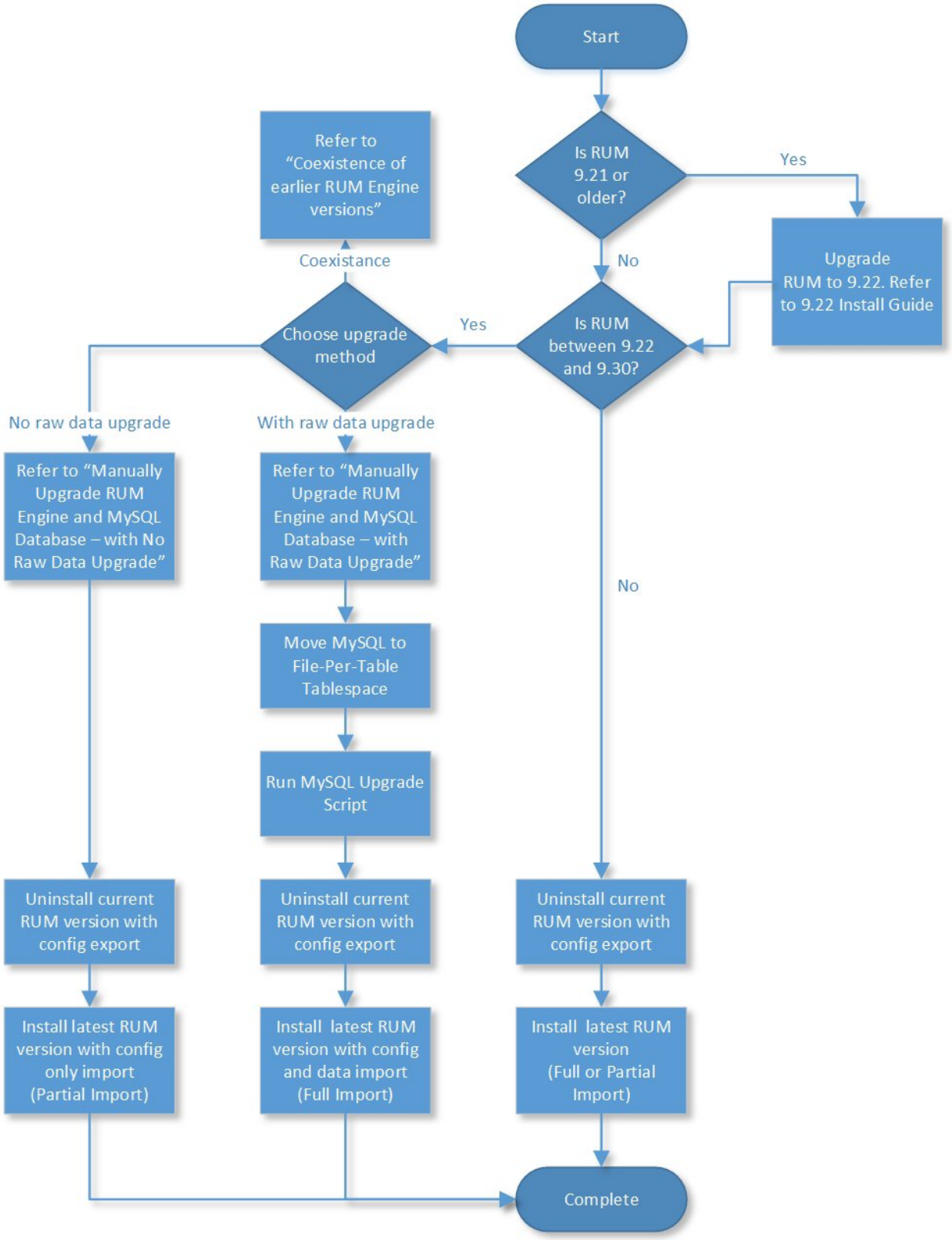
Note: You must upgrade the RUM Sniffer Probe and RUM Engine to version 9.22 before upgrading to version 9.51. Version 9.22 provides an improvement modification in the communication between the RUM Engine and RUM Sniffer Probe.

This section includes:

- "Flow for the RUM Engine Upgrade" below
- "Upgrading from a Typical Installation to a Distributed Installation" on page 82
- "Upgrading from RUM Versions 9.2x and Above" on page 82
- "Upgrading Database Data" on page 83
- "Troubleshooting" on page 84

Flow for the RUM Engine Upgrade

The following flowchart illustrates the steps to follow when upgrading the RUM Engine.


Start
Is RUM 9.21 or older?
Yes
No
Upgrade RUM to 9.22. Refer to 9.22 Install Guide
Refer to "Coexistence of earlier RUM Engine versions"
Coexistance
Is RUM between 9.22 and 9.30?
Yes
Choose upgrade method
No raw data upgrade
With raw data upgrade
No
Refer to "Manually Upgrade RUM Engine and MySQL Database – with No Raw Data Upgrade"
Refer to "Manually Upgrade RUM Engine and MySQL Database – with Raw Data Upgrade"
Move MySQL to File-Per-Table Tablespace
Run MySQL Upgrade Script
Uninstall current RUM version with config export
Uninstall current RUM version with config export
Uninstall current RUM version with config export
Install latest RUM version with config only import (Partial Import)
Install latest RUM version with config and data import (Full Import)
Install latest RUM version (Full or Partial Import)
Complete

Upgrading from a Typical Installation to a Distributed Installation

Regardless of your upgrade path, if you are upgrading from a typical installation (in which both the MySQL database and the RUM Engine are installed on the same machine) to a distributed installation (in which the MySQL database and the RUM Engine are installed on separate machines), you must incorporate the following steps into the instructions detailed below for the relevant upgrade paths.

On the Source (Typical) Machine

When you uninstall RUM on the source machine, you must export the user data settings and configuration when prompted.

On the Destination MySQL Database Machine

1. Copy the exported user data settings and configuration directory, as well as the **RUM_DATA** directory, from the previous version to the new MySQL database machine.

   Note:

   - You can copy the **RUM_DATA** directory only after the RUM Engine is stopped, and after verifying that the MySQL Windows service is not running.
   - The **RUM_DATA** directory must be located in the same path on the new (MySQL database) machine as it was in the source (typical) machine.
   - **RUM_DATA** is the default directory used by the RUM setup program. If you changed the name of this directory in the previous version of RUM, ensure that you use the same name in the new version.

2. When installing the new version of RUM, select the option to install the MySQL database only.
3. During the installation, import the saved user data settings and configuration from the previous version, when prompted.

On the Destination Engine Machine

1. Copy the exported user data settings and configuration directory from the previous version to the new engine machine.
2. In this directory, edit the **<export directory>\AppServer\deploy\mysql-ds.xml** file and modify the **<connection-url>** parameter setting to point to the new MySQL database machine. (Usually, this will involve changing the setting from **localhost** to the new machine name.)
3. When installing the new version of RUM, select the option to install the RUM Engine only.
4. During the installation, import the saved user data settings and configuration from the previous version, when prompted.

Upgrading from RUM Versions 9.2x and Above

Note: If you are upgrading from a typical installation (in which both the MySQL database and the RUM Engine are installed on the same machine) to a distributed installation (in which the MySQL database and

the RUM Engine are installed on separate machines), you must incorporate the steps detailed in "Upgrading from a Typical Installation to a Distributed Installation" on the previous page into the following procedure.

1. In the RUM Engine web console, synchronize configuration data by selecting **Tools > Monitoring Configuration Data > Sync All Configuration**. Ensure that the synchronization is successful. For details, see the Real User Monitor Administration Guide.
2. Uninstall the existing version of the RUM Engine. During the uninstall process you must export the user data settings and configuration when prompted. For details on uninstalling the RUM Engine, see "Uninstalling RUM" on page 65.

   Note: Uninstalling the RUM Engine also uninstalls the MySQL schema database, but does not delete the data files. These data files are located in the **RUM_DATA** directory. Do not make any manual changes to this directory, or to the files in it.

3. Save the RUM setup file for Windows on the machine on which you are upgrading RUM and run the setup. For details on locating the RUM setup file and installing the RUM Engine, see "Installing the RUM Engine" on page 17.

   Note:
   - As part of the installation process, you must import the saved user data settings and configuration from a previous version.
   - As part of the upgrade, during the installation you must connect to the previous, existing MySQL database. The database structure is automatically upgraded.

4. Start the RUM Engine by opening **Real User Monitor** on the RUM Engine machine.
5. Configure the upgraded RUM Engine to connect to the upgraded APM system.You configure the connection settings in the RUM Engine web console by selecting **Configuration > APM Connection Settings**.

   If you have upgraded APM using the Staging Data Replicator (SDR), ensure that the upgraded RUM Engine is configured to connect to the upgraded APM system.
6. If the RUM engine is hardened to be accessed via HTTPS and BSM 9.26 is connected to it, ensure that the BSM server's certificate is reimported to **RUM\JRE\lib\security\cacerts** after the upgrade. This is necessary because importing the older RUM engine configuration during upgrade does not replace the cacerts file provided by the new RUM engine installation. The new cacerts is intentionally not replaced during import to ensure retention of new CA certificates that are provided as part of the newly installed RUM engine's JRE.

Upgrading Database Data

Note: If you are upgrading your MySQL database from version 5.5 to 5.7, see the instructions in "Upgrading MySQL from version 5.5 to 5.7" on page 88.

- **Upgrading Database Data from Versions earlier than RUM 9.22**

  You must upgrade the RUM Sniffer Probe and RUM Engine to version 9.22 before upgrading to version 9.51. Version 9.22 provides an improvement modification in the communication between the RUM Engine and RUM Sniffer Probe.

- **Upgrading Database Data from RUM 9.22, 9.23, or 9.24**

  When upgrading to RUM 9.40 from RUM 9.22, 9.23, or 9.24, if you import an old RUM Engine configuration, or connect to the existing database of an older version, new, empty database tables are created with the new structure and the old database tables are renamed by appending **_old** to their name. However, the actual contents of the tables (that is, the RUM data) is not copied to the new tables. To copy data to the new tables, run the **upgrade_data_from_922_923_924_to_new_version.bat** batch file from a command line on the RUM Engine, using the following format:

  <RUM installation directory>\mysql\scripts\upgrade_data_from_922_923_924_to_new_version.bat <MySQL user name> <MySQL password> <MySQL database schema name>

  We recommend that you run this batch file during off-peak hours as depending on the size of your database, the process can take a long time and may affect RUM Engine performance.

  You can stop or pause the batch file after it has been started by running the batch file:

  <RUM installation directory>\mysql\scripts\stop__upgrade_data_to_new_version.bat<MySQL user name> <MySQL password> <MySQL database schema name>

  To restart the batch file from the point it was stopped, re-run the **upgrade_data_from_922_923_924_to_new_version.bat** file as described above.

Notes and Limitations:

- Until you copy the data from the old tables to the new ones, the data in the old tables is not accessible and any End User Management reports that are based on raw data will be empty (for example, the RUM Session Analyzer report).
- By default, RUM only stores raw data for two weeks back, so no more than this is copied by the batch file.
- Raw data monitored by RUM after you have upgraded to version 9.51 is automatically saved to the new database tables and is included in EUM reports.

Troubleshooting

If RUM Engine 9.51 is configured to be accessed via HTTPS and BSM 9.26 is connected to the RUM Engine, perform the following steps on the BSM side. In addition, follow the procedure in "Securing Connections to the RUM Engine" in the RUM Hardening Guide.

For additional information, see Sweet32: Birthday attacks on 64-bit block ciphers in TLS (https://softwaresupport.softwaregrp.com/km/KM02681808).

1. Open the **< Application Performance Management root directory>/JRE/lib/security/java.security** file.
2. Locate the line:

   jdk.tls.disabledAlgorithms=MD5, SSLv3, RC4, DSA
3. Edit the line as follows:

   jdk.tls.disabledAlgorithms=MD5, DSA, DESede, DES_CBC, DHE, RC4, SSL, ECDH_anon, DH_anon, NULL, DH keySize < 768, RSA keySize < 2048
4. Save the file
5. Open the **< Application Performance Management root directory>/JRE64/lib/security/java.security** file.
6. Locate the line:

   jdk.tls.disabledAlgorithms=MD5, SSLv3, RC4, DSA
7. Edit the line as follows:

jdk.tls.disabledAlgorithms=MD5, DSA, DESede, DES_CBC, DHE, RC4, SSL, ECDH_anon, DH_anon, NULL, DH keySize < 768, RSA keySize < 2048

8. Save the file.
9. Open the **HPBSM\jboss-as\bin\standalone.conf** file and add the following line to the end of the file:

   JAVA_OPTS="$JAVA_OPTS -Dhttps.protocols=TLSv1,TLSv1.1,TLSv1.2"
10. Restart BSM.

Chapter 13: Upgrading the RUM Server Collector

This section describes how to upgrade the RUM Server Collector.

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

To upgrade the RUM Server Collector:

1. Uninstall the old RUM Server Collector as described in "Uninstalling the RUM Server Collector" on page 71.
2. Install the new RUM Server Collector as described in "Installing the RUM Server Collector" on page 61.

Note: Security configuration files, certificates and encryption keys you have added are not deleted or overwritten by the upgrade procedure.

Chapter 14: Upgrading the RUM VDI Agent

This section describes how to upgrade the RUM VDI Agent (in previous versions known as RUM HTTP Agent).

To upgrade the RUM VDI (HTTP) Agent:

1. Uninstall the RUM VDI (HTTP) Agent (see "Uninstalling the RUM VDI Agent" on page 72).
2. Install the new version of the RUM VDI Agent (see "Installing the RUM VDI Agent" on page 64).

Chapter 15: Upgrading MySQL from version 5.5 to 5.7

The following table lists the advantages and disadvantages of the options for upgrading MySQL from version 5.5 to version 5.7. These options are recommended in the order listed.

Option	Advantages	Disadvantages
"Coexistence of earlier RUM Engine versions (9.2x or later) with latest RUM Engine " below	No downtime Minimal Risk	Requires additional hardware during the upgrade period
"Manually Upgrade RUM Engine and MySQL Database – with No Raw Data Upgrade" on the next page	Short downtime No additional hardware required	Loss of raw data
"Manually Upgrade RUM Engine and MySQL Database – with Raw Data Upgrade" on the next page	No additional hardware required	Long downtime

Coexistence of earlier RUM Engine versions (9.2x or later) with latest RUM Engine

This option requires you to install RUM Engine version 9.51 on a new server and connect it to the existing Application Performance Management (APM) application. The old RUM Engine must remain connected to APM until the until the old data is obsolete.

1. From the Probe Management configuration option in the RUM web console, disconnect the earlier version of the RUM Client Monitor Probe and RUM Sniffer Probe from the RUM Engine. For details, see "Probe Management" in the Real User Monitor Administration Guide.
2. Upgrade the RUM Client Monitor Probe to version 9.51. For instructions, see "Upgrading the RUM Client Monitor Probe" on page 79.
3. Upgrade the RUM Sniffer Probe to version 9.51. For instructions, see "Upgrading the RUM Sniffer Probe" on page 77.
4. Install RUM Engine 9.51 on a new server. For instructions, see "Upgrading the RUM Engine" on page 80.
5. Connect new or upgraded Probes to RUM Engine. For instructions, see "Installing the RUM Client Monitor Probe" on page 47 and "Installing the RUM Sniffer Probe" on page 37.
6. Connect RUM Engine 9.51 to the BSM/APM that the earlier version RUM Engine is connected to. For instructions, see "Upgrading the RUM Engine" on page 80.
7. Update the EUM Admin application with RUM Engine 9.51. (Add the new Engine but do not delete the old one). For instructions, see the "APM Application Administration Guide".

Manually Upgrade RUM Engine and MySQL Database – with No Raw Data Upgrade

This option requires you to uninstall the current RUM Engine, export the configuration, install RUM Engine 9.51, and import the previous configuration. Raw data is not imported to the new RUM database.

1. Uninstall the earlier RUM Engine version (9.2x or later) and export the configuration. For instructions, see "Uninstalling the RUM Engine on a Windows Platform" on page 65.
2. Install RUM 9.51 and import the earlier RUM configuration. For instructions, see "How to Install the RUM Engine" on page 17.

Note: In the RUM Configuration Wizard, select *Import* in the Import User Configuration Data Page, and do not check *Connect to existing schema* in the RUM Database Connection Parameters Page.

Manually Upgrade RUM Engine and MySQL Database – with Raw Data Upgrade

The following is the general workflow with links to the actual instructions for manually upgrading RUM Engine from the earlier version (9.2x or later) to 9.51 and MySQL database from version 5.5 to 5.7.

1. "Move MySQL Database to File-Per-Table Tablespace" below.
2. "Run MySQL Upgrade Script" on page 91
3. Uninstall the previous RUM version and export the configuration. For instructions, see "Uninstalling the RUM Engine on a Windows Platform" on page 65.
4. Ensure MySQL services are completely removed post-uninstall. (If not, restart the operating system and confirm the removal, before installing the new version of RUM).
5. Install RUM 9.51 and import the configuration from the previous version. For instructions, see "How to Install the RUM Engine" on page 17.

Move MySQL Database to File-Per-Table Tablespace

1. Stop RUM (pre-upgrade version).

   Run **Disable Real User Monitor** on the computer's Start menu.
2. Dump the MySQL 5.5 schema by entering the following command at a command prompt under **...\RUM\MySQL\bin>**:

   mysqldump -u <MySQL_UserName> -p <MySQL_Schema_Name> > <DUMP_MySQL55_File_Name>.sql

   where:

   - **MySQL_UserName** is the RUM user name
   - **MySQL_Schema_Name** is the current schema name
   - **DUMP_MySQL55_File_Name** is the name for the dump file

   For example: `mysqldump -u rum_user -p rum_schema > C:\dump_old_schema.sql`

Note: If the MySQL database resides on a separate physical device, include the parameter `-h <Hostname of MySQL DB server>`

mysqldump -u <MySQL_UserName> –h <Hostname of MySQL DB server> -p <MySQL_Schema_Name> > <DUMP_MySQL55_File_Name>.sql

For example :

```
mysqldump.exe -u rum_user -h 10.10.10.41 -p rum_schema >  C:\dump_old_schema.sql
```

3. Drop all the schemas (except for the **mysql** schema and **information_schema**).
   a. **...\RUM\MySQL\bin>mysql -u <MySQL_UserName> -p**

   Note: If the MySQL database resides on a separate physical device, include the parameter `-h <Hostname of MySQL DB server>`

   ...\RUM\MySQL\bin>mysql -u <MySQL_UserName> –h <Hostname of MySQL DB server> -p

   For example :

   ```
   ...\RUM\MySQL\bin>mysql -u rum_user -h 10.10.10.41 -p
   ```

   b. Enter the password.
   c. Run the following command to obtain the list of all databases:
   SHOW DATABASES;
   d. To drop each database, run the following command on each database:
   DROP DATABASE <Database_Schema_Name>;
   e. Exit the MySQL prompt by typing the following command:
   exit
4. Stop the MySQL service.
   sc stop MySQL
5. In the **..\RUM\mySQL\rum_options.ini** file under **[mysqld]**:
   a. Add:
   innodb_file_per_table=1
   innodb-buffer-pool-instances=2
   b. Edit as follows:
   - If the server has 4 GB RAM
     - **innodb_buffer_pool_size = 1G**
     - **innodb_log_file_size = 500M**
   - If the server has 8 GB RAM
     - **innodb_buffer_pool_size = 2G**
     - **innodb_log_file_size = 1G**

   c. Save the **rum_options.ini** file.

Note: Check carefully that you have done everything before proceeding to the next step.

6. Delete the following files from the **RUM_DATA** folder:
   - **ibdata1**
   - **ib_logfile0**
   - **ib_logfile1**
7. Start the MySQL service.
   sc start MySQL
8. Import the dump file to the schema.
   a. **C:\RUM\MySQL\bin> mysql -u <MySQL_UserName> -p**
   b. Enter the password.
   c. **CREATE DATABASE IF NOT EXISTS <MySQL_Schema_Name>;**

      Note: Use the same name as was deleted in step 3.

   d. **USE <MySQL_Schema_Name>;**
   e. **Source <DUMP_MySQL55_File_Name>.sql**
   f. Exit the MySQL prompt by running the following command:
      exit

Run MySQL Upgrade Script

Note:

- To run the MySQL upgrade script you must be an Administrator.
- Ensure that mysqld.exe is running and that the memory consumed by the process is greater then 1MB.
- Ensure that the RUM\MySQL folder is not locked.

1. Obtain the MySQL upgrade script. In the Software Support web site https://softwaresupport.softwaregrp.com/, locate and download the upgrade zip file: **RUM_ MySQL_ v5.5_to_v5.7_upgrade_tool.zip**
1. Unzip the contents of this file.
2. From a command line, run **MySQL_v5.5_to_v5.7_upgrade_tool.bat**.
3. To confirm that all services are running, execute the following command::
   mysqlcheck -u rum_user –h 10.10.10.41 -p --all-databases
   The services should display a status of **OK**.

Chapter 16: Upgrading RUM - Notes and Limitations

This section describes the following notes and limitations relevant to upgrading RUM:

- If the RUM Engine is working with SSL and:
  - a customer self-signed Certification Authority (CA) certificate is being used for one of the connections;
  - the self signed CA certificate is in the default JRE truststore (cacerts), and not in a separate keystore;

  You will have to export the CA certificate manually from the original JRE truststore that is saved in the exported data directory to the new JRE used by the upgraded RUM Engine. If you are using a certificate that is trusted by a well-known CA, or a self-signed certificate in a separate keystore file that is located outside of the <Real User Monitor Engine root directory>, you do not have to perform this procedure.
- If you are upgrading a RUM Engine that is running on a different port than the default one (8180), you must manually change each occurrence of port 8180 within the **<Real User Monitor Engine root directory>\EJBContainer\bin\mercury_run.bat** file to the port that the RUM Engine is using.
- A database schema with a name containing invalid characters may cause a RUM upgrade to fail. For details on renaming a database schema, see "Renaming a MySQL Database Schema" on the next page.
- After upgrading to RUM 9.51, the following locations are not supported and traffic monitored from these locations is reported with an unknown location:
  - Democratic Republic of the Congo
  - United States Minor Outlying Islands
  - Republic of Macedonia
  - South Georgia and the South Sandwich Islands
  - Democratic People's Republic of Korea
- The following limitations apply to RUM data saved in the RUM MySQL database that is upgraded:
  - Snapshots are not supported.
  - Sessions that are open during the time of the upgrade will either not be available at all, or will appear as closed sessions.
  - In APM End User Management reports:
    - Entities created after the upgrade that are used in report filters cannot be applied to upgraded RUM data.
    - In the Session Analyzer report, the location field is empty for locations that do not have any related cities.
    - The following reports will not include upgraded RUM data:

      RUM Action Summary, when filtered by transactions, end-user groups, events, or locations.

      RUM Transaction Summary, when filtered by transactions with threshold violations or by end-user groups.

Production Analysis reports, when filtered by transactions with threshold violations.

RUM Session Analyzer, when filtered for the past week (that includes upgraded data) for a single transaction.

Renaming a MySQL Database Schema

The only valid characters for use when naming a MySQL database schema are letters, digits, and the underscore character (_). A schema name that contains other characters may prevent you from successfully upgrading RUM. If your schema name contains invalid characters, rename it so that only valid characters are used.

If you have already uninstalled the RUM Engine as part of an upgrade, but cannot successfully connect to the old database schema, carry out all of the steps in the following procedure. If you have not yet uninstalled the RUM Engine, start from step 3 and carry out all the subsequent steps.

To rename a MySQL database schema

1. Copy the installation files for the old RUM Engine (from which you are upgrading and which match the old database schema version) to the machine on which the old schema is located.

   Note: If you do not have access to the old RUM Engine installation files, continue with step 2 below.

   a. Run the RUM Engine setup file and when prompted, select “Real User Monitor – Custom installation” (distributed).
   b. Select the “RUM – DB” component and continue with the installation.
   c. In the Configuration Wizard:
      - Select “Do not import” user configuration data.
      - Enter the path for the new MySQL database schema.
      - Use the same MySQL credentials that were configured in the previous RUM installation from which you are upgrading.
   d. When the installation is complete, select **Start Menu > Administrative Tools > Services** and stop the MySQL service.
   e. Edit the **\<Real User Monitor root directory>\MySQL\rum_options.ini** file, and ensure that in the **[mysqld]** section, the value for the **datadir** paramater is the path to the old HPRUM_DATA folder.
   f. Navigate to the old <datadir> folder (default HPRUM_DATA) and manually delete the **ib_logfile0** and **ib_logfile1** files.
   g. Select **Start Menu > Administrative Tools > Services** and start the MySQL service.
   h. Continue with step 3 below.
2. If you do not have access to the old RUM Engine installation files, download the relevant MySQL service from the MySQL website. To determine the correct MySQL version number, search for **version** in the **<datadir>\<HOST-NAME>.err** file.
   a. Copy the MySQL installation files to the machine on which the old schema is located.
   b. In a **cmd** window, navigate to the directory containing the downloaded MySQL installation files (for example, `cd "C:\Program Files\MySQL\MySQL Server 5.1\bin\"`).
   c. Run the command `mysqld --install MySQL --defaults-file==<RUM export directory>\MySQL\rum_options.ini`.

When completed, the message "`service successfully installed`" is displayed.

d. Navigate to the old <datadir> folder and manually delete the **ib_logfile0** and **ib_logfile1** files.

e. In the **cmd** window, start the mysql service with the command `net start mysql`.

When the mysql service is running, the message "`the mysql service was started successfully`" is displayed.

3. Ensure that the MySQL service is started. (Open the **Task Manager** and in the **Services** tab, verify that the MySQL service is **Running**.)
4. Open any mysql editor (for example, dbeaver or mysql workbench) and connect to the old (badly named) schema.
5. Open a query tab and run the following script (if successful, a **rename_database** folder is created under **Routines**):

```
DELIMITER $$
DROP PROCEDURE IF EXISTS rename_database $$
CREATE PROCEDURE rename_database(oldSchemaName VARCHAR(64), newSchemaName
VARCHAR(64))
BEGIN
DECLARE done INT DEFAULT 0;
DECLARE tableName VARCHAR(64);
DECLARE tableListCursor CURSOR FOR
SELECT TABLE_NAME
FROM INFORMATION_SCHEMA.TABLES
WHERE TABLE_SCHEMA=oldSchemaName
ORDER BY TABLE_NAME;
DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET done = 1;
SET @createNewSchema = CONCAT_WS('', ' CREATE DATABASE ', newSchemaName);
PREPARE statement from @createNewSchema;
EXECUTE statement;
DEALLOCATE PREPARE statement;
OPEN tableListCursor;
REPEAT
FETCH tableListCursor INTO tableName;
IF NOT done THEN
SET @moveTable = '';
SET @moveTable = CONCAT_WS('', @moveTable, ' RENAME TABLE ' , '`', old
DatabaseName, '`', '.', tableName, ' \n');
SET @moveTable = CONCAT_WS('', @moveTable, ' TO ', '`', newDatabaseNam
e, '`', '.', tableName, ' \n');
PREPARE statement from @moveTable;
EXECUTE statement;
DEALLOCATE PREPARE statement;
END IF;
UNTIL done END REPEAT;
CLOSE tableListCursor;
END $$
```

6. Open another query tab and run the following script (if successful, a new schema is created and data is moved from the old schema to the new one, leaving the old schema empty):

```
call rename_database('<BAD SCHEMA NAME>','<NEW GOOD SCHEMA NAME>');
```

7. After the schema has been successfully renamed:
   - If you carried out step 1 of this procedure, uninstall the RUM database component using the Control Panel (**Control Panel > Programs > Uninstall Real User Monitor**).
   - If you carried out step 2 of this procedure, uninstall the MySQL service by running the command `sc delete "MySQL"` in a **cmd** window, and then restarting the machine.
8. Continue with the RUM upgrade and when prompted, connect to the new, renamed schema.

Linux Installer Troubleshooting

The Linux installer requires full access to the default temporary directory (the /tmp directory). If this directory is restricted in any way (for example because of security requirements) you should choose a different temporary directory with full access before running the installer.

How to Change the Installer Working Directory

In Linux, you can change the Installer's working directory (by default /tmp) by running the following commands:

```
export IATEMPDIR=/new/tmp
```

```
export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp
```

where `/new/tmp` is the new working directory.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Real User Monitor Installation and Upgrade Guide (Real User Monitor 9.51)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to feedback@microfocus.com.

We appreciate your feedback!