

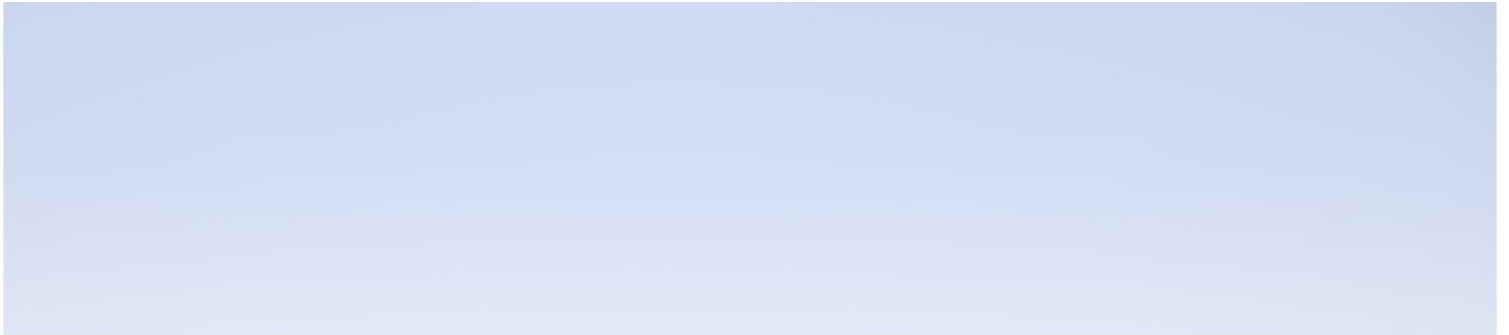


# Real User Monitor

Version 9.50, Released May 2018

## Real User Monitor Administration Guide

Published May 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 Administration Overview .....	9
Part 1: RUM Introduction and Compatibility .....	10
Chapter 1: Introducing RUM Administration .....	11
Overview of RUM .....	11
How RUM Works .....	11
Ports Used by RUM .....	12
Overview of RUM Performance Measurements .....	13
Introduction to Performance Measurements .....	14
TCP Request-Response Measurements .....	14
HTTP Measurements .....	15
Page Performance Measurements .....	15
Component Measurements .....	16
Page Measurements .....	16
Transaction Measurements .....	17
End User Measurements .....	18
Installing and Administering RUM .....	20
Chapter 2: RUM Compatibility Matrixes .....	21
RUM-APM Compatibility Matrix .....	21
RUM Probe-RUM Engine Compatibility .....	21
Part 2: Data Collection Methods .....	22
Chapter 3: RUM Data Collection Methods .....	23
Chapter 4: Data Collection Using a Network Tap or Switch Configuration .....	25
Chapter 5: Sniffing Using the RUM Server Collector .....	26
Configuring the RUM Server Collector .....	26
Configuring the RUM Sniffer Probe .....	27
Administering the RUM Server Collector Service .....	28
RUM Server Collector Log File .....	28
Chapter 6: RUM Client Monitor Probe .....	30
Using the RUM Client Monitor Solution to Monitor Web Applications .....	30
Using the RUM Mobile Solution to Monitor Mobile Applications .....	33
Part 3: Configuring and Administering Real User Monitor .....	36
Chapter 7: Administering the RUM Engine .....	37
Administering RUM Monitor .....	37
RUM Logs .....	38
Chapter 8: Using the RUM Web Console .....	40
Accessing the RUM Engine Web Console .....	40
Logging In .....	40

Logging Out .....	41
Changing Login Parameters .....	41
Changing the Language of the RUM Web Console User Interface .....	42
Changing Timeout Parameters .....	43
Monitoring the Health of RUM Components .....	43
System Health .....	43
Configuration Retrieval From APM Server .....	44
Database .....	45
RUM Sniffer Probe .....	47
RUM Client Monitor Probe .....	69
RUM Engine .....	75
Samples to APM Server .....	85
Data Access Layer .....	86
Partition Manager .....	88
Topology Engine .....	88
Missing Mirrored Data .....	93
Capture Log Files .....	93
RUM Configuration and Settings .....	93
APM Connection Settings .....	94
Docker Host Management .....	97
Action Buttons .....	97
Host Configuration Dialog Box .....	98
Docker Pattern Filter Settings .....	101
Docker Probe Management .....	102
Probe Management .....	103
Action Buttons .....	103
Probe Configuration Dialog Box .....	105
Probe Traffic Discovery .....	107
Common Elements .....	108
Summary View Tab .....	108
Domain View/Server View Tabs .....	109
SSL Keystore Management .....	110
Interface Configurations .....	113
Server Filter Settings .....	114
Probe Traffic Capture .....	115
Session ID Detection .....	117
Configuring Applications in End User Management Administration Using Traffic Discovery and Session ID Detection .....	117
Session ID Detection Page .....	117
Session ID Detection Report .....	118
Advanced Settings .....	121

Data Flow Probe Connection Settings .....	121
System Info .....	122
RUM Diagnostics Tools .....	122
Monitoring Configuration Information .....	123
Applications .....	123
End Users .....	124
Events .....	124
Pages .....	125
Probes .....	125
Transactions .....	126
Engine Settings .....	127
Transaction Snapshot Mode .....	128
JMX Console .....	128
IP Translator .....	128
Time Converter .....	128
Mobile Application Instrumentation .....	129
Signing an APK using Java's jarsigner.exe Tool .....	132
Chapter 9: Using the JMX Console to Configure the RUM Engine .....	133
Using the RUM JMX Console .....	133
Accessing the JMX Console .....	133
Setting URL Correlation Parameters .....	134
Configuring RUM Aggregation .....	134
Configuring the Samples Rate .....	136
Configuring the Amount of Unsent Sample Data to Store in RUM .....	136
Configuring the Classification Type .....	137
URL Correlation Parameters .....	139
Setting URL Correlation Parameters Via the JMX Console .....	139
Correlating Session ID Parameters .....	140
Chapter 10: RUM Engine File Configuration .....	142
Configuring Meaningful Page Names .....	142
About Discovered Page Names .....	142
Formatting Tags .....	143
URL Decoder .....	143
Rename .....	144
Substring .....	144
ExtractStrToStr .....	144
ExtractIndexToStr .....	145
ExtractStrToCount .....	146
Insert .....	147
ChangeCase .....	148
Remove .....	148

RemoveNonAlpha .....	148
Replace .....	149
Alias .....	149
RegExExtract .....	150
RegExMatch .....	150
Rule Tags .....	151
Sample XML File .....	153
Validating Meaningful Name XML Files .....	158
Adding and Deleting Meaningful Name XML Files .....	159
Changing Meaningful Name XML Files .....	159
Viewing Discovered Page Statistics .....	159
Unifying Frames .....	160
Configuring User Name Translation .....	162
Chapter 11: Configuring the RUM Sniffer Probe .....	164
Changing the Protocol for Accessing the RUM Probe .....	164
Configuring the RUM Probe for I18N .....	164
Changing the Header in Which to Locate Client IP Addresses .....	165
Creating Default Configuration and Properties Files for a Specific Probe .....	165
Configuring the RUM Probe to Support Multiprotocol Label Switching (MPLS) .....	166
Configuring the RUM Probe to GRE Support Encapsulated Remote Switch Port Analyzer (ERSPAN) .....	166
Configuring the RUM Probe if Extended Master Secret Exists in SSL Handshake .....	166
Chapter 12: Administering the MySQL Database .....	168
Overview of the MySQL Database .....	168
Creating and Connecting to the MySQL Database .....	168
Starting and Stopping the MySQL Database .....	169
Changing the MySQL Database User Password .....	169
Maintaining the MySQL Database .....	170
Chapter 13: Hardening RUM .....	172
Hardening the RUM Sniffer Probe .....	172
Changing the Probe's User and Password .....	172
Limiting Access to the Probe .....	173
Limiting the SSH Version .....	173
Securing the HTTP Connection to the Probe .....	173
Securing Connections to the RUM Engine .....	175
Using Authentication .....	176
Using HTTPS .....	176
Chapter 14: Deploying RUM in a SiteMinder Environment .....	178
Overview .....	178
Prerequisites .....	178
System Flow .....	179

Configuring the SiteMinder Policy Server .....	179
Create an Agent .....	180
Create the Agent Conf Object .....	180
Create the Authentication Scheme .....	180
Configure the Domain .....	181
Installing and Configuring the SiteMinder Web Agent .....	183
Configuring the Web Server .....	184
Configuring IIS to Work with RUM .....	184
Configuring IIS to Work with the SiteMinder Web Agent .....	187
Configuring the RUM Engine .....	188
Changing the Configuration of the TCP Port .....	188
Testing and Troubleshooting .....	189
RUM Engine .....	189
SiteMinder Web Agent .....	190
Mirror Servlet .....	190
Chapter 15: RUM Data Export .....	191
Enable Data Export .....	191
How Data is Exported .....	191
Data Export XML File .....	192
Valid Channel Types and Fields .....	195
Page .....	195
Transaction .....	199
Session .....	201
Action .....	204
Event .....	207
Chapter 16: RUM Integrations .....	209
RUM Integration with Operations Analytics .....	209
RUM Integration with Performance Center .....	209
<b>Part 4: Supporting Specific Protocols .....</b>	<b>210</b>
Chapter 17: Parsing Supported Protocols .....	211
TCP Level Information .....	212
HTTP .....	213
SOA .....	217
Databases .....	218
Application Servers .....	223
Mailing Applications .....	231
Generically Supported Protocols .....	233
Financial Protocols .....	236
Additional Applications .....	239
Application Suites .....	241
Oracle E-Business .....	241

Citrix Solutions .....	241
View Data for Citrix Sessions .....	241
Extending Protocol Coverage .....	242
Chapter 18: Customizing Error Codes for SAPGUI .....	243
Chapter 19: NDC Protocol Configuration .....	245
NdcOperationInfo.csv .....	245
NdcTerminalInfo.csv .....	245
ndc.def .....	246
Chapter 19: RUM Probe Textual Protocol Configuration .....	246
Textual Protocol Parser Configuration .....	246
Chapter 19: Diebold ATM Protocol Configuration .....	248
NdcOperationInfo.csv .....	249
NdcTerminalInfo.csv .....	249
ndc.def .....	249
Chapter 20: Monitoring Citrix with RUM .....	251
Overview of Citrix Monitoring with RUM .....	251
Overview of the RUM VDI Agent .....	252
Configurations for Working with the RUM VDI Agent for HTTP Traffic .....	253
Advanced Configuration for HTTP Traffic .....	255
Using the RUM VDI Agent with Terminal Services for HTTP Traffic .....	257
Chapter 21: Supporting ISO8583 Based Protocols .....	258
ISO8583 Message Format .....	258
RUM Sniffer Probe Configuration Files .....	258
Configuration .....	259
Message Length .....	260
Padding .....	261
Header .....	261
Default Visa Header .....	261
MTI .....	261
Bitmap .....	262
Data_fields .....	262
Encoding .....	262
Troubleshooting RumProbe - ISO8583 Protocol .....	262
Send Documentation Feedback .....	264



# Real User Monitor Administration Overview

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

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

**Note:** If you are 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 Introduction and Compatibility" on page 10](#)  
Introduces RUM and explains how it works.
- ["Data Collection Methods" on page 22](#)  
Describes the different methods by which the RUM Probe can obtain monitored data.
- ["Configuring and Administering Real User Monitor" on page 36](#)  
Explains how to configure a RUM Probe by changing the default settings, as well as how to configure and administer the RUM Engine and how to administer RUM's MySQL database. Also provides guidelines for hardening RUM, deploying RUM in a SiteMinder environment, and publishing RUM data.
- ["Supporting Specific Protocols" on page 210](#)  
Explains how to configure and work with RUM for monitoring specific protocols.

# Part 1: RUM Introduction and Compatibility

# Chapter 1: Introducing RUM Administration

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

This chapter includes the following topics:

- ["Overview of RUM" below](#)
- ["How RUM Works" below](#)
- ["Ports Used by RUM" on the next page](#)
- ["Overview of RUM Performance Measurements" on page 13](#)
- ["Installing and Administering RUM" on page 20](#)

## Overview of RUM

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

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

## How RUM Works

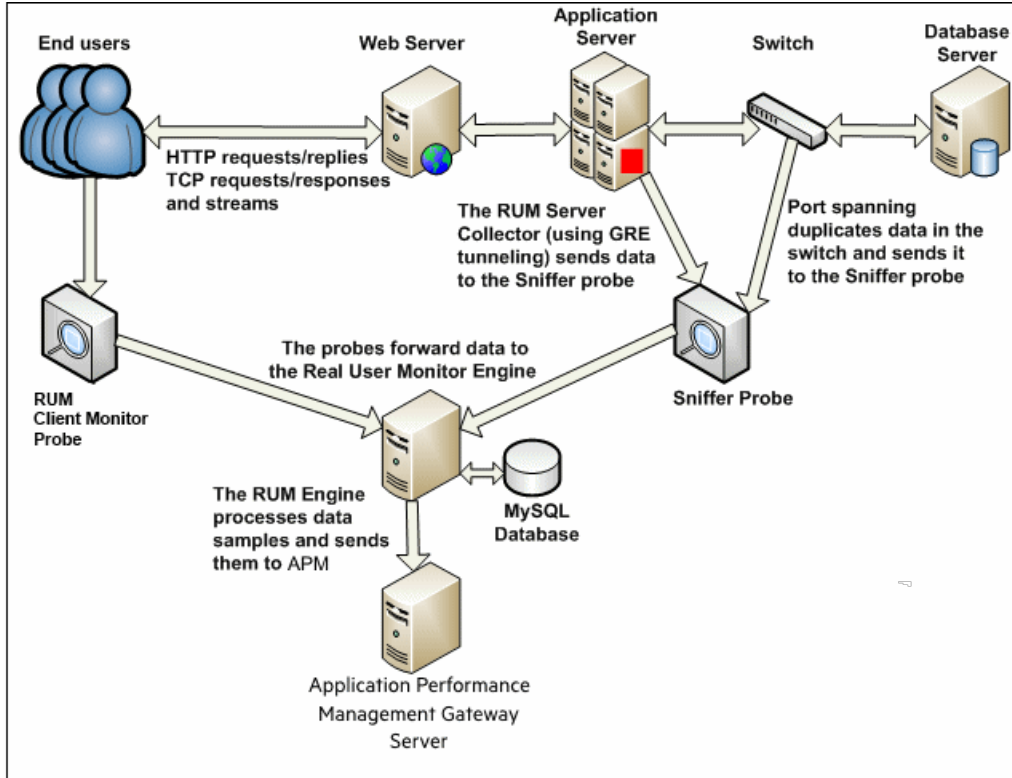
RUM consists of three major components: the probe, the engine, and the MySQL database.

- The **probe** receives data on end-user experience and/or applications, carries out initial processing on this data, and sends it to the RUM Engine. There are two types of probe:
  - **Sniffer Probe** - a non-intrusive, passive listening device that is subject to the same traffic the server receives. The traffic can be collected in a number of different ways. For details, see ["RUM Data Collection Methods" on page 23](#).
  - **RUM Client Monitor Probe** - collects user experience data directly from the client, for monitored web or mobile applications. For details, see ["RUM Client Monitor Probe" on page 30](#).
- The **engine** receives the data collected by the probe and assembles this data according to the configuration specifications it receives from Application Performance Management (APM), that have been configured in End User Management Administration. The engine transmits the page, transaction, end-user, and server data samples it creates to the APM Gateway Server. The APM Gateway Server then distributes the data to the relevant APM components, which create RUM alerts, reports, and Service Health views.

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

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

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

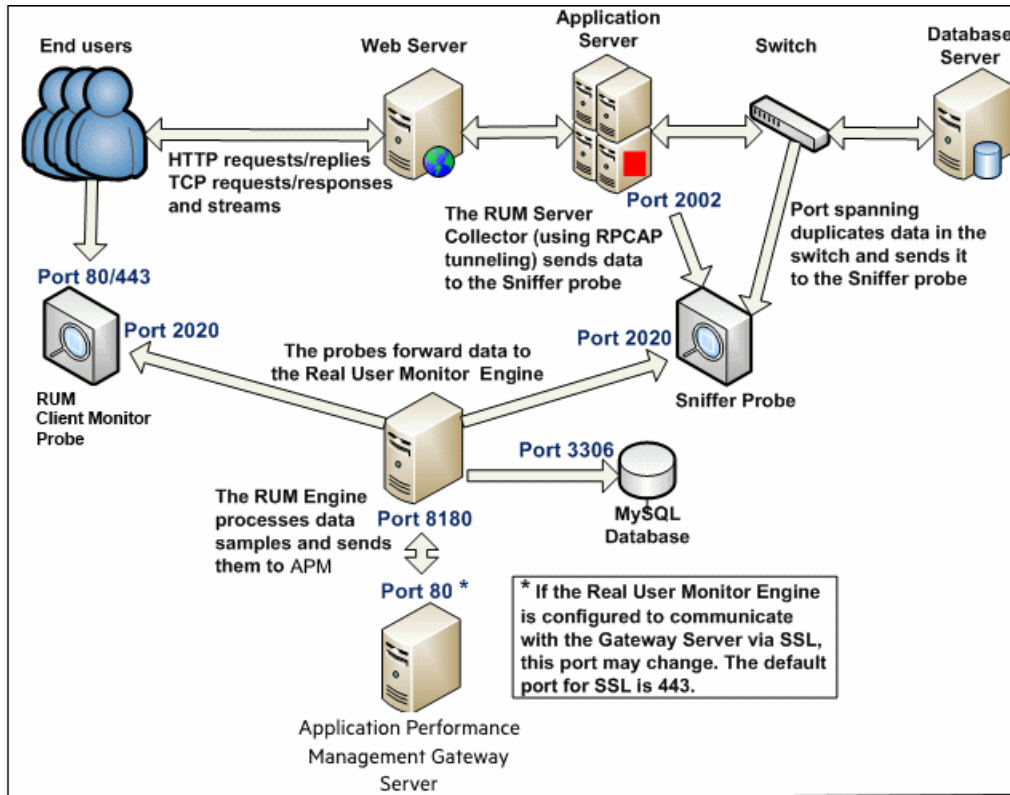


Use the EUM reports to analyze network and application performance and availability data for the servers, applications, pages, transactions, events, and end users that you configure for monitoring, as well as general statistics that are collected and sent by the probes to the engine. When notified by an alert that a certain performance or availability threshold has been exceeded, you can examine the issue in the appropriate reports and try to pinpoint the cause of the problem and the time at which the problem occurred. For detailed information on EUM reports, see "End User Management Reports Overview" in the APM User Guide.

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

## Ports Used by RUM

The following diagram shows the various ports used by RUM:



**Note:**

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

## Overview of RUM Performance Measurements

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

This section includes the following topics:

- ["Introduction to Performance Measurements" on the next page](#)
- ["TCP Request-Response Measurements" on the next page](#)

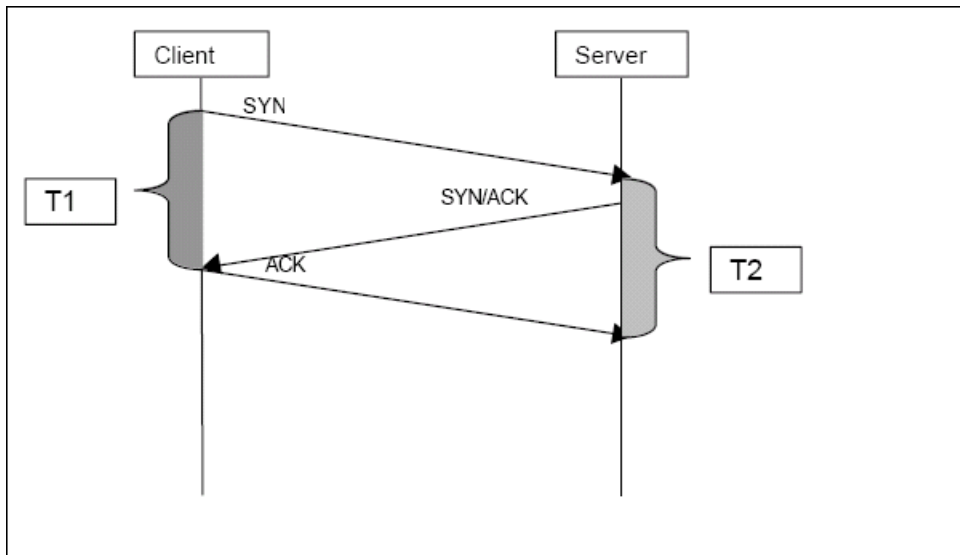
- ["HTTP Measurements" on the next page](#)
- ["End User Measurements" on page 18](#)

## Introduction to Performance Measurements

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

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

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



## TCP Request-Response Measurements

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

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

arrive are incorporated into the network time. RUM measures what part of the network time is due to network errors.

## HTTP Measurements

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

This section includes the following topics:

- ["Page Performance Measurements" below](#)
- ["Component Measurements" on the next page](#)
- ["Page Measurements" on the next page](#)
- ["Transaction Measurements" on page 17](#)

## Page Performance Measurements

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

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

## Component Measurements

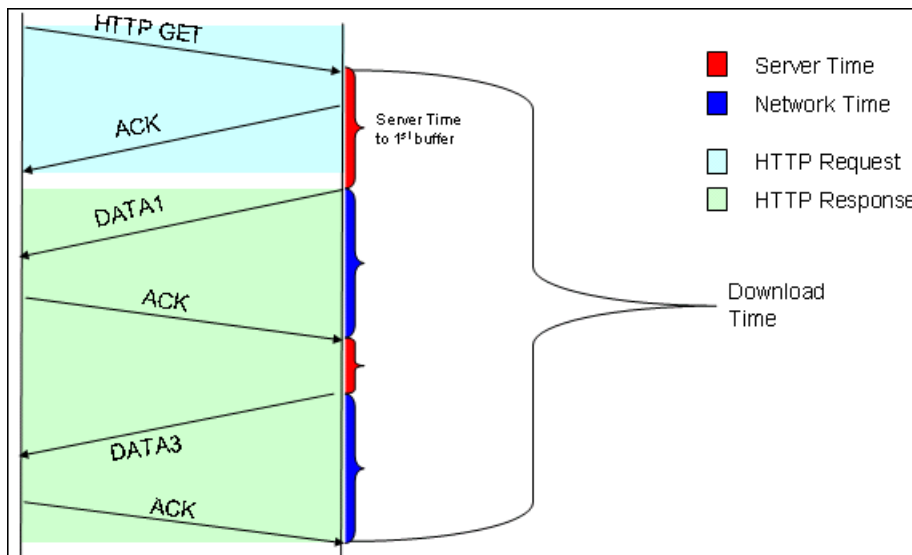
It is important to understand component measurements as they form an integral part of page and transaction measurements.

An http component is a single request response couple.

The following component measurements are used in RUM:

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

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



## Page Measurements

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

The following page measurements are used in RUM:

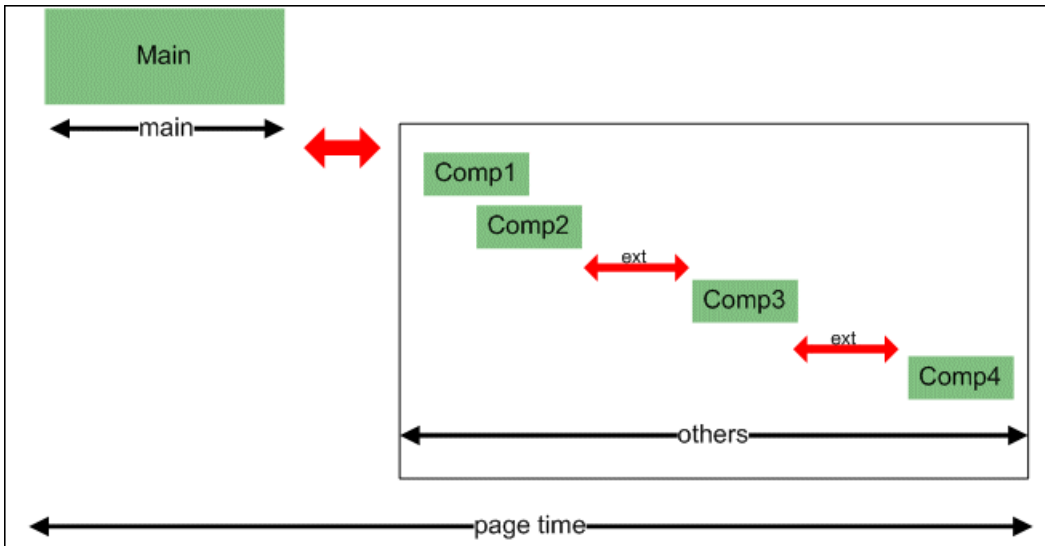
- **Page time.** The time from the first packet of the first component's request to the client ack for the last packet of the last component's response. Page time comprises page client/external time, page network



time and page server time.

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

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



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

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

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

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

## Transaction Measurements

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

The following transaction measurements are used in RUM:

- **Transaction Total Time.** The time from the beginning of the download of the first page until the end of the download of the last page.
- **Transaction Net Time.** The portion of the total time that was actually spent downloading the pages. This calculation excludes gaps between the pages, which are considered as user think time. Transaction net time comprises the following measurements:

- **Transaction Server Time.** The relative part of net time that was spent on server processing. This is calculated considering the server time of the pages. Server time is counted only once for pages that have overlapping sever time. Transaction server time = net transaction time \* (total server time / total download time).
- **Transaction Network Time.** The relative part of net time that was spent on network transportation. This is calculated considering the network time of the pages. Network time is counted only once for pages that have overlapping network time. Transaction network time = net transaction time \* (total network time / total download time).
- **Transaction Client/External Time.** The relative part of net time during which no server processing or network transportation took place (that is, the gaps between components), usually due to client processing. This is calculated considering the client time of the pages. Client time is counted only once for pages that have overlapping client time. Transaction client time = net transaction time \* (total client time / total download time).

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

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

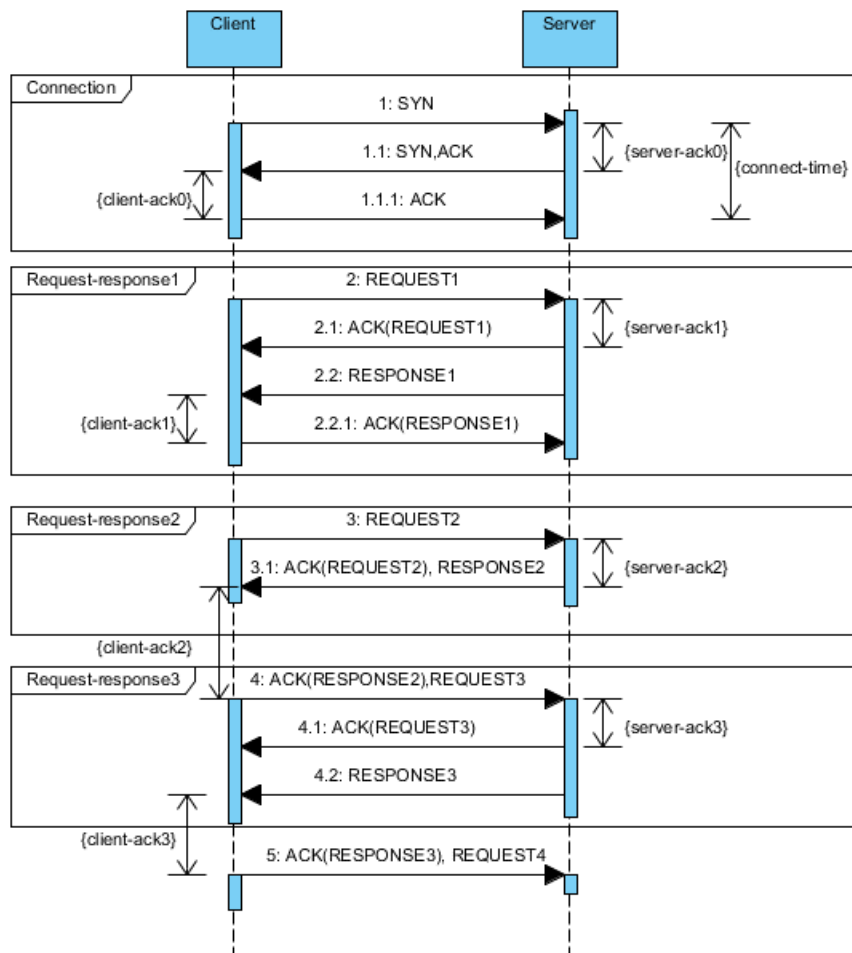
It is possible for a transaction’s server, network, or client time to be less than the individual server, network, or client time of one of its included pages. This can occur when the download time of the pages included in the transaction overlap, but register different measurements for the same time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

## End User Measurements

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

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

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



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

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

The following ACK durations are not considered in the calculation:

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

The latency for the connection is calculated as:

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

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

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

# Installing and Administering RUM

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

## **Install the RUM Engine.**

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

## **Create and connect to the MySQL database.**

You can create and connect to the MySQL database either as part of the RUM Engine installation procedure or separately, at a later time. For details on creating the MySQL database as part of the RUM Engine installation procedure, see "Installing the RUM Engine" in the Real User Monitor Installation and Upgrade Guide. For details on creating the MySQL database at a later time, see ["Overview of the MySQL Database" on page 168](#).

## **Install one or more RUM Probes.**

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

## **If necessary, reconfigure the connection between RUM and APM.**

If connection parameters (such as SSL, proxy, and authentication) have changed since the installation of APM, use the RUM Engine's web console to reconfigure the connection between RUM and APM. For detailed information, see ["Using the RUM Web Console" on page 40](#).

## **Configure RUM in APM End User Management Administration.**

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

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

# 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 9.50	✓	✓	✓	✓	✓
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: Data Collection Methods

# Chapter 3: RUM Data Collection Methods

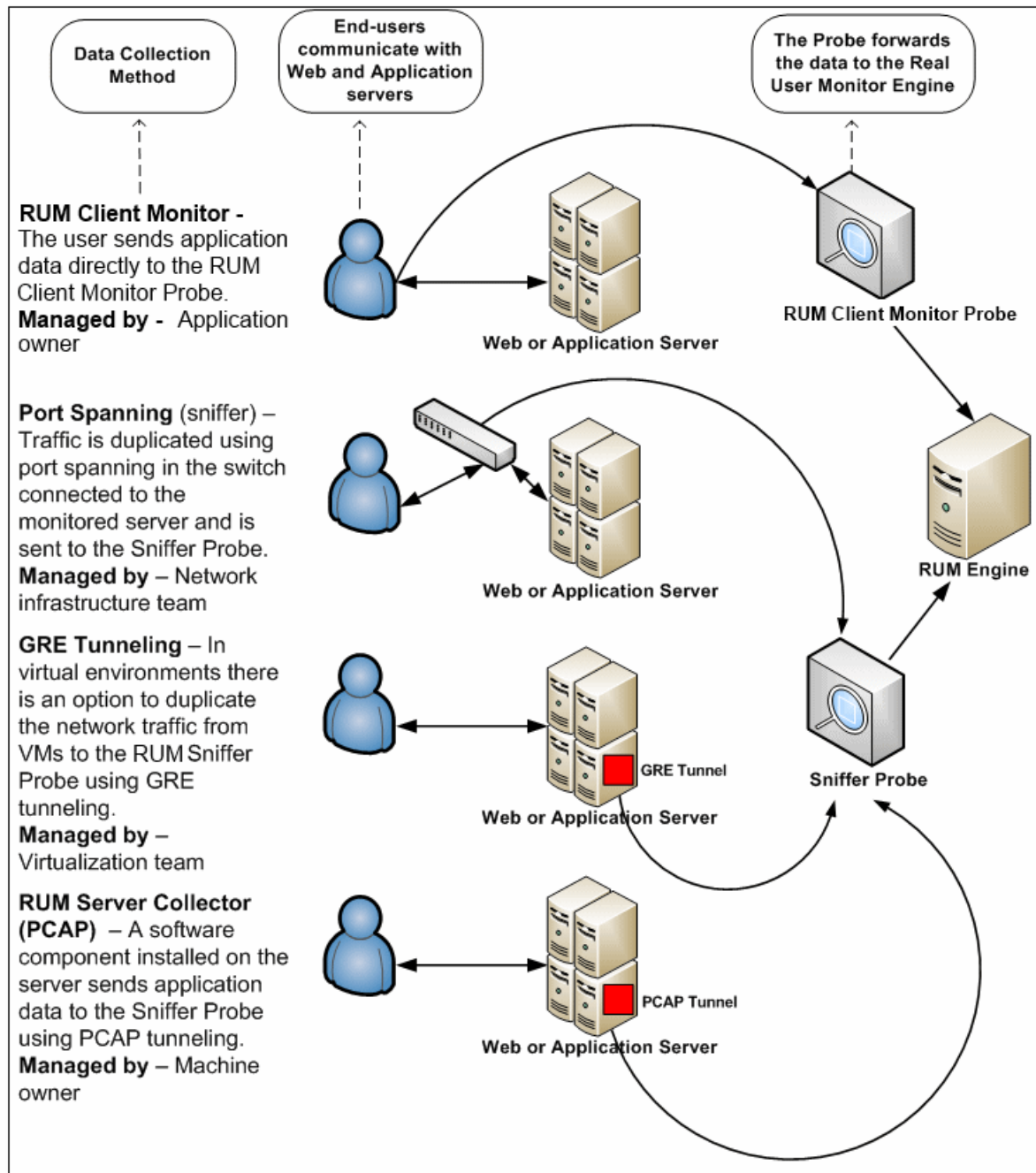
There are a number of ways by which the RUM Probe can obtain data for monitored applications. The available monitoring solutions depend on the type of RUM Probe you use:

- **Sniffer Probe** data collection methods:
  - **Network tap or switch configuration.** For details, see ["Data Collection Using a Network Tap or Switch Configuration"](#) on page 25.
  - **RUM Server Collector.** For details, see ["Sniffing Using the RUM Server Collector"](#) on page 26.
  - **VMware.** For details see Duplicating Traffic for RUM with VMware in the RUM Deployment Guide.
- **RUM Client Monitor Probe.** For details, see ["RUM Client Monitor Probe"](#) on page 30.

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

For information on how RUM protects the collected data, contact Support.

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



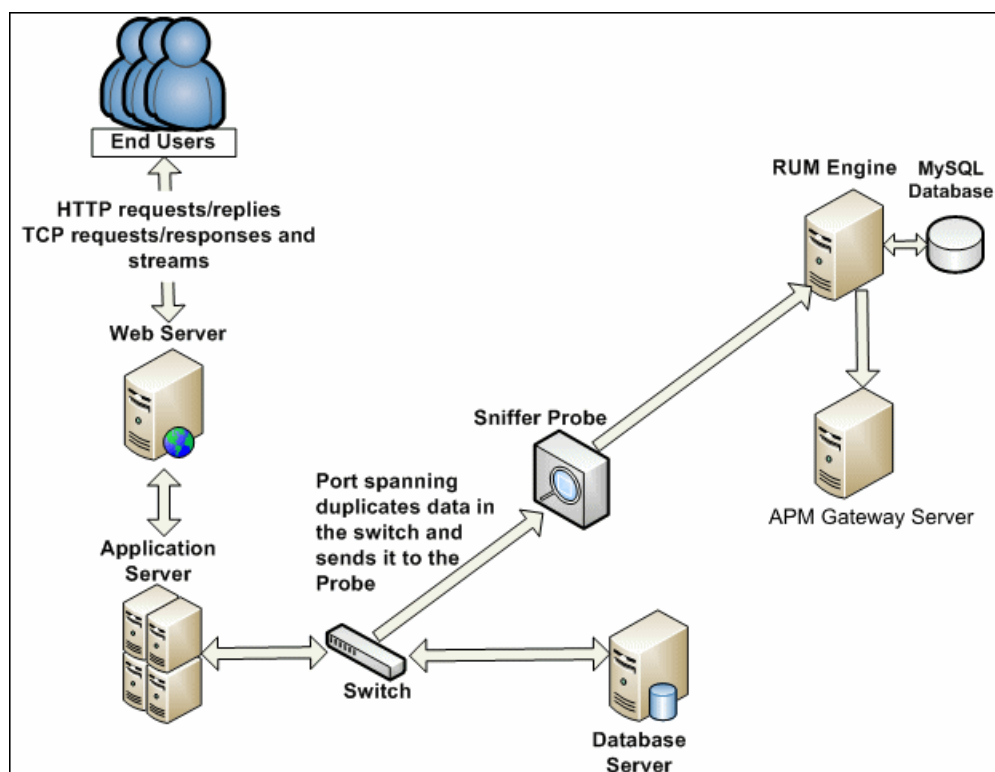


# Chapter 4: Data Collection Using a Network Tap or Switch Configuration

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

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

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



# Chapter 5: Sniffing Using the RUM Server Collector

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

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

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

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

To work with the RUM Server Collector, you must:

1. Install the RUM Sniffer Probe. For details, see "Installing the RUM Sniffer Probe" in the Real User Monitor Installation and Upgrade Guide.
2. Install the RUM Server Collector on the server you want to monitor. For details, see "Installing the RUM Server Collector" in the Real User Monitor Installation and Upgrade Guide.
3. Configure the RUM Server Collector. For details, see ["Configuring the RUM Server Collector" below](#).
4. Configure the RUM Sniffer Probe to retrieve data from the RUM Server Collector. For details, see ["Configuring the RUM Sniffer Probe" on the next page](#).
5. Start the RUM Server Collector service. For details, see ["Administering the RUM Server Collector Service" on page 28](#).

## Configuring the RUM Server Collector

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

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

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

- **Windows:** <RUM Server Collector installation directory>\etc\rum\_collector\  
(The default RUM Server Collector installation directory is C:\RUMSC)
- **Linux:** <RUM Server Collector installation directory>/etc/rum\_collector/  
(The default RUM Server Collector installation directory is /opt/Micro Focus/RUMSC)

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

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

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

- **Security.** By default, the RUM Server Collector is configured to enforce SSL connectivity. You can change this by setting the **use\_ssl** parameter in the **[security]** section of the file to **false**.  
The default security keys and certificates used by the RUM Server Collector for SSL connections are predefined. If you want to use different keys and certificates, you must update the following parameters in the **[security]** section of the file:

- **ssl\_ca\_file.** The full path to the certificate file used to validate the client certificate sent by the probe.
- **ssl\_key.** The full path to the private key file used for accepting server SLL connections from the probe.
- **ssl\_cert.** The full path to the certificate file used for accepting server SLL connections from the probe.

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

## Configuring the RUM Sniffer Probe

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

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

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

To configure the RUM Sniffer Probe to connect to the RUM Server Collector to retrieve data, on the RUM Engine edit the `\RUM\conf\configurationmanager\Beatbox_<Sniffer Probe name>_Const_Configuration.xml` file.

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

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

where:

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

#### Examples:

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

## Administering the RUM Server Collector Service

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

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

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

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

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

## RUM Server Collector Log File

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

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

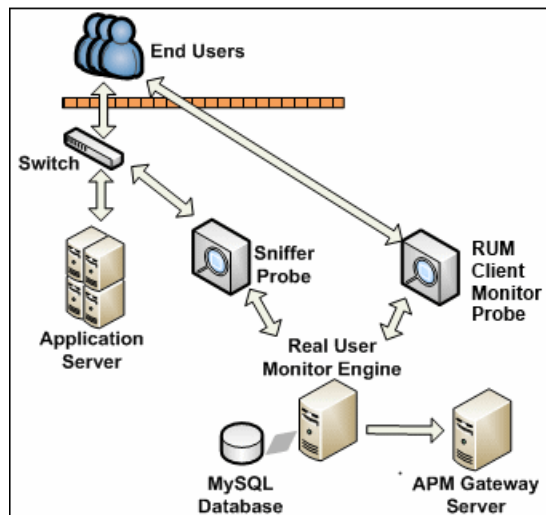
**Linux:** `<RUM Server Collector installation directory>/var/log/rum_collector/collector.log`

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

# Chapter 6: RUM Client Monitor Probe

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

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



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

- The RUM client monitor solution enables you to monitor web applications through an end user's Internet browser. For details, see ["Using the RUM Client Monitor Solution to Monitor Web Applications" below](#).
- The RUM mobile solution enables you to monitor mobile applications through an app on an end user's mobile device. For details, see ["Using the RUM Mobile Solution to Monitor Mobile Applications" on page 33](#).

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

When monitoring mobile applications using Client Monitor Probes, RUM Engine creates a Running Software CI. This CI is not labeled with an IP address since it is situated on the client side and RUM cannot determine the server IP address. Therefore, RUM labels the CI with the application domain. When a crash occurs, RUM cannot retrieve the domain name so the CI is labeled as *application name\_crash*. You can filter out these mobile application Running Software CIs.

## Using the RUM Client Monitor Solution to Monitor Web Applications

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

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

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

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

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

This section includes the following topics:

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

## Supported Browsers

The RUM client monitor solution supports the following Internet browsers:

- Internet Explorer
- Google Chrome
- Firefox
- Safari
- Opera

## Getting Started with the RUM Client Monitor Probe

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

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

## Configuring Applications in APM for the RUM Client Monitor Solution

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

Configuration Setting	Configured In	Remarks
<b>Session Properties</b>	RUM Session Page > Session Properties Area	You must configure the following session properties, although apart from the name, the rest of the session property settings are not used: <ul style="list-style-type: none"> <li>• Operating System</li> <li>• Browser</li> </ul>
<b>User Name Detection</b>	RUM Application General Page > User Name Detection Area	N/A. User name detection can be configured in the JavaScript snippet.
<b>Parameter Extraction</b>	RUM Application General Page > Parameter Extraction Area	N/A
<b>TCP Settings</b>	RUM Application General Page > TCP/Network Settings Area	N/A. TCP data is not reported for applications configured for the RUM Client Monitor Probe.
<b>Session ID</b>	RUM Session Page > Session Identification Area	N/A. The RUM Client Monitor Probe uses its own mechanism for user session tracking.
<b>Exclude BPM Data</b>	RUM Data Collection Page > General Area	N/A
<b>Sensitive Data</b>	RUM Data Collection Page > Sensitive Data Area	N/A
<b>Snapshots</b>	RUM Data Collection Page > Snapshot Collection Area	N/A
<b>Events</b>	RUM Application Events Page	The following events are applicable to applications monitored by the RUM Client Monitor Probe: <ul style="list-style-type: none"> <li>• <b>Error Page</b></li> <li>• <b>Text Pattern</b> - you configure the name of the text pattern event in EUM, but define the actual text pattern settings in the JavaScript snippet.</li> <li>• <b>Session Pages</b></li> <li>• <b>Page Size</b> - the RUM Client Monitor Probe cannot always determine page size.</li> <li>• <b>Page Time</b></li> </ul> All other events are not applicable to applications monitored by the RUM Client Monitor Probe.



# Using the RUM Mobile Solution to Monitor Mobile Applications

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

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

This section includes the following topics:

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

## Supported Operating Systems

The RUM mobile solution supports the following operating systems:

- Android 2.2 and later
- iOS 5 and later

## Supported Libraries

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

- iOS
  - NSURLConnection (NSURLSession)
  - AFNetworking
  - UIWebView and WKWebView
- Android
  - HttpURLConnection
  - ApacheHttpClient
  - MultiDex
- HTML5 (in Hybrid applications)
  - Page load time - Android version 4 and up only
  - Ajax

## Getting Started with the RUM Client Monitor Probe

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

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

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

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

### Configuring Applications in APM for the RUM Mobile Solution

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

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

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

<b>Configuration Setting</b>	<b>Configured In</b>	<b>Remarks</b>
<b>Session ID</b>	RUM Session Page > Session Identification Area	N/A. The RUM Client Monitor Probe uses its own mechanism for user session tracking.
<b>Exclude BPM Data</b>	RUM Data Collection Page > General Area	N/A
<b>Sensitive Data</b>	RUM Data Collection Page > Sensitive Data Area	N/A
<b>Snapshots</b>	RUM Data Collection Page > Snapshot Collection Area	N/A
<b>Events</b>	RUM Application Events Page	N/A

# Part 3: Configuring and Administering Real User Monitor

# Chapter 7: Administering the RUM Engine

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

This chapter includes the following topics:

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

## Administering RUM Monitor

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

This section includes the following topics:

- ["RUM Windows Start Menu" below](#)
- ["RUM Engine Nanny" below](#)

### RUM Windows Start Menu

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

#### Administration

The Administration menu option includes the following options:

Option	Description
RUM Configuration Tool	Runs the RUM Configuration Tool, which enables you to create a MySQL database schema, and to connect RUM to a MySQL database. For details, see <a href="#">"Creating and Connecting to the MySQL Database" on page 168</a> .
Database (only if the MySQL database has been installed)	Opens a submenu with options for starting and stopping the MySQL database on the machine on which it is installed.
Disable RUM	Stops RUM on the specific machine, and disables it from being run automatically whenever the machine is started.
Enable RUM	Starts RUM on the specific machine, and sets it to run automatically whenever the machine is started.

#### Open RUM Web Console

Selecting this option opens the web console used for administering RUM. For details, see ["Using the RUM Web Console" on page 40](#).

#### RUM Engine Nanny

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

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

#### To view the status of RUM:

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

## RUM Logs

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

This section includes:

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

### Engine Logs

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

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

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

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

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

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

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

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

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

## Jboss and Tomcat Logs

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

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

## Core Logs

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

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

# Chapter 8: Using the RUM Web Console

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

This chapter includes the following topics:

- ["Accessing the RUM Engine Web Console" below](#)
- ["Monitoring the Health of RUM Components" on page 43](#)
- ["RUM Configuration and Settings" on page 93](#)
- ["APM Connection Settings" on page 94](#)
- ["Probe Management" on page 103](#)
- ["Advanced Settings" on page 121](#)
- ["Data Flow Probe Connection Settings" on page 121](#)
- ["System Info" on page 122](#)
- ["RUM Diagnostics Tools" on page 122](#)

## Accessing the RUM Engine Web Console

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

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

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

**Note:** On a Windows machine on which the RUM Engine is installed, you can also access the RUM Engine web console by opening **Open Real User Monitor Web Console** on the computer's Start menu.

This section includes the following topics:

- ["Logging In" below](#)
- ["Logging Out" on the next page](#)
- ["Changing Login Parameters" on the next page](#)
- ["Changing the Language of the RUM Web Console User Interface" on page 42](#)

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

## Logging In

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



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

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

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

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

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

## Logging Out

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

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

## Changing Login Parameters

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

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

**Note:**

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

### To add a RUM user:

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

### To change a RUM user:

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

### To delete a RUM user:

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

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

## Changing the Language of the RUM Web Console User Interface

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

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

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

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

1. Select **Tools > Internet Options** and click **Languages**. The Language Preference dialog box opens.
2. Select the language in which you want to view the RUM web console.
3. If the language you want is not listed in the dialog box, click **Add** to display the list of languages. Select the language you want to add and click **OK**.

4. Click **Move Up** to move the selected language to the first row.
5. Click **OK** to save the settings.
6. Refresh the page: the RUM web console user interface is displayed in the selected language.

**Note:**

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

## Changing Timeout Parameters

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

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

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

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

## Monitoring the Health of RUM Components

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

This section includes:

- ["System Health" below](#)
- ["Capture Log Files" on page 93](#)

### System Health

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

	OK
	Minor
	Critical

	No status
---	-----------

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

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

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

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

- ["Configuration Retrieval From APM Server" below](#)
- ["Database" on the next page](#)
- ["RUM Sniffer Probe" on page 47](#)
- ["RUM Client Monitor Probe" on page 69](#)
- ["RUM Engine" on page 75](#)
- ["Samples to APM Server" on page 85](#)
- ["Data Access Layer" on page 86](#)
- ["Partition Manager" on page 88](#)
- ["Topology Engine" on page 88](#)
- ["Missing Mirrored Data" on page 93](#)

## Configuration Retrieval From APM Server

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Connection to APM server	Status of the connection to the APM Gateway Server for retrieving RUM Engine and Probe configurations	Connection to APM server is operational	N/A	Connection to APM server is not operational	Check the <RUM>/log/config.manager.log file

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Data type <type name> retrieval	Status of the last attempt to retrieve data type <type name> configuration from the APM Gateway Server	Configuration of data type <type name> successfully retrieved from APM server	N/A	Errors while trying to retrieve configuration data type <type name> from APM server	<ul style="list-style-type: none"> <li>• Check the &lt;RUM&gt;/log/config.manager.log file</li> <li>• Files in the &lt;RUM&gt;/log/configuration/dataType folder describe the configuration retrieved for each data type</li> </ul>

## Database

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Database connectivity	Status of the connectivity between the RUM Engine and the MySQL database	Connection to database OK	N/A	Connection to database not working	<ul style="list-style-type: none"> <li>• Check that the MySQL service is running.</li> <li>• Check the following files: <ul style="list-style-type: none"> <li>• &lt;RUM_DATA&gt; \&lt;hostname&gt;.err</li> <li>• &lt;RUM&gt;\log\repository.dataaccesslayer.log</li> </ul> </li> </ul>
Database free space	Percentage of free space (including free space in the tablespace) on the disk on which the MySQL database is installed	More than 4% is free.	3–4% is free.	Less than 3% is free.	<ul style="list-style-type: none"> <li>• Increase disk space</li> <li>• Remove heavy configuration items (such as snapshots, clickstream, and extracted parameters)</li> </ul>

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

## RUM Sniffer Probe

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

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



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

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

- Check the connection to the probe
- Check for errors in the <RUM>\log\config.-manager.log file

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Disk Utilization for	The RUM Probe disk utilization on a specific partition	Free disk space is sufficient	Free disk space is nearing its limit	Free disk space is insufficient	You can reduce disk size utilized by the Probe by disabling snapshot collection in EUM Administration.
Incomplete Transactions	The percentage of incomplete packets (that is, requests without responses). A high number can indicate a problem with a switch, or with a probe's network configuration.	N/A	N/A	N/A	<ul style="list-style-type: none"> <li>• If the Probe gives a response code 202, 590 or 591 and the server time is 0, see troubleshooting for Missing Mirrored Data.</li> <li>• If you are using a switch, ensure that both TX and RX are configured. You can trace this using a sniffer.</li> <li>• If the time to first buffer (the time between the request and the beginning of the response) is greater than two minutes, increase the following processor configuration values in the Probe's Beatbox_Default_Const_Configuration.xml file:                         <ul style="list-style-type: none"> <li>• encrypted_request_timeout (seconds)</li> <li>• unencrypted_request_timeout (seconds)</li> </ul>                         Create a pcap and open it with a tcp.analysis.lost_segment filter. Validate that there are no such packets.                     </li> </ul>

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

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

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

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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Packets processed sum	The total number of packets (IPv4 and IPv6) that were processed	N/A	N/A	N/A	
Packets with bad checksum	The percentage of packets with bad checksums	N/A	N/A	N/A	If the RUM Probe is on a client/server machine, edit the <RUM>\conf\configurationmanager\Beatbox_Default_Const_Configuration.xml file and in the <static_global_params> section change the global_skip_checksum value to true. The checksum is calculated only after passing the network card.
Pages Cached	The number of page views currently being cached to the RUM Probe's memory	The page rate is stable	The page rate is nearing the limit for normal caching	The page rate is too high	Verify that monitored traffic does not exceed sizing recommendations.
Pages Channel Processing Delay	Displays the difference between the time a page hit was received by the probe to when it was reported to the RUM Engine	N/A	N/A	N/A	<ul style="list-style-type: none"> <li>• Check that the number of pages/sec is within Engine sizing guidelines.</li> <li>• The connection between the Engine and the Probe is slow, or the Engine needs a lot of time to connect to the Probe using SSH:                             <ul style="list-style-type: none"> <li>• Check the bandwidth between the Engine and the Probe.</li> <li>• Check the &lt;RUM&gt;\log\btretriever.log file.</li> </ul> </li> </ul>



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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe and Engine Time Difference	Displays the status of the time synchronization between the RUM Engine and Probe	The RUM Engine and Probe are in sync	The RUM Engine and Probe are slightly out of sync	The RUM Engine and Probe are grossly out of sync	<ul style="list-style-type: none"> <li>Compare system time and time zone on the APM, RUM Engine, and RUM Probe servers. They should display the current time +/- 2 minutes.</li> <li>If the APM server is deployed on a virtual machine (VM), check the APM Gateway JMX:                      (<code>http://&lt;APM_Gateway_Server&gt;:29000/mbean?objectname=Mercury%3AService%3DDate%2FTime+Manager</code>).</li> </ul> <p>The GMTTime should display the current time in terms of GMT+0. An incorrect time indicates a time drift on the ESX server hosting the VM.</p> <p>To resolve this problem:</p> <ul style="list-style-type: none"> <li>Contact the ESX server admins. or</li> <li>Resolve the time difference locally on the RUM Engine as follows:                             <ol style="list-style-type: none"> <li>In a text editor, open the file <code>&lt;RUM&gt;\conf\common\common.properties</code></li> <li>Locate the line <code>TimeService=BAC</code> and change it to <code>TimeService=LOCAL</code></li> </ol> </li> </ul>
Probe Channel rum-components Guarantee Delivery Files Total Size	The total size of component channel files on the RUM Probe	N/A	N/A	N/A	

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

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

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

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

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

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



Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Process Memory Utilization	The total amount of non-swapped physical memory used by the probe process, out of the total amount of physical system memory, in kilobytes	Memory utilization is normal	Memory utilization is high	Memory utilization is nearing the maximum permissible value	The Probe may be processing too much traffic. Check the sizing guidelines.
Probe Queue Overflow Count	The number of time the Probe Queue was overflowed	< 2	> 2 and < 4	>= 4	Probe Queue overflow indicates that the probe is not able to monitor the traffic. This could happen due to a temporary spike. In this case, increasing the maximum_queue_size in the Beatbox_Default_Const_Configuration.xml file or the probe specific Beatbox file on the RUM Engine machine in the /conf/configurationmanager path in the RUM engine installation can help. Another reason for the overflow could be that the traffic being monitored is consistently beyond the capacity of the probe. The resolution for this scenario is to reduce the load on the current probe, and add more probes if required.
Probe Queue Overflow Last Occurrence Time	The last time the Probe Queue Overflow occurred	= 0	Not 0	N/A	

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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Storage mainpagedb Status	The current status of the database for main pages	Database status is normal	N/A	Database status is bad	
Probe Storage pcapnetwork Number of Errors	The number of non critical errors for network captures that occurred when working with the database	N/A	N/A	N/A	
Probe Storage pcapnetwork Number of Total Records	The total number of records for network captures in the database	N/A	N/A	N/A	
Probe Storage pcapnetwork Status	The current status of the database for network captures	Database status is normal	N/A	Database status is bad	
Probe Total Traffic	The amount of traffic which passed the kernel filter and came to the probe for further analysis	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Received Bytes on Network Device	The total number of bytes received per specific NIC, in bits per second	Network device load is normal	Network device load is nearing the probe's limit	N/A	
SSL Bytes Received	The total number of ssl bytes received by the servers from clients	The current load of https received traffic is normal	N/A	The current load of https received traffic is too high for a single RUM Probe	The Probe may be processing too much traffic. Check the sizing guidelines.
SSL Bytes Sent	The total number of ssl bytes sent by the servers to clients	The current load of https sent traffic is normal	N/A	The current load of https sent traffic is too high for a single RUM Probe	
SSL Packets	The total number of ssl packets processed by the RUM Probe	The https packet rate is normal	N/A	The https packet rate is too high for a single RUM Probe	
Total Memory	The total amount of physical system memory, in kilobytes	Always	N/A	N/A	

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

## RUM Client Monitor Probe

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

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

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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Channel "poorRequests" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	
Channel "sessions" Status	Status of the last attempt to connect to the channel	The RUM Engine has successfully connected to this probe channel	The RUM Engine experienced problems while connecting to this probe channel	The RUM Engine has failed to connect to this probe channel more than three consecutive times	
Configuration to Probe	Status of the last attempt to send the configuration to the RUM Probe	Probe was configured successfully	N/A	Errors during probe configuration process	<ul style="list-style-type: none"> <li>• Check the connection to the probe</li> <li>• Check the connection to the probe</li> </ul>
Connection to Probe	Status of the http connection from the RUM Engine to the RUM Probe	The connection is successful	N/A	There is no connection	
Pages Cached	The number of page views currently being cached to the RUM Probe's memory	The page rate is stable	The page rate is nearing the limit for normal caching	The page rate is too high	Verify that monitored traffic does not exceed sizing recommendations.



Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe and Engine Time Difference	Displays the status of the time synchronization between the RUM Engine and Probe	The RUM Engine and Probe are in sync	The RUM Engine and Probe are slightly out of sync	The RUM Engine and Probe are grossly out of sync	Where the identified time difference between the RUM Engine and the probe is greater than a minute (applies for Sniffer or Client Monitor probe - this can happen even if the products are on the same physical VM or server), it is recommended to set the <b>ProbeSyncTimeIntervalMin</b> value on the Engine to 10 minutes (default is 1440 minutes). Change from the RUM JMX console: http://<Engine Host>:8180/jmx-console/HtmlAdaptor?action=inspectMBean&name=RUM.modules%3Aservice%3DConfigurationManagerConf
Probe Client Monitor Page Hits	The number of hits from a client browser on a mobile device	N/A	N/A	N/A	
Probe Channel Delay	The delay between the read time from the probe and the current time	N/A	N/A	N/A	
Probe Channels Data Flow	Status of retrieving data from the RUM Probe	Data from the probe successfully retrieved	Probe has not produced new data for some time	N/A	Problem with the connection between the RUM Engine and the RUM Probe, or problems with one or more channels on the Probe side: <ul style="list-style-type: none"> <li>• Check the &lt;RUM&gt;\log\btretriever.log file</li> <li>• Try to restart the RUM Probe</li> </ul>
Probe Dropped Page Hits Due Other Reasons	The number of pages dropped due to other reasons	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Probe Dropped Page Hits Due Traffic	The number of pages dropped due to traffic issues	N/A	N/A	N/A	
Probe Dropped Page Hits Due Unresolved Host	The number of pages dropped due to an unresolved host	N/A	N/A	N/A	
Probe Dropped Page Hits of Undefined Application	The number of pages dropped as they do not belong to a defined application	N/A	N/A	N/A	
Probe License Status	The license status according to the license configured in APM	The license status is OK	N/A	Check license status and details in APM	In APM > End User Management Administration, check license status for current Probe
Probe Mobile Page Hits	The number of hits from a mobile device to a remote server	N/A	N/A	N/A	
Probe Session Hits	The number of closed sessions monitored by the RUM Probe	N/A	N/A	N/A	

## RUM Engine

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Application Transaction Count	The total number of open application transactions	Always	N/A	N/A	
BBRetriever hold time due to load on Entry Topic	The time (in milliseconds) that the BBRetriever was stopped due to JMS load on the Entry topic	N/A	N/A	N/A	
BBRetriever hold time due to load on RawEntry Topic	The time (in milliseconds) that the BBRetriever was stopped due to JMS load on the RawEntry topic	N/A	N/A	N/A	
BBRetriever hold time due to load on TCP Entry Topic	The time (in milliseconds) that the BBRetriever was stopped due to JMS load on the TCP Entry topic	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
BBRetriever hold time due load on TCP RawEntry Topic	The time (in milliseconds) that the BBRetriever was stopped due to JMS load on the TCP RawEntry topic	N/A	N/A	N/A	
BBRetriever Thrown Objects	The total number of objects thrown by the BBRetriever	N/A	N/A	N/A	
BBRetriever Total Actions Published	The number of actions being published by the BBRetriever in the RUM Engine	The number of actions being published is normal	The number of actions being published is above average	The number of actions being published is high	There is more traffic (actions/connections/pages) than the Engine can handle. Check sizing guidelines.
BBRetriever Total Connections Published	The number of connections being published by the BBRetriever in the RUM Engine	The number of connections being published is normal	The number of connections being published is above average	The number of connections being published is high	
BBRetriever Total Pages Published	The number of pages being published by the BBRetriever in the RUM Engine	The number of pages being published is normal	The number of pages being published is above average	The number of pages being published is high	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
BBRetriever Total Poor Requests Published	The number of Poor requests published by the BBRetriever in the RUM Engine	N/A	N/A	N/A	
Classification total application tiers with classification disabled	The number of applications whose actions will no longer be classified	0	> 0	N/A	A specific application is not supported by the RUM classification algorithm.  You can view application statistics in the RUM JMX console:  <a href="http://&lt;Engine_host&gt;:8180/jmx-console/HtmlAdaptor?action=inspectMBean&amp;name=RUM.modules%3Aservice%3DResolverClassification">http://&lt;Engine_host&gt;:8180/jmx-console/HtmlAdaptor?action=inspectMBean&amp;name=RUM.modules%3Aservice%3DResolverClassification</a> > viewStatistics
Classification total clusters number	The total number of classification clusters	The number is below the threshold	N/A	The number exceeds the threshold	If the application has more than 200 clusters, we recommend disabling classification for the application (in APM, select EUM Admin > <application> > Data Collection and clear the Enable automatic page classification check box).
Classification total nodes number	The total number of classification nodes	The number is below the threshold	N/A	The number exceeds the threshold	
Data Access Layer	Click <b>Data Access Layer</b> to see the entities that comprise the Data Access Layer component.				
Data Publisher Channel Configuration Status	The status of building the last published Data Publisher configuration	Always	N/A	The latest published configuration failed to build	

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

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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Location Configuration Validity	Displays the correctness of location configurations	Location configuration is OK	Overlap of IP addresses. One of the overlapping locations is automatically deleted. Check resolver.log for details. Manually reconfigure the locations so that there is no overlap. (You can delete all manually created locations; default locations are automatically recreated.)	Location configuration is problematic. All data is discarded. Check resolver.log for details.	The location configuration received from APM is invalid. Check locations in the Location manager in APM. Ensure that there are no overlapping IP ranges.
Login Maps Size per Name	The total number of login names mapped to sessions	Always	N/A	N/A	
Login Maps Size per Session	The total number of sessions mapped to login names	Always	N/A	N/A	
Partition Manager	Click <b>Partition Manager</b> to see the entities that comprise the Partition Manager component.				



Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Publish configuration to module <module name> on host <IP address>	Status of the last attempt to publish the configuration to the RUM Engine internal modules	Configuration to module <module name> on host <IP address> successfully published	N/A	Error while trying to publish configuration to module <module name> on host <IP address>	
Publisher Chunks in Memory	The number of sample chunks (not yet sent to APM) stored in memory	N/A	N/A	N/A	
Poor Request Network Captures Retrieved	The number of Poor request capture files retrieved by the RUM Engine	N/A	N/A	N/A	
Poor Request Network Captures Thrown	The number of Poor request capture files thrown by the RUM Engine	N/A	N/A	N/A	
Poor Requests with Network Captures	The number of Poor requests that have a network capture file	N/A	N/A	N/A	
Publisher Chunks in Queue	The total number of sample chunks waiting to be sent to APM	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Resolver Active End Users	The status of received end-user configuration from APM	Valid end-user configuration received	N/A	Valid end-user configuration not received	
Resolver End User DNS Cache size	The size of the end user DNS cache	N/A	N/A	N/A	
Resolver Ignored Sessions Cache Size	The size of the ignored sessions cache	Cache size is normal	N/A	Cache size has exceeded the permissible limit	
Resolver Server DNS Cache size	The size of the server DNS cache	N/A	N/A	N/A	
Resolver Thrown Actions Because Empty Descriptor	The number of actions for which the template (generic) descriptor is empty or null	N/A	N/A	N/A	
SessionManager Application Session Count	The total number of open application sessions	Always	N/A	N/A	
SessionManager BB Session Count	The total number of open BB sessions	Always	N/A	N/A	
SessionManager Opened Session Count	The total number of open sessions	Always	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Snapshot Jobs Alive Count	The total number of open snapshot jobs waiting to be processed	RUM can process all the open snapshots	The number of open snapshots waiting to be processed is nearing the limit for RUM under the current load	RUM might not be able to process all the snapshots	In APM, check the snapshot configuration (EUM Admin > End User Management > Data Collection > Snapshot collection) and ensure that a reasonable number of pages back are configured for snapshots.
Snapshot Jobs Submit Denials	The total number of submit requests for snapshot failures	Always	N/A	N/A	
Snapshot Relevant Events	The total number of events that should trigger snapshot creation	Always	N/A	N/A	
Snapshot Sessions Map Size	The total number of open sessions for which at least one snapshot was created	The number of current sessions is normal	The number of current sessions is nearing the permissible limit	The number of current sessions has exceeded the permissible limit	<ul style="list-style-type: none"> <li>• Check resource connectivity.</li> <li>• Check the application session count (which may be a root cause for this indication). Try to reduce the number of snapshots per application.</li> </ul>

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Statistics Total Aggregation Size	The number of aggregation buckets in memory	The number of aggregation buckets is normal	The number of aggregation buckets is nearing the permissible limit	The number of aggregation buckets has exceeded the permissible limit	<ul style="list-style-type: none"> <li>Try restarting the Engine.</li> <li>There may be a problem with the aggregation manager module. Look for a problematic type (such as pages, transactions, and so forth) in the RUM Engine JMX console:  <pre>http://&lt;Engine_host&gt;:8180/jmx-console/HtmlAdaptor?action=inspectMBean&amp;name=RUM.modules%3Aservice%3DStatisticsMgrConf &gt;viewStatus</pre> </li> </ul>
Statistics Total Messages Ignored	The number of entities filtered out by the statistics manager	Always	N/A	N/A	
Topology Engine	Click <b>Topology Engine</b> to see the entities that comprise the Topology Engine component.				
Total application tiers with number of page names above threshold	The number of applications for which the total number of page names was exceeded and no more page names will be given	0	N/A	N/A	
Total number of page names	The total number of pages (for all applications) that have been given names	< 50000	= 50000	> 50000	

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

## Samples to APM Server

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

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

## Data Access Layer

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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Average response time for <entity>	The amount of time taken to write the <entity> objects to the database	Response time of database is normal	Response time of database is high, which might indicate a database problem	Response time of database is very high, which might indicate a database problem
DAL Active	Whether the Data Access Layer is active or not. In some instances, when free disk space on the database server is running low, the Data Access Layer stops sending data to the database.	The Data Access Layer is active	N/A	The Data Access Layer is not active

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)
Number of cache misses in <entity> lookup table cache	The number of queries to the <entity>'s cache for which data was not available, but should have been	N/A	N/A	N/A
Number of files in <entity> cache	The size of the cache for each <entity> type	There is no backlog	A backlog of objects to be sent to the database exists, which could indicate a database problem or a temporary load peak	A large backlog of objects to be sent to the database exists, which could indicate a database problem or a temporary load peak
Number of futile queries to <entity> lookup table cache	The number of queries to the <entity>'s cache for which data was not available	N/A	N/A	N/A
Number of <entity> objects sent	The number of <entity> objects sent to the database since startup	N/A	N/A	N/A
Number of queries to <entity> lookup table cache	The total number of queries to the <entity>'s cache	N/A	N/A	N/A
Size of <entity> lookup table cache	The size of the <entity> table in the memory cache	Within the cache limit	N/A	Cache limit breached

## Partition Manager

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

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

## Topology Engine

To access, click Topology Engine in RUM Engine monitors.

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



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

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
IP accumulator permanently unresolved set size	The number of IP ranges sent to APM, that the Location Manager could not resolve to a specific location	< 10,000	N/A	>= 10,000	
IPs accumulator size	The number of IP ranges waiting to be sent to APM for location matching	<= 5,000	N/A	> 5,000	
Location accumulator permanently unresolved set size	The size of cached unresolved locations to be published to APM	Within the permitted cache size	N/A	Greater than the permitted cache size	
Locations accumulator size	The size of cached locations to be published to APM	Within the permitted cache size	N/A	Greater than the permitted cache size	
Number of accumulated IP ranges	The accumulated data structure size of discovered IP ranges	N/A	N/A	N/A	This may be critical (red) during peak traffic periods.
Number of accumulated tiers	The accumulated data structure size of discovered tiers	N/A	N/A	N/A	

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Number of new accumulated IP ranges	The accumulated data structure size of new IP ranges	N/A	N/A	N/A	This may be critical (red) during peak traffic periods.
Reporters connection to APM status	The status of the connection to APM	Connection OK	N/A	No connection	<p>Check the RTSM password in the RUM Engine web console (Configuration &gt; APM Connection Settings &gt; RTSM-RUM integration user password field) and test it using the Test RTSM password button. This password may have been changed from the default one in this specific APM installation and was not changed in the RUM Engine. You can change the password in BPM using JMX:</p> <p>http://&lt;APM Data Processing Server machine&gt;:21212/jmx-console/HtmlAdaptor?action=inspectMBean&amp;name=UCMDB:service=SecurityServices#changeIntegrationUserPassword</p> <p>where:</p> <ul style="list-style-type: none"> <li>• customerId = 1</li> <li>• userName = rum_integration_user</li> </ul>

Entity	Description	OK Status (Green)	Minor Status (Yellow)	Critical Status (Red)	Troubleshooting
Resolved Hosts cache size	The number of hosts to be reported to APM for CI creation	<= 10,000	N/A	> 10,000	Check in the RTSM that your topology is really this big. If so, consider increasing the maximum value in the xml file for the monitor (c:\<RUM>\conf\monitoringmanager\RumEngine\TopologyEngine\<monitor name>.xml).
Resolved Software Elements - Application links cache size	The number of application and software element links reported to APM	<= 10,000	N/A	> 10,000	
Resolved Software Elements cache size	The number of software elements reported to APM	<= 10,000	N/A	> 10,000	
Resolved Subgroups cache size	The number of end-user subgroups reported to APM	<= 30,000	N/A	> 30,000	
Unresolved Hosts cache size	The number of hosts waiting to be reported to APM	<= 1,000	N/A	> 1,000	

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

## Missing Mirrored Data

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

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

## Capture Log Files

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

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

## RUM Configuration and Settings

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

- **APM Connection Settings.** Used to view and configure the connection parameters between RUM and APM. For details, see ["APM Connection Settings" below](#).
- **Probe Management.** Used to configure communication settings with the RUM Probe. For details, see ["Probe Management" on page 103](#).
- **Advanced Settings.** Provides links to specific areas of the Real User Monitor JMX console for configuring parameters and settings for individual RUM modules. For details, see ["Advanced Settings" on page 121](#).
- **Data Flow Probe Connection Settings.** Used to view and configure the connection parameters between RUM and Universal Discovery. For details, see ["Data Flow Probe Connection Settings" on page 121](#).
- **System Info.** Provides general system information about RUM. For details, see ["System Info" on page 122](#).

## APM Connection Settings

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

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

The page contains the following panes:

- ["RUM General Settings Pane" below](#)
- ["Connection to APM Pane" on the next page](#)
- ["Authentication Pane" on the next page](#)
- ["Proxy Pane" on the next page](#)
- ["SSL Pane" on page 96](#)

### RUM General Settings Pane

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

## Connection to APM Pane

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

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

## Authentication Pane

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

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

## Proxy Pane

Field	Description
<b>Use proxy</b>	Select the check box if the RUM Engine connects to the APM Gateway Server machine via a proxy server.
<b>Proxy host</b>	If the RUM Engine connects to the APM Gateway Server machine via a proxy server, enter the IP address or host name of the proxy server.
<b>Proxy port</b>	If you connect to the APM Gateway Server machine via a proxy server, enter the port number used to connect to the proxy server.
<b>Use proxy authentication</b>	Select the check box if authentication is required when connecting to the proxy server.
<b>Proxy user name</b>	If authentication is required when connecting to the proxy server, enter the user name to use.

Field	Description
<b>Proxy password</b>	If authentication is required when connecting to the proxy server, enter the password to use.
<b>Proxy domain</b>	If authentication is required when connecting to the proxy server, enter the applicable domain for the user.

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

## SSL Pane

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



Field	Description
<b>Validate that the server certificates are not expired</b>	Select this check box to validate that the certificate is current.

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

## Docker Host Management









You use the Docker Host Management configuration option to create and administer Docker Engine or Docker Swarm Manager hosts whose containers you would like to monitor with RUM or Kubernetes Master hosts whose Docker hosts (nodes), pods, and services you would like to monitor with RUM.

When you select the Docker Host Management option from the Configuration drop-down menu, the Docker Host Management page opens and displays a table with the following information for each Docker host or Kubernetes Master host:

Column	Description
<b>Enabled</b>	This value denotes whether the Docker Engine, Docker Swarm Manager, or Kubernetes Master host is enabled or not. A host that is not enabled will not have its containers monitored. It also implies that the host will not be queried for the type and number of containers it hosts.  <b>Note:</b> Not all the configuration options are enabled for disabled hosts.
<b>Name</b>	The name you configured for the Docker host or Kubernetes Master host.
<b>Host IP</b>	The IP address of the Docker Engine, Docker Swarm Manager, or Kubernetes Master host whose containers are ready to be monitored.
<b>Type</b>	<ul style="list-style-type: none"> <li>• <b>DockerEngine</b> – For a Docker Engine host</li> <li>• <b>KubernetesMaster</b> – For a Docker cluster managed by Kubernetes</li> <li>• <b>DockerSwarmManager</b> – For a Docker cluster managed by Docker Swarm</li> </ul>
<b>Description</b>	A free text description qualifying the configured Docker Engine, Docker Swarm Manager, or Kubernetes Master host.



## Action Buttons

You use the actions buttons displayed above the table to configure a Docker Engine host, Docker Swarm Manager host, or Kubernetes Master host and to manage the table. You select a Docker Engine host, Docker Swarm Manager host, or Kubernetes Master host by clicking a row in the table. The following table lists and describes the available action buttons:

Icon	Description	For details, see ...
	<b>New Host Configuration.</b> Opens the New Host Configuration dialog box, where you configure a new Docker host whose containers are to be monitored or Docker Swarm Manager or Kubernetes Master host whose underlying Docker hosts are to be monitored.	<a href="#">"Host Configuration Dialog Box" below</a>
	<b>Edit Host Configuration.</b> Opens the Edit Host Configuration dialog box, where you configure an existing Docker host whose containers are to be monitored or Docker Swarm Manager or Kubernetes Master host whose underlying Docker hosts are to be monitored.	<a href="#">"Host Configuration Dialog Box" below</a>
	<b>Delete Host Configuration.</b> Deletes a selected Docker host or Docker Swarm Manager or Kubernetes Master host configuration from the engine.	N/A
	<b>Docker Probe Management.</b> Opens the Docker Probe Management page for the selected Docker host. This button is enabled for Docker hosts of type Docker Swarm Manager and Docker Engine.	<a href="#">"Docker Probe Management" on page 102</a>
	<b>Container Patterns Filter.</b> Enables you to fine tune monitoring based on the container name or container image and specify the containers that should be monitored for each application tier.	<a href="#">"Docker Pattern Filter Settings" on page 101</a>
	<b>Refresh.</b> Refreshes the list of Docker host and Docker Swarm Manager or Kubernetes Master host in the table.	N/A
	<b>Reset columns width.</b> Resets the columns in the table to their default width.	N/A
	<b>Select Columns.</b> Selects the columns displayed in the table.	N/A

## Host Configuration Dialog Box

You use the Host Configuration dialog box to configure a new host whose containers are to be monitored, or to edit the settings of an existing host. Hosts can either be Docker Engine, Docker Swarm Manager, or Kubernetes Master hosts.

To access the Host Configuration dialog box, click the **New Host Configuration** button  or the **Edit Host Configuration** button  on the Docker Host Management page. The Host Configuration dialog box includes the following fields that you configure for a Docker Engine, Docker Swarm Manager, or Kubernetes Master host:

### Host Details Pane

Field	Description
<b>Enabled</b>	Select the check box to enable the Docker Engine, Docker Swarm Manager, or Kubernetes Master host, or clear the check box to disable the host.  <b>Note:</b> <ul style="list-style-type: none"> <li>• A host that is not enabled will not have its containers monitored.</li> <li>• If you enable the host and the IP address is not valid, an error message will appear.</li> </ul>
<b>Name</b>	The Docker Engine, Docker Swarm Manager, or Kubernetes Master host name.  <b>Note:</b> This field is mandatory.  <b>Syntax exceptions:</b> Cannot exceed 255 characters.
<b>Description</b>	A free text description of the Docker Engine, Docker Swarm Manager, or Kubernetes Master host.  Cannot exceed 255 characters.

### Connection to Host Pane

Field	Description
<b>Host</b>	The IPv4/IPv6 address of the machine on which the Docker Engine, Docker Swarm Manager, or Kubernetes Master is installed.  <b>Note:</b> This field is mandatory.  <b>Syntax exceptions:</b> <ul style="list-style-type: none"> <li>• Cannot exceed 255 characters.</li> <li>• Allowed characters are a-z, A-Z, 0-9, and - \ . ] *.</li> </ul>
<b>Port</b>	The port number used to connect to the Docker Engine, Docker Swarm Manager, or Kubernetes API.  <b>Default value:</b> <ul style="list-style-type: none"> <li>• 2375 for a Docker Engine Host and Docker Swarm Manager</li> <li>• 8080 for a Kubernetes Master host</li> </ul> <b>Syntax exceptions:</b> Cannot exceed 100 characters.

Field	Description
<b>Probe Management</b>	<p>Select the probe management type.</p> <ul style="list-style-type: none"> <li>• <b>Automatic</b> – RUM Engine will ensure that at least one probe container is running on the host and that a probe configuration on the Engine side is connected to this probe container.</li> <li>• <b>Manual</b> – User is responsible for creating a probe container, ensuring that it is running, creating a probe configuration on the Engine, and connecting the probe configuration to the probe container.</li> </ul>
<b>Type</b>	<p>For a Docker Engine host, select <b>Docker Engine</b>.</p> <p>For a Kubernetes Master host, select <b>Kubernetes Master</b>.</p> <p>For a Docker Swarm Manager host, select <b>Docker Swarm Manager</b>.</p>
<b>Protocol</b>	<p>The protocol used to connect to the Docker Engine, Docker Swarm, or Kubernetes API. Select either <b>HTTP</b> or <b>HTTPS</b>.</p>

### Authentication Pane

Field	Description
<b>Use authentication</b>	Select the check box if authentication is required to connect to the the Docker Engine, Docker Swarm, or Kubernetes API.
<b>Authentication user name</b>	If authentication is required, enter the user name to use.
<b>Authentication password</b>	If authentication is required, enter the password to use.
<b>Authentication domain</b>	If authentication is required, enter the applicable domain for the user.

### Proxy Pane

Field	Description
<b>Use proxy</b>	Select the check box if the RUM Engine connects to Docker Engine, Docker Swarm Manager, or Kubernetes Master host machine via a proxy server.
<b>Proxy host</b>	If the RUM Engine connects to the Docker host, Docker Swarm Manager, or Kubernetes Master host machine via a proxy server, enter the IP address or host name of the proxy server.
<b>Proxy port</b>	If you connect to the Docker host, Docker Swarm Manager, or Kubernetes Master host machine via a proxy server, enter the port number used to connect to the proxy server.
<b>Use proxy authentication</b>	Select the check box if authentication is required when connecting to the proxy server.

Field	Description
<b>Proxy user name</b>	If authentication is required when connecting to the proxy server, enter the user name to use.
<b>Proxy password</b>	If authentication is required when connecting to the proxy server, enter the password to use.
<b>Proxy domain</b>	If authentication is required when connecting to the proxy server, enter the applicable domain for the user.






## SSL Pane

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

## Docker Pattern Filter Settings





The Docker Pattern Filter Settings page enables you to fine tune monitoring based on the container name or container image and specify the containers that should be monitored for each application tier.

Your filters are listed according to the Application Name and Tier Name.

Icon	Description
	<b>Select all filters.</b>
	<b>Select no filters.</b>
	<b>Invert filter selection.</b>
	<b>Delete.</b> Click to delete the selected filter. You must then click <b>Save Configuration</b> to process this change.
	<b>Edit.</b> Opens the Edit Docker Pattern Filters Settings page to enable you to edit the selected filter.
	<p><b>New Definition.</b> Opens the Edit Docker Pattern Filters Settings page to create a new filter. On this page you enter the following information:</p> <ul style="list-style-type: none"> <li>• <b>Tier Name</b> - Select the application/tier name for which you want to add the filter.</li> <li>• <b>Image Name Filter</b> - Enter the image name of the containers to filter into the selected tier. You can use wildcards (*) in this field.</li> <li>• <b>Container Name Filter</b> - Enter the name of the containers to filter into the selected tier. You can use wildcards (*) in this field.</li> </ul> <p>Click <b>Submit</b> after entering the information.</p>
	<b>Save Configuration.</b> After creating a filter, click to save the filter to the backend xml.
	<b>Reload Current Configuration.</b> Click to reload the current filter into the table.

## Docker Probe Management

When you click the Docker Probe Management button from the Docker Host Management page, the Docker Probe Management page opens and displays a table with the following probe information for the selected Docker Host:

UI Element	Description
	<b>Remove and Recreate Container.</b> Deletes selected container on Docker host and recreates it. This is useful if probe is unresponsive.
	<b>Remove Container.</b> Deletes probe container from Docker host. If automatic probe management is enabled for the Docker host, although RUM deletes the probe container, RUM would recreate the container in the next configuration cycle.
	<b>Check RUMProbe Process Status.</b> Connects to the probe container and checks that the RUM probe process is running with the probe container.
	<b>Retrieve Container Log.</b> Connects to the probe container and displays the last 20 lines of the capture log. This is useful for troubleshooting.
	<b>Refresh.</b> Repopulates the Docker Probe Management table with updated data.

UI Element	Description
	<b>Force Docker Discovery.</b> RUM Engine connects to all the Docker hosts and performs Discovery to check if new container or new images have been created, or if a host requires deployment of probe containers. If a container was deleted and automatic probe management is enabled for the probe, the Docker host recreates the container.
<b>Node</b>	Name of the Docker node.
<b>Probe Name</b>	Name of the probe that is managed by the engine. This matches the name of the probe created under <b>Configuration &gt; Probe Management</b> for this probe container.
<b>Container Image</b>	Name of the image from which the probe container was created.
<b>Container Name</b>	Name of the probe container on this node.
<b>Container Port</b>	Port on which this probe container is listening.
<b>Container Status</b>	Status of container ( <b>Up</b> or <b>Down</b> ).

## Probe Management














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

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

Column	Description
<b>Enabled</b>	This value denotes whether the probe is enabled or not. A probe that is not enabled does not monitor RUM traffic. <b>Note:</b> Not all the configuration options are enabled for disabled probes.
<b>Name</b>	The name you configured for the probe.
<b>Host Name</b>	The host name of the machine on which the probe is installed.
<b>Description</b>	A free text description you configured for the probe.



## Action Buttons

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

Icon	Description	For details, see ...
	<b>New Probe Configuration.</b> Opens the New Probe Configuration dialog box, where you configure a new probe for the engine.	<a href="#">"Probe Configuration Dialog Box"</a> on the next page
	<b>Edit Probe Configuration.</b> Opens the Edit Probe Configuration dialog box, where you configure an existing probe for the engine.	<a href="#">"Probe Configuration Dialog Box"</a> on the next page
	<b>Delete Probe Configuration.</b> Deletes a selected probe from the engine.	N/A
	<b>Probe Traffic Discovery.</b> Opens the Probe Traffic Discovery page, where you enable the probe to automatically discover the servers and domains being accessed by the traffic to which it is listening.  <b>Note:</b> This button is not enabled for disabled probes.	<a href="#">"Probe Traffic Discovery"</a> on page 107
	<b>Probe Information.</b> Displays general information about the selected probe in a new window. The information displayed shows the status of the probe, the operating system and version running on the probe, the last configuration time of the probe, and the last successful configuration time.	N/A
	<b>SSL Keystore Management.</b> Opens the SSL Keystore Management page, where you manage the keys used by the probe to monitor SSL encrypted traffic.  <b>Note:</b> This button is not enabled for disabled probes.	<a href="#">"SSL Keystore Management"</a> on page 110
	<b>Interfaces Configuration.</b> Opens the Interfaces Configuration page, where you list and select a probe's Ethernet devices used to monitor server traffic.  <b>Note:</b> This button is not enabled for disabled probes.	<a href="#">"Interface Configurations"</a> on page 113
	<b>Server Filter Settings.</b> Opens the Server Filter Settings page, where you list and configure the filters to be used for monitoring server traffic.  <b>Note:</b> This button is not enabled for disabled probes.	<a href="#">"Server Filter Settings"</a> on page 114
	<b>Probe Traffic Capture.</b> Opens the Probe Traffic Capture page where you instruct a RUM Probe to save the traffic it monitors to a file.	<a href="#">"Probe Traffic Capture"</a> on page 115
	<b>Session ID Detection.</b> Opens the Session ID Detection page, where you instruct a RUM Probe to detect Session IDs in the traffic it monitors.	<a href="#">"Session ID Detection"</a> on page 117
	<b>Refresh.</b> Refreshes the list of probes in the table.	N/A
	<b>Reset columns width.</b> Resets the columns in the table to their default width.	N/A
	<b>Select Columns.</b> Selects the columns displayed in the table.	N/A



## Probe Configuration Dialog Box

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

### Probe Details Pane

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

### Connection to Probe Pane

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

### Authentication Pane

Field	Description
<b>Use authentication</b>	Select the check box if authentication is required when connecting to the host machine on which the probe is installed.

Field	Description
<b>Authentication user name</b>	If authentication is required, enter the user name to use.
<b>Authentication password</b>	If authentication is required, enter the password to use.
<b>Authentication domain</b>	If authentication is required, enter the applicable domain for the user.

## Proxy Pane

Field	Description
<b>Use proxy</b>	Select the check box if the RUM Engine connects to the probe machine via a proxy server.
<b>Proxy host</b>	If the RUM Engine connects to the probe machine via a proxy server, enter the IP address or host name of the proxy server.
<b>Proxy port</b>	If you connect to the probe machine via a proxy server, enter the port number used to connect to the proxy server.
<b>Use proxy authentication</b>	Select the check box if authentication is required when connecting to the proxy server.
<b>Proxy user name</b>	If authentication is required when connecting to the proxy server, enter the user name to use.
<b>Proxy password</b>	If authentication is required when connecting to the proxy server, enter the password to use.
<b>Proxy domain</b>	If authentication is required when connecting to the proxy server, enter the applicable domain for the user.

## SSL Pane


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

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

## Probe Traffic Discovery

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

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

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



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

This section includes the following topics:

- ["Common Elements" on the next page](#)
- ["Summary View Tab" on the next page](#)
- ["Domain View/Server View Tabs" on page 109](#)

## Common Elements

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

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

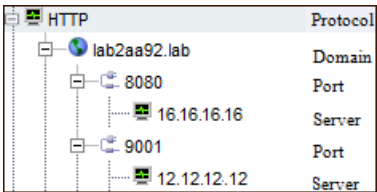

## Summary View Tab

The Summary View tab displays a pie chart in which each slice represents a different, discovered protocol and the slice size is determined by the percentage of protocol throughput out of the total throughput for all the protocols. Click the slice representing the http protocol to display the Domain View tab, or click on any other slice to display the Server View tab. The Domain View or Server View tab opens with the selected protocol expanded in the hierarchical tree.

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



## Domain View/Server View Tabs

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

UI Element	Description
<b>Search</b>	<p>You can filter the data displayed by searching for domains or servers that match a specific pattern or IP address. Enter the search pattern in the Search filter located at the top left of the page, and click <b>Search Domain</b> or <b>Search Server</b>. The data is redisplayed according to the records matching the search criteria.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>When using the search feature in the <b>Domain View</b> tab, you can enter alpha-numeric characters, the asterisk (*) wild card character, and use partial strings for matching. The search filters domain names that include the search string.</li> <li>In the <b>Server View</b> tab, you can enter only valid IP addresses in the search field. The search filters server IP addresses that exactly match the search string.</li> </ul>
<b>&lt;Domain View protocol tree&gt;</b>	<p>For each discovered protocol, the statistics are grouped by domain names (for http), or IP addresses (for other protocols). For each port in the domain, the IP address of each server that connected to the domain is listed. For example:</p>  <p><b>Note:</b> This is the default view when you drill down from the Summary View pie chart for the http protocol.</p>
<b>&lt;Server View protocol tree&gt;</b>	<p>For each discovered protocol, the statistics are grouped by server IP addresses and for each server, by port. For example:</p>  <p><b>Note:</b> This is the default view when you drill down from the Summary View pie chart for protocols other than http.</p>
<b>% Throughput</b>	The percentage of throughput for a specific protocol out of the total throughput for all protocols.
<b>Throughput</b>	The total throughput to and from the domain or server, for a specific protocol.
<b>Peak Traffic</b>	The peak amount of traffic transmitted to and from the domain or server, for a specific protocol. Peak traffic is determined based on 30 second intervals.

UI Element	Description
<b>Peak Pages/sec</b>	The peak number of pages per second for the domain or server for http. <b>Note:</b> This is applicable for http only.
<b>Compressed</b>	Ticked if any of the traffic sent and received by the domain or server was compressed.
<b>Encrypted</b>	Ticked if any of the traffic sent and received by the domain or server was encrypted.
<b>Server Info</b>	The name of the server, if available.
<b>More Details</b>	Reserved for future use.

## SSL Keystore Management

You use the SSL Keystore Management page to manage the keys used by a selected RUM Probe to monitor SSL encrypted traffic. To access the SSL Keystore Management page, click the **SSL Keystore Management** button  on the Probe Management page. The Keystore Management page contains three panes – **SSL Keystore Administration**, **SSL Application Decryption Statistics**, and **SSL Server Decryption Statistics**. To refresh the information on this page, click the **Refresh** button .

### Note:

- The RUM web console keystore import tool supports PEM, DER, PKCS8, and PKCS12 unencrypted private key types, as well as encrypted Java Keystore. Other key types can be imported if they are converted to one of the supported types.
- The RUM Probe cannot decrypt traffic that uses Diffe Helman keys. If there is a high percentage of such traffic (which you can see in the **Decryption Failed (unsupported algorithm)** column in the ["SSL Application Decryption Statistics Pane" on page 112](#)) it is recommended that you configure the web server of the monitored server not to support the Diffe Helman protocol.
- The following is a list of ciphers that can be decrypted while monitoring:

#### SSL v3.0 cipher suites

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

### TLS v1.0 cipher suites

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

### TLS v1.2 cipher suites

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

This section includes:

- ["SSL Keystore Administration Pane" below](#)
- ["SSL Application Decryption Statistics Pane" on the next page](#)
- ["SSL Server Decryption Statistics Pane" on page 113](#)

## SSL Keystore Administration Pane

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

### To add a key:


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

the applicable settings:

Key Type	Setting	Description
Import from Key File	<b>File</b>	The path and name of the file containing the private key. You can click <b>Browse</b> to navigate to the relevant file.
	<b>Password</b>	The password with which the key is encrypted, or null if the key is not encrypted.
Import from Keystore	<b>Keystore file</b>	The path and name of the keystore file. You can click <b>Browse</b> to navigate to the relevant file.
	<b>Keystore password</b>	The keystore password. <b>Note:</b> This field is mandatory.
	<b>Private key alias</b>	The alias of the specific key in the keystore. If no alias is configured, the first key in the keystore is used.
	<b>Private key password</b>	The password of the specific key in the keystore.

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

#### To delete a key:

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

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

### SSL Application Decryption Statistics Pane

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

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



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

## SSL Server Decryption Statistics Pane

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

## Interface Configurations

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


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

To sniff from an Ethernet device with a different name:

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

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

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

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

UI Element	Description
<b>Sniff</b>	Check box to select the device to monitor server traffic.
<b>Link Up</b>	Whether the network interface is physically connected to a cable.
<b>Name</b>	The logical name of the Ethernet device.

UI Element	Description
<b>Up</b>	Whether the device is running or not.
<b>Sniffable</b>	Whether the device can be used to listen to Ethernet traffic.
<b>Hardware</b>	The hardware details of the device.
<b>Driver</b>	The name of the driver used for the device.
<b>IP</b>	The IP address assigned to the device, if any.
<b>Interface Details</b>	Click the <b>Interface Details</b> button for a device to display link, driver, other settings, and statistics information in a new window.

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


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

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

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

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

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

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


## Server Filter Settings

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

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

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

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

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

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

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

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


### Add a new filter

1. Click **New Definition**. The Edit Server Filter Settings page opens.
2. In the Edit Server Filter Settings page, enter the following:


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

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

### Delete a filter


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


### Edit a filter

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

## Probe Traffic Capture

You use the Probe Traffic Capture feature to instruct a RUM Probe to save the traffic it monitors to a file. This is useful for analysis and troubleshooting. To configure and start probe traffic capturing, click the **Probe**

**Traffic Capture** button  on the Probe Management page. The Probe Traffic Capture page opens and displays the following elements:

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

## Session ID Detection

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

This section includes the following topics:


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

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


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

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

## Session ID Detection Page

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

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

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

## Session ID Detection Report

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

UI Element	Description
<b>Application Name</b>	The application name, as defined in End User Management Administration. For applications not been defined in End User Management Administration, the application name is <b>Default Website</b> . For information on configuring applications in End User Management Administration, see "RUM Application Configuration Wizard" in the APM Application Administration Guide.
<b>Application Components</b>	The total number of hits in the application.
<b>Application Pages</b>	The total number of pages in the application.
<b>Application Clients</b>	The total number of clients that accessed the application.
<b>Application Connections</b>	The total number of connections to the application.
<b>All Session IDs Coverage</b>	The percentage of hits in the application that contain a discovered session ID key.
<b>Session ID Key</b>	The session ID key name of the session ID discovered for the application.

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

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

### To display data for a specific application only:

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

### To display detailed information for a specific session ID key:

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

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

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

Click **View Raw Data**. The **Session ID Detection Raw Data** report is displayed, and shows the following information for the end-user IP address:

UI Element	Description
<b>#</b>	A sequential number indicating the row number in the report.



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

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

## Advanced Settings

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

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

For details on working with the JMX console, see ["Using the JMX Console to Configure the RUM Engine" on page 133](#).

## Data Flow Probe Connection Settings

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

### Overview

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

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

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

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

- The RUM Probe sends its filter settings to Universal Discovery, so that it knows what traffic the RUM Probe is monitoring.

## Prerequisites

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

## Configuration

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

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

### Note:

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

## System Info

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

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

## RUM Diagnostics Tools

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

- **Monitoring Configuration Information.** Displays general configuration data of the applications, end users, pages, probes, transactions, and engine that have been configured for monitoring by RUM in End User Management Administration. For details, see "[Monitoring Configuration Information](#)" on the next page.
- **JMX Console.** Provides a link to the RUM JMX console for configuring RUM parameters, such as URL correlation parameters. For details, see "[JMX Console](#)" on page 128. (For details on URL correlation, see "Correlating Collected Data with Configured Pages" in the APM Application Administration Guide.)

- **IP Translator.** Used to convert between the internal number used by the engine to represent an IP address and the actual IP address it represents. For details, see ["IP Translator" on page 128](#).
- **Time Converter.** Used to convert a date and time to an internal number used by the engine machine to represent this value. You can also convert the number used by the engine machine to the date and time it represents. For details, see ["Time Converter" on page 128](#).
- **Mobile Application Instrumentation.** Used to instrument Android APKs for monitoring mobile applications. For details, see ["Mobile Application Instrumentation" on page 129](#).

## Monitoring Configuration Information

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

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

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

This section includes the following topics:

- ["Applications" below](#)
- ["End Users" on the next page](#)
- ["Events" on the next page](#)
- ["Pages" on page 125](#)
- ["Probes" on page 125](#)
- ["Transactions" on page 126](#)
- ["Engine Settings" on page 127](#)
- ["Transaction Snapshot Mode" on page 128](#)

## Applications

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

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

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

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

## End Users

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

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

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

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

## Events

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

Column	Description
<b>ID</b>	An internal ID number allocated by APM.
<b>Is Event enabled</b>	True or False – as configured in End User Management Administration.
<b>Name</b>	The name of the event as configured in End User Management Administration.
<b>Event type</b>	The event type as configured in End User Management Administration.
<b>Report As Error</b>	True or False – as configured in End User Management Administration.
<b>Create Snapshot</b>	True or False – as configured in End User Management Administration.
<b>Collection Session Snapshot</b>	True or False – as configured in End User Management Administration.

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

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

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

## Pages

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

Column	Description
<b>Page ID</b>	An internal ID number allocated by APM.
<b>Is Page Enabled</b>	True or False – as configured in End User Management Administration.
<b>Page Name</b>	The name of the page as configured in End User Management Administration.
<b>Application</b>	The name of the application in which the page is included.
<b>Description</b>	The description of the page as configured in End User Management Administration.
<b>Monitored Type</b>	The monitoring condition as configured in End User Management Administration. The possible conditions are:  1 = Always 2 = Never 3 = Only as part of a transaction
<b>Page Type</b>	Currently not used
<b>Page Time Threshold</b>	The page time threshold, in milliseconds, as configured for the page in End User Management Administration.
<b>Server Time Threshold</b>	The server time threshold, in milliseconds, as configured for the page in End User Management Administration.
<b>Availability Threshold</b>	The availability threshold, in percent, configured for the page in End User Management Administration.
<b>Timeout</b>	The amount of time, in milliseconds, after which the page is considered to have timed out, as configured for the page in End User Management Administration.
<b>Page URL</b>	The URL of the page as configured in End User Management Administration.

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

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

## Probes

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

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

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

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

## Transactions

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

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

Column	Description
<b>Net Time Threshold</b>	The net transaction time threshold, in milliseconds, for the pages included in the transaction, as configured in End User Management Administration.
<b>Server Time Threshold</b>	The server time threshold, in milliseconds, as configured for the transaction in End User Management Administration.
<b>Availability Threshold</b>	The availability threshold, in percent, as configured for the transaction in End User Management Administration.
<b>Trx pages</b>	The names of the pages included in the transaction, as configured in End User Management Administration.

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

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

## Engine Settings

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

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

## Transaction Snapshot Mode

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

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

## JMX Console

This option provides a link to the RUM JMX console, which you use to view and configure RUM parameters, for example, URL correlation parameters. For details on configuring URL correlation parameters, see "Correlating Collected Data with Configured Pages" in the APM Application Administration Guide. For details on working with the JMX console, see ["Using the JMX Console to Configure the RUM Engine" on page 133](#).

## IP Translator

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

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

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

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

## Time Converter

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

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

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

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



## Mobile Application Instrumentation

The RUM mobile solution enables you to monitor mobile applications through apps on a user's mobile device and sends the collected data from the app directly to the RUM Client Monitor Probe. For details, see ["Using the RUM Mobile Solution to Monitor Mobile Applications"](#) on page 33.

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

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

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

User interface elements are described below:

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

UI Element	Description								
<b>Instrument for Production</b>	Select this option to fully sign the APK using a Java keystore file with a private key. If you select this option, configure the following:								
	<table border="1"> <tr> <td data-bbox="298 373 451 550"> <b>Application</b> </td> <td data-bbox="451 373 1421 550">           From the drop-down list, select the application configured in APM to which the monitored data will be associated.   <b>Note:</b> Only applications that use the Network for Mobile Application template are displayed in the list.         </td> </tr> </table>	<b>Application</b>	From the drop-down list, select the application configured in APM to which the monitored data will be associated.  <b>Note:</b> Only applications that use the Network for Mobile Application template are displayed in the list.						
	<b>Application</b>	From the drop-down list, select the application configured in APM to which the monitored data will be associated.  <b>Note:</b> Only applications that use the Network for Mobile Application template are displayed in the list.							
	<b>RUM Client Monitor Probe URL</b>	Enter the URL for the RUM Client Monitor Probe to which monitored data is sent. The format is:  https://<RUM Client Monitor Probe host name>:443/<path to the RUM Client Monitor Probe on the host>  <b>Note:</b> If no port is specified, port 443 is used by default.							
	<b>Application Signing</b>	Leave the following fields blank if you want to sign the APK later. You can sign the APK later using Java's jarsigner.exe tool (see " <a href="#">Signing an APK using Java's jarsigner.exe Tool</a> " on page 132). <table border="1" data-bbox="462 909 1414 1402"> <tr> <td data-bbox="462 909 737 1083"> <b>Keystore file</b> </td> <td data-bbox="737 909 1414 1083">           The path and name of the keystore file. You can click <b>Browse</b> to navigate to the relevant file.             If you do not configure a keystore file, the APK will not be signed.         </td> </tr> <tr> <td data-bbox="462 1083 737 1142"> <b>Keystore password</b> </td> <td data-bbox="737 1083 1414 1142">           A password for the keystore, if configured.         </td> </tr> <tr> <td data-bbox="462 1142 737 1310"> <b>Key alias</b> </td> <td data-bbox="737 1142 1414 1310">           The alias to the private key entry in the keystore.   <b>Note:</b> This field is mandatory if you configure a keystore file.         </td> </tr> <tr> <td data-bbox="462 1310 737 1402"> <b>Key password</b> </td> <td data-bbox="737 1310 1414 1402">           A password for the private key entry in the keystore, if configured.         </td> </tr> </table>	<b>Keystore file</b>	The path and name of the keystore file. You can click <b>Browse</b> to navigate to the relevant file.  If you do not configure a keystore file, the APK will not be signed.	<b>Keystore password</b>	A password for the keystore, if configured.	<b>Key alias</b>	The alias to the private key entry in the keystore.  <b>Note:</b> This field is mandatory if you configure a keystore file.	<b>Key password</b>
<b>Keystore file</b>	The path and name of the keystore file. You can click <b>Browse</b> to navigate to the relevant file.  If you do not configure a keystore file, the APK will not be signed.								
<b>Keystore password</b>	A password for the keystore, if configured.								
<b>Key alias</b>	The alias to the private key entry in the keystore.  <b>Note:</b> This field is mandatory if you configure a keystore file.								
<b>Key password</b>	A password for the private key entry in the keystore, if configured.								
<b>Add Access Network State permission to the application</b>	Select this check box to enable the APK to determine and report the type of user connection (WiFi/2G/G3/4G).								
<b>Allow access to http content</b>	Select one of the following to define when to apply mobile device configuration changes performed in APM Admin to the mobile devices. This includes change to parameters, user name, or un hiding query parameters.								

UI Element	Description	
	<b>Apply any configuration change to the mobile device even after instrumentation</b>	Select this option to enable the application to send any change in content extraction to the mobile device. Changes to the configuration can be performed even after the application is deployed on the mobile device.
	<b>Apply content extraction configuration change at instrumentation time only</b>	Select this option to enable the application to extract content configuration only when instrumenting the application. To apply a configuration change, you need to repeat the instrumentation.
	<b>Do not allow content extraction</b>	Select this option to disable the application from using any extracted content (parameter settings, username detection, or allowed POST parameters) configured for it in APM, when the application runs.
<b>Instrument for Testing</b>	Select this radio button to sign the APK with a self-signed debug certificate. <b>Note:</b> This is sufficient for testing the APK, but not for uploading it to the Google Play store. If you select this option, configure the following:	
	<b>Application</b>	From the drop-down list, select the application configured in APM to which the monitored data will be associated.  <b>Note:</b> Only applications that use the Network for Mobile Application template are displayed in the list.
	<b>RUM Client Monitor Probe URL</b>	Enter the URL for the RUM Client Monitor Probe to which monitored data is sent. The format is:  https://<RUM Client Monitor Probe host name>:443/<path to the RUM Client Monitor Probe on the host>  <b>Note:</b> If no port is specified, port 443 is used by default.

UI Element	Description	
<b>Instrument for Offline Testing and Data Collection</b>	Select this option not to sign the APK after instrumentation. You can test the application offline and collect data locally only.  <b>Note:</b> The APK must be fully signed before you can upload it to the Google Play store.  If you select this option, configure the following:	
	<table border="1"> <tr> <td><b>Store monitored data locally</b></td> <td>Select this check box to configure the APK not to send collected network data to the probe and to store it locally in the application folder on the mobile device.  This data includes the POST content of requests, which can assist you in defining extracted parameters for the application in APM. For details on extracted parameters, see "Parameter Extraction Area" in the Real User Monitor Application General Page in the APM Application Administration Guide.</td> </tr> </table>	<b>Store monitored data locally</b>
<b>Store monitored data locally</b>	Select this check box to configure the APK not to send collected network data to the probe and to store it locally in the application folder on the mobile device.  This data includes the POST content of requests, which can assist you in defining extracted parameters for the application in APM. For details on extracted parameters, see "Parameter Extraction Area" in the Real User Monitor Application General Page in the APM Application Administration Guide.	

## Signing an APK using Java's jarsigner.exe Tool

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

1. From a cmd window, enter:

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

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

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

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

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

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

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

You configure RUM Engine settings via the JMX console.

**Note:** You also use the web console to configure the engine, monitor system health, and use a number of diagnostic tools. For details, see ["Using the RUM Web Console" on page 40](#).

This chapter includes the following topics:

- ["Using the RUM JMX Console" below](#)
- ["URL Correlation Parameters" on page 139](#)

## Using the RUM JMX Console

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

This section includes the following topics:

- ["Accessing the JMX Console" below](#)
- ["Setting URL Correlation Parameters" on the next page](#)
- ["Configuring RUM Aggregation" on the next page](#)
- ["Configuring the Samples Rate" on page 136](#)
- ["Configuring the Amount of Unsent Sample Data to Store in RUM" on page 136](#)
- ["Configuring the Classification Type" on page 137](#)

## Accessing the JMX Console

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

Once you start the RUM Engine after installation, you can access the RUM Engine JMX console by launching the RUM Engine web console and choosing **JMX Console** from the Tools drop-down menu. To access a specific area of the JMX console for an individual RUM module, select **Advanced Settings** from the **Configuration** drop-down menu in the RUM Engine web console and then click the links for the module you want to view. For details on the RUM Engine web console, see ["Using the RUM Web Console" on page 40](#).

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

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

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

## Setting URL Correlation Parameters

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

Some of the URL correlation parameters are set using the RUM JMX console. For details on changing URL correlation parameters via the RUM JMX console, see ["Setting URL Correlation Parameters Via the JMX Console" on page 139](#).

## Configuring RUM Aggregation

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

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

This section includes the following topics:

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

## Pre-aggregated Data Sample Types

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

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

## Changing Default Aggregation Periods

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

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

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

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

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

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

```
attribute name=aggregation period
```

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

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

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

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

## Configuring the Samples Rate

The maximum burst rate controls the number of samples per second that the RUM Engine can send to APM. The default setting is 300. You can increase the maximum burst rate to allow more samples to be sent per second, provided that APM is capable of handling the increased number. You can see the state of the flow of samples between RUM and APM by looking at the **Publisher burst state** in RUM system health. For details on RUM system health, see ["Monitoring the Health of RUM Components" on page 43](#).

### To configure the maximum burst rate:

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

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

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

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

## Configuring the Amount of Unsent Sample Data to Store in RUM

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



planned downtime in APM. Bear in mind that when a lot of data has been stored in RUM, it can take a long time for all of it to be sent to APM, which might cause a delay in seeing real time data. If you increase the number of data chunks to store, you should reset it to the original number once APM is running and all the stored data has been transmitted to it.

**To increase the maximum number of data chunks stored:**

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

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

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

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

## Configuring the Classification Type

The classification algorithm groups similar, unconfigured actions under one name (a generic descriptor) and aggregates their measurements to obtain values for the descriptor. The aggregated actions can be viewed in the RUM Action Summary report in APM. For HTTP-Web based protocols, there are two methods of classification:

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

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

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

### Example 1

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

**Example 2**

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

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

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

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

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

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

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

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

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

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

## URL Correlation Parameters

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

This section includes the following topics:

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

## Setting URL Correlation Parameters Via the JMX Console

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

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

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

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

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

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

- **adaptCaseSensitive**. By default, RUM URL correlation is case-insensitive, so that a recorded URL such

as `http://www.anycompany.com/rumEnginePage.html` is correlated with the configured URL `http://www.anycompany.com/rumenginepage.html`. To instruct RUM to use case-sensitive URL correlation (for all but the host and protocol parts of a URL), you set this parameter to **False**.

- **basicAuthentication**. By default, RUM ignores basic authentication when performing URL correlation. For example, the recorded URL `http://bob:my_password@www.anycompany.com` is correlated with the configured URL `http://www.anycompany.com`. To instruct RUM to consider basic authentication when performing URL correlation, you set this parameter to **False**.

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

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

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

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

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

## To restart the RUM Engine Resolver

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

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

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

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

## Correlating Session ID Parameters

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

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

```
http://www.anycompany.com/~anand/Ticket_Confirm.jsp?BV_SessionID=@@@@1812057630.1043567934@@@@&BV_EngineID=cccdadchgidfmlmcefecehidfhdfdfk.0&value=0000144976
```

The URL is translated as follows:

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

The parameters to be ignored are defined per application server.

### To configure session ID parameters to be ignored

1. Open the `<Real User Monitor root directory>\conf\configurationmanager\Application_Server_Types_configuration.xml` file in a text editor.
2. Locate the application server type for which you are configuring the parameters to be ignored. This appears in the format `<AppServer name="app_server_name">`, where `app_server_name` is the name of the application server type. For example, for a Broadvision application server, the entry is:  
**`<AppServer name="BroadVision">`**
3. Under the application server name, in the section beginning with the **`<DiscardParameters>`** tag, is a list of the most common session ID parameters for that application server. You can add and delete parameters to create a list of all the parameters you want RUM to ignore during correlation. Parameters are entered in the format `<parameter>parameter_name</parameter>`, where `parameter_name` is the name of the parameter. For example, for a parameter called `BV_EngineID`, the entry is:  
**`<parameter>BV_EngineID</parameter>`**
4. If you want RUM to consider the parameters you enter as a regular expression instead of a string (which is the default), you add **`type="regEx"`** to the **`<DiscardParameters>`** tag. For example,  
**`<DiscardParameters type="regEx">`**
5. Under the application server name, in the line:  
**`<attribute name="enabled">>false</attribute>`**  
change **false** to **true**.
6. Save the file and exit the editor.

# Chapter 10: RUM Engine File Configuration

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

This chapter includes the following topics:

- ["Configuring Meaningful Page Names" below](#)
- ["Unifying Frames" on page 160](#)
- ["Configuring User Name Translation" on page 162](#)

## Configuring Meaningful Page Names

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

This section includes the following topics:

- ["About Discovered Page Names" below](#)
- ["Formatting Tags" on the next page](#)
- ["Rule Tags" on page 151](#)
- ["Sample XML File" on page 153](#)
- ["Validating Meaningful Name XML Files" on page 158](#)
- ["Adding and Deleting Meaningful Name XML Files" on page 159](#)
- ["Changing Meaningful Name XML Files" on page 159](#)
- ["Viewing Discovered Page Statistics" on page 159](#)

## About Discovered Page Names

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

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

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

```
\<Real User Monitor root directory>\conf\resolver\meaningful_pages\myapplication.xml
```

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

The XML file contains the following main sections:

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

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

## Formatting Tags

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

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

The following formatting tags can be used. For the XML schema to be validated (for details, see ["Validating Meaningful Name XML Files" on page 158](#)), the tags must appear in the XML file in the order in which they are listed below:

- ["URL Decoder" below](#)
- ["Rename" on the next page](#)
- ["Substring" on the next page](#)
- ["ExtractStrToStr" on the next page](#)
- ["ExtractIndexToStr" on page 145](#)
- ["ExtractStrToCount" on page 146](#)
- ["Insert" on page 147](#)
- ["ChangeCase" on page 148](#)
- ["Remove" on page 148](#)
- ["RemoveNonAlpha" on page 148](#)
- ["Replace" on page 149](#)
- ["Alias" on page 149](#)
- ["RegExExtract" on page 150](#)
- ["RegExMatch" on page 150](#)

## URL Decoder

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

<b>Syntax</b>	<code>&lt;URLDecoder Name="<b>Command_Name</b>" EncodingScheme="<b>Scheme</b>"/&gt;</code>
<b>Explanation</b>	<b>Command_Name.</b> The name of the Substring formatting tag that can be used in Rule tags. <b>Scheme.</b> The decoding scheme to be used.

<b>Example</b>	<pre>&lt;URLDecoder Name="DecodeUTF-8" EncodingScheme="UTF-8"/&gt;</pre> <p>When the DecodeUTF-8 formatting command is referenced in a rule, the string is decoded using the UTF-8 decoding scheme.</p>
<b>Note</b>	If the URLDeocder tag is used, but no encoding scheme is specified, the UTF-8 scheme is used by default.

## Rename

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

<b>Syntax</b>	<pre>&lt;Rename Name="<b>Command_Name</b>" NewName="<b>Rename_String</b>"/&gt;</pre>
<b>Explanation</b>	<p><b>Command_Name.</b> The name of the Rename formatting tag that can be used in Rule tags.</p> <p><b>Rename_String.</b> The string to be substituted for the source string.</p>
<b>Example</b>	<pre>&lt;Rename Name="RenameToABC123" String="AnyCompany"</pre> <p>When the <b>RenameToABC123</b> formatting command is referenced in a rule, the entire source string is renamed to <b>AnyCompany</b>.</p>

## Substring

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

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

## ExtractStrToStr

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



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

## ExtractIndexToStr

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

<b>Syntax</b>	<pre>&lt;ExtractIndexToStr Name="Command_Name" fromIndex="Start_Char_Index" toString="End_String" toInclude="Include_End_String" toOccurrences="Occurrences_End_String"/&gt;</pre>
---------------	--

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

## ExtractStrToCount

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

<b>Syntax</b>	<pre>&lt;ExtractStrToCount Name="<b>Command_Name</b>" fromString="<b>Start_String</b>" fromInclude="<b>Include_Start_String</b>" fromOccurrences="<b>Occurrences_Start_String</b>" Count="<b>Length</b>" /&gt;</pre> <p><b>Note:</b> The parameter names are case sensitive.</p>
---------------	--

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

## Insert

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

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

## ChangeCase

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

<b>Syntax</b>	<ChangeCase Name=" <b>Command_Name</b> " Type="Case_Type" BeginIndex=" <b>Start_Char_Index</b> " Count=" <b>Length</b> "/>
<b>Explanation</b>	<p><b>Command_Name.</b> The name of the ChangeCase formatting tag that can be used in Rule tags.</p> <p><b>Case_Type.</b> The type of conversion to be carried out. The valid options are:</p> <ul style="list-style-type: none"> <li>• <b>UpperCase.</b> Lower case to upper case. This is the default if no type is specified.</li> <li>• <b>LowerCase.</b> Upper case to lower case.</li> <li>• <b>OppositeCase.</b> Switches the case of characters.</li> </ul> <p><b>Start_Char_Index.</b> The position in the source string of the starting character to be converted. The first position in the source string is the zero index.</p> <p><b>Length.</b> The number of characters from the Start_Char to be converted.</p>
<b>Example</b>	<pre>&lt;ChangeCase Name="UpperCaseFirstChar" Type="UpperCase" BeginIndex="0" Count="1"/&gt;</pre> <p>When the <b>UpperCaseFirstChar</b> formatting command is referenced in a rule, the first character of the source string is converted to upper case.</p>
<b>Note</b>	If <b>Length</b> is not specified, the ChangeCase conversion is carried out from the <b>Start_Char</b> to the end of the source string.

## Remove

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

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

## RemoveNonAlpha

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

<b>Syntax</b>	<RemoveNonAlpha Name=" <b>Command_Name</b> ">
---------------	---

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

## Replace

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

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

## Alias

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

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

## RegExExtract

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

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

## RegExMatch

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

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

## Rule Tags

The second main section in the XML file is the rules section, which contains the logic for assigning a meaningful name to a page. The rules section is responsible for matching a page to a single rule and then using the formatting tags included in the rule to assign a meaningful name to the page. Matching is carried out on the different parts of the URL—URL protocol, URL path, URL host, and parameters (both the GET and POST parameters of a page).

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

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

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

### Rules format

Rules are written in the following format:

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

where:

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

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

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

- **Rule\_Name.** The name of the rule.
- **URL\_Path.** The URL path that is required for the rule to be applied.
- **URL\_Host.** The URL host that is required for the rule to be applied.
- **URL\_Protocol.** The URL protocol that is required for the rule to be applied. This option does not support the use of a wildcard.

- **Param\_Name.** The key (name) of a parameter in the URL that is required for the rule to be applied.
- **Param\_Value.** The value in the Param\_Name parameter that is required for the rule to be applied. Use "" to denote an empty parameter value.
- **Index\_Number.** The position that the formatted string occupies in the meaningful name to be created.
- **Format\_Name.** The name of the format to be used on the selected string to format it into a string that is used as part of the created meaningful name for a page. The format name must be one of the formats defined in the formatting section of the XML file (for details, see ["Formatting Tags" on page 143](#)). If no format name is specified, no formatting is applied to the input string, resulting in an identical output string that is used as part of the created meaningful name for a page.

**Note:** URL\_Path, URL\_Host, URL\_Protocol, Param\_Name, and Param\_Value are always in lower case.

### The following points apply to rules:

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

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

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

#### Note:

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

### Example of multiple formatting commands in separate Formatter tags:

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



```
<Formatter Index="2">Format_Name2</Formatter>
<Formatter Index="3">Format_Name3</Formatter>
</Path>
```

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

### Example of multiple formatting commands in the same Formatter tag:

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

Format\_Name1 is applied to the path **/mypath/home**; Format\_Name2 is applied to the output from Format\_Name1.

## Sample XML File

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

- ["XML File" below](#)
- ["Examples of Meaningful Names for URL" on page 157](#)

### XML File

```
<?xml version="1.0" ?>
- <Meaningful_Pages xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="./meaningfulpages.xsd">
- <Formatting>
  <Rename Name="RenameToWelcome" NewName="Welcome" />
  <Rename Name="RenameToSignIn" NewName="Sign In" />
  <Rename Name="RenameToStoreEntrance" NewName="Store Entrance" />
  <Rename Name="RenameToEditAccount" NewName="Edit Account" />
  <Rename Name="RenameToProduct" NewName="Product" />
  <Rename Name="RenameToCheckOut" NewName="Check Out" />
  <Rename Name="RenameToOrderSubmitted" NewName="Order Submitted" />
  <Rename Name="RenameToSignOut" NewName="Signed Out" />
  <SubString Name="ExtractTwoFirstLetters" BeginIndex="0" Count="2" />
  <SubString Name="ExtractItem" BeginIndex="20" Count="4" />
  <SubString Name="ExtractUpdate" BeginIndex="16" Count="6" />
  <SubString Name="ExtractCart" BeginIndex="22" Count="4" />
  <SubString Name="ExtractQuantities" BeginIndex="26" Count="10" />
  <Insert Name="AppendCategory" String="Category" ToIndex="0" />
  <Insert Name="AppendAddItemPrefix" String="Add Item" ToIndex="0" />
  <Insert Name="AppendToCartSuffix" String="to Cart" ToIndex="0"
CountFromBeginning="false" />
  <Insert Name="AppendRemoveItemPrefix" String="Remove Item" ToIndex="0" />
  <Insert Name="AppendFromCartSuffix" String="from Cart" ToIndex="0"
```

```
CountFromBeginning="false" />
  <Insert Name="InsertSpaceAfterOrder" String="" ToIndex="5" />
  <Insert Name="InsertSpaceAfterConfirm" String="" ToIndex="7" />
  <Insert Name="InsertNotAfterOrder" String="Not" ToIndex="6" />
  <ChangeCase Name="UpperCaseFirstChar" Type="UpperCase" BeginIndex="0" Count="1" />
  <ChangeCase Name="UpperCaseAll" Type="UpperCase" BeginIndex="0" />
  <ChangeCase Name="UpperCaseSixthLetter" Type="UpperCase" BeginIndex="6" Count="1" />
  <ChangeCase Name="UpperCaseEighthLetter" Type="UpperCase" BeginIndex="8" Count="1" />
  <Remove Name="RemoveNew" String="/jpetstore/shop/new" />
  <Remove Name="RemoveSHTML" String=".shtml" />
  <Replace Name="ReplaceNewWithConfirm" Old="/jpetstore/shop/new" New="Confirm" />
- <Alias Name="RelateLettersToCategory">
  <Pair Name="FI" Alias="Fish" />
  <Pair Name="K9" Alias="Dogs" />
  <Pair Name="RP" Alias="Reptiles" />
  <Pair Name="FL" Alias="Cats" />
  <Pair Name="AV" Alias="Birds" />
</Alias>
- <Alias Name="RelateProductIdToProductName">
  <Pair Name="FI-FW-01" Alias="'Koi'" />
  <Pair Name="FI-FW-02" Alias="'Goldfish'" />
  <Pair Name="FI-SW-01" Alias="'Angelfish'" />
  <Pair Name="FI-SW-02" Alias="'Tiger Shark'" />
  <Pair Name="K9-BD-01" Alias="'Bulldog'" />
  <Pair Name="K9-CW-01" Alias="'Chihuahua'" />
  <Pair Name="K9-DL-01" Alias="'Dalmation'" />
  <Pair Name="K9-PO-02" Alias="'Poodle'" />
  <Pair Name="K9-RT-01" Alias="'Golden Retriever'" />
  <Pair Name="K9-RT-02" Alias="'Labrador Retriever'" />
  <Pair Name="RP-LI-02" Alias="'Iguana'" />
  <Pair Name="RP-SN-01" Alias="'Rattlesnake'" />
  <Pair Name="FL-DLH-02" Alias="'Persian'" />
  <Pair Name="FL-DSH-01" Alias="'Manx'" />
  <Pair Name="AV-CB-01" Alias="'Amazon Parrot'" />
  <Pair Name="AV-SB-02" Alias="'Finch'" />
</Alias>
- <Alias Name="RelateItemNameToItemDesc">
  <Pair Name="EST-28" Alias="'Adult Female Golden Retriever'" />
  <Pair Name="EST-27" Alias="'Adult Female Chihuahua'" />
  <Pair Name="EST-26" Alias="'Adult Male Chihuahua'" />
  <Pair Name="EST-25" Alias="'Adult Female Labrador Retriever'" />
  <Pair Name="EST-24" Alias="'Adult Male Labrador Retriever'" />
  <Pair Name="EST-23" Alias="'Adult Female Labrador Retriever'" />
  <Pair Name="EST-22" Alias="'Adult Male Labrador Retriever'" />
  <Pair Name="EST-21" Alias="'Adult Female Goldfish'" />
  <Pair Name="EST-20" Alias="'Adult Male Goldfish'" />
  <Pair Name="EST-19" Alias="'Adult Male Finch'" />
  <Pair Name="EST-18" Alias="'Adult Male Amazon Parrot'" />
  <Pair Name="EST-17" Alias="'Adult Male Persian'" />
  <Pair Name="EST-16" Alias="'Adult Female Persian'" />
```

```
<Pair Name="EST-15" Alias="'With tail Manx'" />
<Pair Name="EST-14" Alias="'Tailless Manx'" />
<Pair Name="EST-13" Alias="'Green Adult Iguana'" />
<Pair Name="EST-12" Alias="'Rattleless Rattlesnake'" />
<Pair Name="EST-11" Alias="'Venomless Rattlesnake'" />
<Pair Name="EST-10" Alias="'Spotted Adult Female Dalmation'" />
<Pair Name="EST-9" Alias="'Spotless Male Puppy Dalmation'" />
<Pair Name="EST-8" Alias="'Male Puppy Poodle'" />
<Pair Name="EST-7" Alias="'Female Puppy Bulldog'" />
<Pair Name="EST-6" Alias="'Male Adult Bulldog'" />
<Pair Name="EST-5" Alias="'Spotless Koi'" />
<Pair Name="EST-4" Alias="'Spotted Koi'" />
<Pair Name="EST-3" Alias="'Toothless Tiger Shark'" />
<Pair Name="EST-2" Alias="'Small Angelfish'" />
<Pair Name="EST-1" Alias="'Large Angelfish'" />
</Alias>
</Formatting>
- <Rules DefaultDelimiter="">
- <Rule Priority="0" Name="Welcome">
- <Path Name="/jpetstore/">
  <Formatter Index="1">RenameToWelcome</Formatter>
</Path>
</Rule>
- <Rule Priority="1" Name="Welcome">
- <Path Name="/jpetstore/index.html">
  <Formatter Index="1">RenameToWelcome</Formatter>
</Path>
</Rule>
- <Rule Priority="2" Name="Sign In">
- <Path Name="/jpetstore/shop/signonForm.shtml">
  <Formatter Index="1">RenameToSignIn</Formatter>
</Path>
</Rule>
- <Rule Priority="3" Name="Store Entrance">
- <Path Name="/jpetstore/shop/signon.shtml">
  <Formatter Index="1">RenameToStoreEntrance</Formatter>
</Path>
</Rule>
- <Rule Priority="4" Name="Category [any]">
  <Path Name="/jpetstore/shop/viewCategory.shtml" />
- <Parameters>
- <Param Key="categoryId" Value="*" CompareMethod="Wildcard">
  <Formatter Index="1">UpperCaseAll AppendCategory</Formatter>
</Param>
</Parameters>
</Rule>
- <Rule Priority="5" Name="Edit Account">
- <Path Name="/jpetstore/shop/editAccountForm.shtml">
  <Formatter Index="1">RenameToEditAccount</Formatter>
</Path>
```

```
</Rule>
- <Rule Priority="6" Name="Any Product [product]">
  <Path Name="/jpetstore/shop/v*Product.shtml" CompareMethod="WildCard" />
- <Parameters>
- <Param Key="productId" Value="*" CompareMethod="WildCard">
  <Formatter Index="1">ExtractTwoFirstLetters RelateLettersToCategory</Formatter>
  <Formatter Index="2">RenameToProduct</Formatter>
  <Formatter Index="3">RelateProductIdToProductName</Formatter>
</Param>
</Parameters>
</Rule>
- <Rule Priority="7" Name="Item [any]">
- <Path Name="/jpetstore/shop/viewItem.shtml">
  <Formatter Index="1">ExtractItem UpperCaseFirstChar</Formatter>
</Path>
- <Parameters>
- <Param Key="itemId" Value="*" CompareMethod="WildCard">
  <Formatter Index="2">RelateItemNameToItemDesc</Formatter>
</Param>
</Parameters>
</Rule>
- <Rule Priority="8" Name="Add Item [any] To Cart">
  <Path Name="/jpetstore/shop/addItemToCart.shtml" />
- <Parameters>
- <Param Key="workingItemId" Value="*" CompareMethod="WildCard">
  <Formatter Index="1">RelateItemNameToItemDesc AppendAddItemPrefix
AppendToCartSuffix</Formatter>
</Param>
</Parameters>
</Rule>
- <Rule Priority="9" Name="Update Cart">
- <Path Name="/jpetstore/shop/updateCartQuantities.shtml">
  <Formatter Index="1">ExtractUpdate UpperCaseFirstChar</Formatter>
  <Formatter Index="2">ExtractCart UpperCaseFirstChar</Formatter>
  <Formatter Index="3">ExtractQuantities UpperCaseFirstChar</Formatter>
</Path>
</Rule>
- <Rule Priority="10" Name="Remove Item [any] From Cart">
  <Path Name="/jpetstore/shop/removeItemFromCart.shtml" />
- <Parameters>
- <Param Key="workingItemId" Value="*" CompareMethod="WildCard">
  <Formatter Index="1">RelateItemNameToItemDesc AppendRemoveItemPrefix
AppendFromCartSuffix</Formatter>
</Param>
</Parameters>
</Rule>
- <Rule Priority="11" Name="Check Out">
- <Path Name="/jpetstore/shop/checkout.shtml">
  <Formatter Index="1">RenameToCheckOut</Formatter>
</Path>
```

```

    </Rule>
  - <Rule Priority="12" Name="Order Form">
  - <Path Name="/jpetstore/shop/newOrderForm.shtml">
    <Formatter Index="1">RemoveNew InsertSpaceAfterOrder RemoveSHTML UpperCaseFirstChar
    UpperCaseSixthLetter</Formatter>
  </Path>
  </Rule>
  - <Rule Priority="13" Name="Order Submitted">
  - <Path Name="/jpetstore/shop/newOrder.shtml">
    <Formatter Index="1">RenameToOrderSubmitted</Formatter>
  </Path>
  - <Parameters>
    <Param Key="confirmed" Value="true" />
  </Parameters>
  </Rule>
  - <Rule Priority="14" Name="Order Not Submitted">
  - <Path Name="/jpetstore/shop/newOrder.shtml">
    <Formatter Index="1">RenameToOrderSubmitted InsertNotAfterOrder</Formatter>
  </Path>
  - <Parameters>
    <Param Key="confirmed" Value="false" />
  </Parameters>
  </Rule>
  - <Rule Priority="15" Name="Confirm Order">
  - <Path Name="/jpetstore/shop/newOrder.shtml">
    <Formatter Index="1">ReplaceNewWithConfirm InsertSpaceAfterConfirm RemoveSHTML
    UpperCaseEighthLetter</Formatter>
  </Path>
  </Rule>
  - <Rule Priority="16" Name="Sign Out">
  - <Path Name="/jpetstore/shop/signoff.shtml">
    <Formatter Index="1">RenameToSignOut</Formatter>
  </Path>
  </Rule>
</Rules>
</Meaningful_Pages>

```

### Examples of Meaningful Names for URL

URL	Meaningful Name
http://pluto:8080/jpetstore/	Welcome
http://pluto:8080/jpetstore/index.html	Welcome
http://pluto:8080/jpetstore/shop/signonForm.shtml	Sign In
http://pluto:8080/jpetstore/shop/signon.shtml	Store Entrance
http://pluto:8080/jpetstore/shop/viewCategory.shtml?categoryId=CATS	Category CATS

URL	Meaningful Name
http://pluto:8080/jpetstore/shop/editAccountForm.shtml	Edit Account
http://pluto:8080/jpetstore/shop/viewProduct.shtml?productId=FI-FW-01	Fish Product 'Koi' (FI=Fish, K9=Dogs, RP=Reptiles, FL=Cats, AV=Birds)
http://pluto:8080/jpetstore/shop/viewItem.shtml?itemId=EST-4	Item 'Spotted Koi'
http://pluto:8080/jpetstore/shop/addItemToCart.shtml?workingItemId=EST-6	Add Item 'Male Adult Bulldog' to Cart
http://pluto:8080/jpetstore/shop/updateCartQuantities.shtml	Update Cart Quantities
http://pluto:8080/jpetstore/shop/removeItemFromCart.shtml?workingItemId=EST-6	Remove Item 'Male Adult Bulldog' from Cart
http://pluto:8080/jpetstore/shop/checkout.shtml	Check Out
http://pluto:8080/jpetstore/shop/newOrderForm.shtml	Order Form
http://pluto:8080/jpetstore/shop/newOrder.shtml	Confirm Order
http://pluto:8080/jpetstore/shop/newOrder.shtml?confirmed=true	Order Submitted
http://pluto:8080/jpetstore/shop/newOrder.shtml?confirmed=false	Order Not Submitted
http://pluto:8080/jpetstore/shop/signoff.shtml	Signed Out

## Validating Meaningful Name XML Files

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

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

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

### To validate a meaningful name XML file:

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

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

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

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

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

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

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

**Note:** The Formatting tags must be included in the XML file in a specific order (for details, see ["Formatting Tags" on page 143](#)). If the Formatting tags are not in the correct order, a validation error message is displayed, but no indication of the order mismatch is given.

## Adding and Deleting Meaningful Name XML Files

If you add or delete a meaningful name XML file in an application in End User Management Administration and would like to apply the change immediately, you can force RUM to reread the End User Management Administration configuration. In the RUM Engine web console, synchronize configuration data by selecting **Tools > Monitoring Configuration Information > Sync All Configuration**. For details, see ["Monitoring Configuration Information" on page 123](#).

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

## Changing Meaningful Name XML Files

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

### To force RUM to reload the configuration for an application:

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

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

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

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

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

## Viewing Discovered Page Statistics

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

### To view discovered page statistics:

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

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

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

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

UI Element	Description
<b>Application name</b>	The name of the application as defined in End User Management Administration. (For details on configuring applications in End User Management Administration, see "RUM Application Configuration Wizard" in the APM Application Administration Guide.)
<b>Configuration file name</b>	The name of the meaningful name XML file used by the application.
<b>Published pages</b>	The total number of pages monitored in the application published to the meaningful pages module.
<b>Successful pages</b>	The total number of pages that were successfully processed by the meaningful pages module.
<b>Unmatched pages</b>	The total number of pages successfully processed by the meaningful pages module, but for which no meaningful name was assigned as no match was found.
<b>Failed pages</b>	The total number of pages that were not successfully processed by the meaningful pages module.

## Unifying Frames

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

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

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

### To change the default settings for frame unification

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



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

3. Change the settings for your system, where:

- **TimeoutMS.** The amount of time it takes a frame to load after the previous frame has finished loading. Within this time, if the frame matches the other parameters, such as the referring URL, it is considered as a child of the previous frame, otherwise it is considered as a parent frame.
- **InnerFrames maxInnerFrame.** The maximum number of children that a parent frame can contain. Use **-1** for an unlimited number.
- **CanBeInnerFrame.** Set to **true** to enable frames to be considered as children. Set to **false** to consider all frames as parents, unless specific page settings have been defined which are applicable to a frame.
- **MatchInnerFramesReferrer.** Set to **true** to allow child frames to be matched to parent frames by URLs (if specific page settings have been configured), or **false** to use only the TimeoutMS setting to create child pages.

4. Save the file and exit.

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

## To create frame unification settings for specific pages

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

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

where:

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

Within this time, the frame is considered as a child of the parent frame that matches the first **Pattern** setting, otherwise it is considered as a parent frame itself.

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

**Note:**

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

## Configuring User Name Translation

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

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

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

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

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

```
<Resolver name="CSVLoginUserNameResolver">

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

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

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

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

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

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

# Chapter 11: Configuring the RUM Sniffer Probe

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

This chapter includes the following topics:

- ["Changing the Protocol for Accessing the RUM Probe" below](#)
- ["Configuring the RUM Probe for I18N" below](#)
- ["Changing the Header in Which to Locate Client IP Addresses" on the next page](#)
- ["Creating Default Configuration and Properties Files for a Specific Probe" on the next page](#)
- ["Configuring the RUM Probe to Support Multiprotocol Label Switching \(MPLS\)" on page 166](#)

## Changing the Protocol for Accessing the RUM Probe

The default protocol used for accessing the RUM Probe is HTTPS with a client certificate. In the RUM Engine web console, you can manually configure the protocol used to access the RUM Probe. For details, see ["Probe Configuration Dialog Box" on page 105](#).

## Configuring the RUM Probe for I18N

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

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

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

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

where:

- **<false/true>**. Set to **true** to enable RUM to support I18N by using character sets other than UTF-8. The default setting is **false**.
- **<length>**. The number of bytes in the page content in which RUM searches for a character set. By default, RUM does not search the page content for a character set and only searches the page header. The maximum permissible length is 1024 characters.
- **<name>**. The default character set to use, if RUM does not locate a character set in either the page header or content. Valid character sets are those that are by default supported by the ICU library.

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

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

## Changing the Header in Which to Locate Client IP Addresses

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

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

1. In the **<RUM root directory>\conf\configurationmanager\Beatbox\_Default\_Const\_Configuration.xml** file on the RUM Engine, under the **[global]** section, add the following line:  
forwarded\_for\_header <HEADER\_NAME>  
where <HEADER\_NAME> is the name of the new header to use for locating client IP addresses.
2. In the RUM Engine web console, synchronize configuration data by selecting **Tools > Monitoring Configuration Data > Sync All Configuration**. For details, see ["Monitoring Configuration Information" on page 123](#).

## Creating Default Configuration and Properties Files for a Specific Probe

The RUM Engine uses the same, default, static configuration file and properties file for all the probes attached to it. You can create individual, static configuration and properties files for a specific probe, so that it will be configured with specific settings, instead of the general, default ones.

**To create a default configuration file for a specific probe**

1. On the RUM Engine, in the **<RUM root directory>\conf\configurationmanager** directory, make a copy of the **Beatbox\_Default\_Const\_Configuration.xml** file.
2. Rename the copy of the file, substituting **Default** with the name of the probe as configured in RUM. For example:

```
Beatbox_123.4.5.67_Const_Configuration.xml
```

3. Edit the file as required with the configuration settings for the specific probe.

**To create a default properties file for a specific probe**

1. On the RUM Engine, in the **<RUM root directory>\conf\probes** directory, make a copy of the

probe.default.properties file.

2. Rename the copy of the file, substituting **default** with the name of the probe as configured in RUM. For example:

```
probe.123.4.5.67.properties
```

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

## Configuring the RUM Probe to Support Multiprotocol Label Switching (MPLS)

By default, the RUM Probe does not support MPLS.

**To enable MPLS support:**

1. Edit the `<RUM root directory>\conf\configurationmanager\Beatbox_Default_Const_Configuration.xml` file on the RUM Engine.
2. Under the `[collector]` section, add the following line:

```
mpls_levels 0
```

Setting the level to 0, instead of to a specific number, configures the probe to calculate the number of MPLS levels needed for the monitored traffic automatically.

3. Save the file.

## Configuring the RUM Probe to GRE Support Encapsulated Remote Switch Port Analyzer (ERSPAN)

By default, the RUM Probe does not support GRE (ERSPAN).

**To enable GRE (ERSPAN) support:**

1. Edit the `<RUM root directory>\conf\configurationmanager\Beatbox_Default_Const_Configuration.xml` file on the RUM Engine.
2. Under the `[collector]` section, add the following lines:

```
process_gre true
```

If it is a fake erspan (fake erspan packets do not have the ERSPAN header), add the following

```
enable_fake_erspan_mode true
```

3. Save the file.

## Configuring the RUM Probe if Extended Master Secret Exists in SSL Handshake

Extended Master Secret provides an additional security layer for TLS/SSL communications (see <https://tools.ietf.org/html/rfc7627> for more information). Some application and web servers have started supporting Extended Master Secret. However, enabling Extended Master Secret decryption can cause a

degradation in performance in RUM and may also cause an increase in the memory footprint. Therefore, Extended Master Secret decryption is disabled by default in configurations created in APM.

However, if the RUM Probe log shows that there are too many decrypting or package loss errors, you should determine if Extended Master Secret is being used. If it is, then you will need to enable Extended Master Secret decryption in RUM to reduce decryption errors.

To determine if Extended Master Secret is used and enable it:

1. Open the capture log and see if there is an error message that looks something like this:  

```
017-06-06 11:16:41 [5176] DEBUG sniffer.SSL
<..\..\..\collector\sniffer\TransactionDecoder.cpp:1622> - the record's padding/AEAD-
authenticator is invalid or, if sending, an internal error occurred.
```

2. If the error message in step 1 appears:
  - a. Open the captured SSL traffic (as pcap) using tcpdump/wireshark on wireshark and apply the filter **ssl.handshake**.
  - b. Locate and select the **Server Hello, Certificate, Server Hello Done** line.

No.	Time	Source	Destination	Protocol	Length	Sequence number	ix:Forwarded-For	Stream index	Type	Info
4	0.005245	49.33.30.125	10.16.15.14	TLSv1.2	234	1		0	0	Client Hello
5	0.005801	10.16.15.14	49.33.30.125	TLSv1.2	2908	1		0	0	Server Hello, Certificate, Server Hello Done
9	0.160948	49.33.30.125	10.16.15.14	TLSv1.2	408	169		0	0	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.162781	10.16.15.14	49.33.30.125	TLSv1.2	141	2835		0	0	Change Cipher Spec, Encrypted Handshake Message

- c. In the lower screen, expand **Secure Sockets Layer > TLSv1 Recorded Layer: Handshake Protocol: Server Hello > Handshake Protocol: Server Hello**.
- d. Search for **Extension: Extended Master Secret**.

```

---Version: TLS 1.2 (0x0303)
---Length: 2829
[-] Handshake Protocol: Server Hello
  ---Handshake Type: Server Hello (2)
  ---Length: 81
  ---Version: TLS 1.2 (0x0303)
  [+ Random
    ---Session ID Length: 32
    ---Session ID: 1c3c0000688f65d6925501c441488b24833080096ae7ec11...
    ---Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
    ---Compression Method: null (0)
    ---Extensions Length: 9
    [-] Extension: Extended Master Secret
      ---Type: Extended Master Secret (0x0017)
      ---Length: 0
    [+ Extension: renegotiation_info
  [+ Handshake Protocol: Certificate
  [+ Handshake Protocol: Server Hello Done
  
```

3. If **Extension: Extended Master Secret** exists:
  - a. Open the **<Real User Monitor root directory>\conf\configurationmanager\Beatbox\_Default\_Const\_Configuration.xml** file.
  - b. In the global section, add the line **use\_extended\_master\_key true**.

# Chapter 12: Administering the MySQL Database

For RUM to work, it must be connected to a MySQL database that has been created and started.

This chapter includes the following topics:

- ["Overview of the MySQL Database" below](#)
- ["Creating and Connecting to the MySQL Database" below](#)
- ["Starting and Stopping the MySQL Database" on the next page](#)
- ["Maintaining the MySQL Database" on page 170](#)

## Overview of the MySQL Database

The MySQL database is the RUM's data repository. The data that is stored in the MySQL database is data that is either not forwarded at all to APM, or that is only sent on request.

Data that is not forwarded at all to APM is RUM configuration data. Data that is sent to APM on request is open session data and session clickstream data (data and snapshots of pages included in sessions). Clickstream data accounts for the majority of the data stored in the MySQL database.

The MySQL database can be installed on the same machine as the RUM Engine or on its own machine. For system requirements for the MySQL database, see "Reviewing System Requirements" in the Real User Monitor Installation and Upgrade Guide.

**Note:** If you are upgrading your MySQL database from version 5.5 to 5.7, see "Upgrading MySQL from version 5.5 to 5.7" in the RUM Installation and Upgrade Guide.

## Creating and Connecting to the MySQL Database

The RUM Engine MySQL database is created during the RUM Engine installation process, if that option is selected. When the MySQL database is created during the installation process, the RUM Engine is connected to it, and the MySQL database is started automatically. The MySQL database to which the RUM Engine is connected must be started for the RUM Engine to work.

You can create a new MySQL database schema and connect the RUM Engine to it, or connect the RUM Engine to a different, existing MySQL database completely, if required.

**Note:** The RUM Engine can only be connected to one MySQL database.

### To create schemas and connect to MySQL databases on a RUM Windows installation:

On the machine on which the RUM Engine is installed, open **RUM Configuration Tool** on the computer's Start menu. The RUM Configuration tool starts. For details on working with the RUM Configuration tool, see "RUM Configuration Wizard" in the Real User Monitor Installation and Upgrade Guide.



## Starting and Stopping the MySQL Database

When the MySQL database is created during RUM installation, it is started automatically as part of the process. You can start and stop the MySQL database manually if required.

**Note:** When stopping or starting the MySQL database, make sure that the RUM Engine is disabled. You can confirm that the Rum Engine is disabled in the Task Manager.

### To start the MySQL database:

1. Ensure that the RUM Engine is stopped. If not, on the machine on which the RUM Engine is installed, run **Disable Real User Monitor** on the computer's Start menu.
2. Run **Start Real User Monitor Database** on the computer's Start menu.
3. Run **Enable Real User Monitor** on the computer's Start menu.

### To stop the MySQL database:

1. Ensure that the RUM Engine is stopped. If not, on the machine on which the RUM Engine is installed, run **Disable Real User Monitor** on the computer's Start menu.
2. Run **Stop Real User Monitor Database** on the computer's Start menu.

## Changing the MySQL Database User Password

When the MySQL database is created during RUM installation, a user name and password is created.

### To change the MySQL database user password:

1. Ensure that the RUM Engine is stopped. If not, on the machine on which the RUM Engine is installed, run **Disable Real User Monitor** on the computer's Start menu.
2. From a Windows Command Prompt window, login to the MySQL console.
3. Connect to the SQL database using your current user name and password.

```
C:\<RUM Home>\MySQL\bin>mysql -h localhost --user=user_name -p
```

4. Show the available database schemas.

```
mysql> show databases;
+-----+
| Database          |
+-----+
| information_schema |
| mysql             |
| performance_schema |
| rumdb234          |
| test              |
+-----+
```

5. Access your database schema.

```
mysql>use rumdb234;
```

6. Create new password for the selected MySQL database schema.

```
mysql> set password for 'rum_user'@'localhost' = PASSWORD('new_password');
```

7. Close the Windows Command Prompt window.
8. Run the RUM configuration wizard. On the machine on which the RUM Engine is installed, open **RUM Configuration Tool** on the computer's Start menu.
9. On the Connect to Database page, select **Connect to RUM database**.
10. On the MySQL Database Properties page, enter the new password.

## Maintaining the MySQL Database

For details on maintaining the MySQL database, including strategies and procedures for backing up and restoring the database, refer to the Database Administration chapter in the MySQL Reference Manual on the MySQL web site (<http://dev.mysql.com/doc/#manual>).

### Purging MySQL Binary Log Files

The MySQL binary log contains all statements that updated data in the MySQL database.

The purpose of the binary log is to help update the database to the most current status during a restore operation, as it contains all updates made since the last backup. For details on MySQL binary log files and restoring databases, refer to the Database Administration chapter in the MySQL Reference Manual on the MySQL web site (<http://dev.mysql.com/doc/#manual>).

RUM purges the MySQL binary log files on a daily basis, by deleting all the log files older than five days. You can change the default number of days for which to keep the MySQL binary log files.

#### To change the default number of days for which to keep MySQL binary log files:

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

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

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

2. In the JMX Agent View, scroll down to the **RUM.modules** section and click **service=MaintenanceDBConfigurationJMX**.
3. In the **MySQLBinaryLogsDaysCount** parameter, change the setting to the required number of days.
4. Click the **Apply Changes** button.

### Purging MySQL Real User Monitor Data

The data stored in the MySQL database is raw data used by Real User Monitor reports to present session clickstreams and snapshots, and to enable queries for various report filters. The data is sent to Application Performance Management on request.

Raw data is kept in the MySQL database for a default period of 14 days, after which it is automatically purged from the database. The amount of time raw data is stored in the MySQL database can be changed to any number of days between 7 and 100.

**To change the period of time that raw data is stored in the database:**

1. Edit the `<RUM root directory>\conf\partitionmanager\pm_tables_config.xml` file on the RUM Engine machine.
2. Change the setting `<archiveDuration units="DAYS" qty="14"/>` from 14 to the required number of days.
3. Save the file.
4. After changing the default Purging policy in RUM, open APM and change the RUM data purging settings:
  - a. In APM, click **Admin > Platform > Infrastructure Settings**.
  - b. Select **Applications > End User/System Availability Management**.
  - c. In the End User/System Availability Management - Data table, locate **Number of days back to include data in RUM reports** and change the value to the new value you just configured in RUM.

**Note:** By increasing the number of days for which session clickstream data is stored, you may significantly increase the size of the database, which may necessitate additional disk capacity.

# Chapter 13: Hardening RUM

You can harden the RUM platform so that it can be part of a secure architecture, and can therefore meet the challenge of dealing with security threats to which it could potentially be exposed.

This chapter includes the following topics:

- ["Hardening the RUM Sniffer Probe" below](#)
- ["Securing Connections to the RUM Engine" on page 175](#)

**Note:** For details on securing connections between RUM and APM, see the APM Hardening Guide.

## Hardening the RUM Sniffer Probe

You can harden the RUM Sniffer Probe by changing users and creating passwords for them, disabling non-SSH access, limiting the SSH version that can be used, and by securing the http connection to the probe.

This section includes the following topics:

- ["Changing the Probe's User and Password" below](#)
- ["Limiting Access to the Probe" on the next page](#)
- ["Limiting the SSH Version" on the next page](#)
- ["Securing the HTTP Connection to the Probe" on the next page](#)

## Changing the Probe's User and Password

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

When the RUM Probe is installed, a user called **rum\_probe** is automatically created, which has access to the probe channels only. This user does not have a password and you should configure one for it.

By default, the RUM Probe is run under the **root** user. It is recommended to run the probe process under the **rum\_probe** user, or another specially created user, rather than the **root** user.

### To change the user that runs the probe process

1. Log on to the probe as the **root** user.
2. Change the user running the probe process by executing the command:

```
rp_user.pl <USER>
```

where <USER> is the name of the user with which you want to run the probe process.

### To configure a password for a user

1. Log on to the probe as the **root** user.
2. Define a password for the user by executing the command:

```
passwd <USER>
```

where <USER> is the name of the user for which you are defining the password. For example, to configure a password for the **rum\_probe** user, execute the command:

```
passwd rum_probe
```

3. Follow the on-screen prompts.

## Limiting Access to the Probe

The RUM Engine connects to the RUM Probe via the probe's web console. It is recommended to limit access to the RUM Probe by disabling access to other, unnecessary services according to your organization's security policies.

## Limiting the SSH Version

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

By default, Linux accepts both SSH 1 and SSH 2 connections. To increase security, it is recommended to configure Linux to accept SSH 2 connections only.

### To configure Linux to accept SSH 2 connections only:

On the RUM Probe machine, edit the `/etc/ssh/sshd_config` file and change the line:

```
#Protocol 2,1  
to  
Protocol 2
```

## Securing the HTTP Connection to the Probe

You can secure the http connection to the probe by using https connections.

In RUM version 7.0 and later, the RUM Engine by default connects to the probe via an https connection, using default server and client certificates. In some instances (for example, after upgrading an earlier version of RUM) it might be necessary to manually configure RUM to use https.

This section describes how to manually set an https connection to the probe, as well as how to replace the default, generic, server and client certificates that are included in the probe.

**Note:** On Windows installations of the probe, the `/etc/rum_probe` directory is located in the RUM Probe root directory.

### To manually set an https connection to the probe

1. Log on to the probe machine and edit the `/etc/rum_probe/rpsecurity.conf` file.
2. Uncomment, edit or add the following line:

```
use_ssl true
```

3. Restart the probe:
  - For Linux installations use the command `/etc/init.d/rum_probe-capture restart`
  - For Windows installations execute **Start RUMProbe** on the computer's Start menu.

4. On the engine machine, edit the `\<RUM root directory>\conf\probes\probe.<PROBE IP>.properties` file, where `<PROBE IP>` is the IP address of the probe machine for which you are configuring basic authentication. If this file does not exist, create it.

5. Uncomment, edit or add the following line:

```
connection.http.ssl=true
```

6. Force an update of the probe configuration by accessing the RUM web console and selecting **Tools > Monitoring Configuration Information > Sync All Configuration**. For details on working with the RUM web console, see ["Using the RUM Web Console" on page 40](#).

## To replace the default server certificate

1. Convert the new server certificate and private key to PEM (base64) format, unencrypted (that is, without a password) and copy them to the probe machine.
2. Log on to the probe machine and edit the `/etc/rum_probe/rpsecurity.conf` file.
3. Uncomment, edit or add the following lines:

```
ssl_key <PRIVATE_KEY_FILE>  
ssl_cert <SERVER_CERTIFICATE>
```

**Note:** The certificate and private key can be included in the same file. In such cases, both lines should refer to that file.

4. Restart the probe:
  - For Linux installations use the command `/etc/init.d/rum_probe-capture restart`
  - For Windows installations execute **Start RUMProbe** on the computer's Start menu.

5. Copy the server certificate (without the private key) to the engine machine.
6. Import the certificate into a new or existing keystore with the command:

```
\<RUM root directory>\JRE\bin\keytool -import -alias rum_probe_cert -keystore  
<KEYSTORE_FILE> -file <CERTIFICATE_FILE>
```

**Note:** The RUM Engine should be configured to trust the imported certificate.

7. Edit the `\<RUM root directory>\conf\probes\probe.<PROBE IP>.properties` file. If this file does not exist, create it.
8. Uncomment, edit or add the following lines:

```
connection.http.ssl.truststore.file=<KEYSTORE_FILE>  
connection.http.ssl.truststore.password=<KEYSTORE_PASSWORD>
```

9. Force an update of the probe configuration by accessing the RUM web console and selecting **Tools > Monitoring Configuration Information > Sync All Configuration**. For details on working with the RUM web console, see ["Using the RUM Web Console" on page 40](#).

## To replace the default client certificate

1. On the engine machine, generate a new private key and certificate into a new, or existing keystore with the command:

```
\<RUM root directory>\JRE\bin\keytool -genkey -alias rum_probe_client_cert -keyalg  
RSA -keystore <KEYSTORE_FILE>
```

2. Enter the details of the certificate and when prompted, approve them.

**Note:** If you choose a different password for the private key than the keystore password you must also specify this password when configuring the engine to use the keystore (see no. 3).

3. Edit the `\<RUM root directory>\conf\probes\probe.<PROBE IP>.properties` file. If this file does not exist, create it.

4. Uncomment, edit or add the following lines:

```
connection.http.ssl.keystore.file=<KEYSTORE_FILE >  
connection.http.ssl.keystore.password=<KEYSTORE PASSWORD>
```

If you chose a different password for the private key in step 2, edit or add the following line:

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

5. Export the client certificate with the command:

```
\<RUM root directory>\JRE\bin\keytool -export -rfc -alias rum_probe_client_cert -  
keystore <KEYSTORE_FILE> -file <CERTIFICATE_FILE>
```

6. Copy the certificate file to the probe machine
7. Log on to the probe and edit the `/etc/rum_probe/rpsecurity.conf` file
8. Uncomment, edit or add the following line:

```
ssl_ca_file <CLIENT_CERTIFICATE_FILE>
```

9. Restart the probe:

- For Linux installations use the command `/etc/init.d/rum_probe-capture restart`
- For Windows installations execute **Start RUMProbe** on the computer's Start menu.

10. Force an update of the probe configuration by accessing the RUM web console and selecting **Tools > Monitoring Configuration Information > Sync All Configuration**. For details on working with the RUM web console, see ["Using the RUM Web Console" on page 40](#).

## Securing Connections to the RUM Engine

You can access the RUM Engine by different http access points, for the following purposes:

- RUM web console
- RUM JMX console
- RUM Gateway/Proxy Server (for APM and the replay applet)

You can secure access to the RUM Engine by using authentication and https connections.

This section includes the following topics:

- ["Using Authentication" on the next page](#)
- ["Using HTTPS" on the next page](#)

## Using Authentication

All http access points on the RUM Engine are protected via authentication mechanisms. The two main authentication mechanisms used are:

- **User and password protection.** Used for access to the RUM Engine web and JMX consoles.
- **Basic authentication.** Used for all other access points to the RUM Engine.

You can add users for access to the web console and change passwords for users to access both the web and JMX consoles. For details on adding, changing, and deleting users to access the web console, and changing their passwords, see ["Using the RUM Web Console" on page 40](#).

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

1. On the engine machine, edit the `\<RUM root directory>\EJBContainer\server\mercury\conf\users.xml` file.
2. In the appropriate line, enter the new password in the **password** parameter.
3. Ensure that the **encryptedPassword** parameter is blank and the **Roles** parameter value is **RUMAdmin**.
4. Save the file and restart the engine.

## Using HTTPS

When you configure the RUM Engine to work with https, all connections to the engine are affected. This means that Application Performance Management must also be configured to communicate with the RUM Engine using https. For details on hardening Application Performance Management, including creating, configuring, and trusting client and server certificates, see the APM Hardening Guide.

In APM, when viewing session details in RUM reports, you can view snapshots of pages and replay a session. By default, the Session Replay applet retrieves data from the RUM Engine via the APM Gateway Server, but can be configured to retrieve data directly from the RUM Engine (for details, see "Determining How the RUM Snapshot Applet Retrieves Snapshots" in the APM User Guide). If the Session Replay applet is configured to retrieve data directly from the RUM Engine and the RUM Engine is configured to require a client certificate, you must copy and import the necessary certificate on the client machine running the Session Replay applet.

### To copy and import a client certificate on a machine running the Session Replay applet:

1. Export the certificate from the keystore on the RUM Engine with the command:

```
\<RUM root directory>\JRE\bin\keytool -export -rfc -alias rum_client_cert -keystore <KEystore_FILE> -file <CERTIFICATE_FILE>
```

2. For each client machine on which the Session Replay applet is run:
  - a. Copy the certificate exported in step 1 to the client machine.
  - b. Import the certificate to the default APM truststore with the command:

```
<Latest JRE home>\bin\keytool -import -alias rum_client_cert -keystore > -keystore <Latest JRE home>\JRE\lib\security\cacerts" -file <CERTIFICATE_FILE>
```

**Tip:** We recommend that you locate truststore and keystore files outside of the `<Real User Monitor Engine root directory>` to avoid possible upgrade issues.

- c. Restart the browser.



**Note:** We recommend that you configure the Session Replay applet to retrieve data from the RUM Engine via the APM Gateway Server, when the RUM Engine is configured to require a client certificate.

# Chapter 14: Deploying RUM in a SiteMinder Environment

You use the RUM SiteMinder identity adapter to work with the SiteMinder Web Agent that enables retrieving the USER's attributes from the SiteMinder Server Policy Server.

This chapter includes the following topics:

- ["Overview" below](#)
- ["Prerequisites" below](#)
- ["System Flow" on the next page](#)
- ["Configuring the SiteMinder Policy Server" on the next page](#)
- ["Installing and Configuring the SiteMinder Web Agent" on page 183](#)
- ["Configuring the Web Server" on page 184](#)
- ["Configuring the RUM Engine" on page 188](#)
- ["Changing the Configuration of the TCP Port" on page 188](#)
- ["Testing and Troubleshooting" on page 189](#)

## Overview

**Note:** This chapter describes the configuration of Internet Information Server (IIS) 6.0 for Windows 2003 only. (While neither Apache Server nor IIS 7.0 configurations are included, they are supported and are conceptually the same.)

This chapter is intended for system administrators experienced in the configuration and maintenance of the following components:

- IIS
- SiteMinder Policy Server
- SiteMinder Web Agent
- RUM Engine

Refer to the relevant RUM and SiteMinder documentation as necessary.

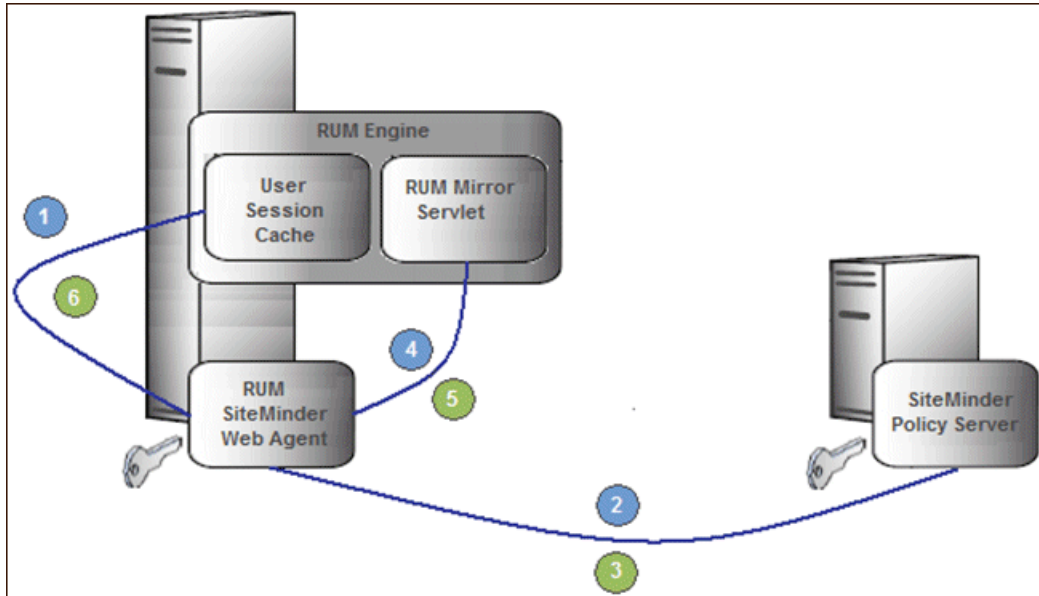
## Prerequisites

The following are prerequisite for the RUM–SiteMinder integration:

- The RUM Engine and SiteMinder Web Agent must be installed on the same machine.
- RUM version 9.12 or later.
- IIS.

## System Flow

The following diagram illustrates the flow between the RUM Engine, the RUM SiteMinder Web Agent, and the SiteMinder Policy Server.



Processing Steps:

1. The User Session Cache component sends a request with an SMSESSION cookie to the RUM Mirror Servlet for retrieving the USER name (through the RUM SiteMinder Web Agent).
2. The RUM SiteMinder Web Agent intercepts the request and requests the USER data from the SiteMinder Policy Server (relies on the SMSESSION cookie).
3. The SiteMinder Policy Server validates the SMSESSION cookie and sends the Server Policy Response object with USER data.
4. The RUM SiteMinder Web Agent transfers the Server Policy Response object with USER data to a RUM Mirror Servlet.
5. The RUM Mirror Servlet extracts the USER data and sends a response with USER Name back to the User Session Cache component through the RUM SiteMinder Web Agent.
6. The RUM SiteMinder Web Agent redirects the response back to the User Session Cache component.

## Configuring the SiteMinder Policy Server

This section describes the following steps for configuring the SiteMinder Policy Server:

- ["Create an Agent" on the next page](#)
- ["Create the Agent Conf Object" on the next page](#)
- ["Create the Authentication Scheme" on the next page](#)
- ["Configure the Domain" on page 181](#)

## Create an Agent

To create an agent, use the SiteMinder Administration console to add the RUM Web Agent to the Policy Server.

1. Right-click **Agents** and select **Create Agent**. The SiteMinder Agent dialog box opens.
2. In the **Name** field, enter the hostname of the machine on which the RUM SiteMinder Web Agent is installed. If you are not using the standard, default port **80**, you must also specify the port number after the name (separated by a colon). By default, the RUM Engine's mirror servlet uses port number **8181**, so you enter the name as:

```
<agent_host_machine>:8181
```

**Note:** If you change the port value in this dialog box, you must also change the port value in other places. For details, see "[Changing the Configuration of the TCP Port](#)" on page 188.

3. For the Description, enter **RUM SM Web Agent**.
4. For the Agent Type, select **Web Agent**.
5. Click **OK**.

## Create the Agent Conf Object

Use the SiteMinder Administration console to create the Agent Conf Object to the Policy Server.

1. In the left pane of the SiteMinder Administration console, click **AgentConfObjects**.
2. In the right pane, right-click **IISDefaultSettings** and select **Duplicate Configuration Object** from the menu. The SiteMinder Agent Configuration Object dialog box opens.
3. For the Name, enter the hostname of the machine on which the **RUM SiteMinder Web Agent** is installed.
4. For the Description, enter **RUM SM Web Agent**.
5. Edit the **#DefaultAgentName** configuration value:
  - a. Select the **#DefaultAgentName** configuration value.
  - b. Click **Edit**. The Edit Parameter dialog box opens.
  - c. Select the **Plain** radio button.
  - d. For the Parameter Name, enter **DefaultAgentName**.
  - e. For the Value, enter the agent name exactly as it appears in the SiteMinder Agent Properties dialog box.
  - f. Click **OK**.
6. Click **OK**.

## Create the Authentication Scheme

In the SiteMinder Administration console, add the Authentication Scheme to the Policy Server.

1. Right-click **Authentication Schemes** and select **Create Authentication Scheme**. The SiteMinder Authentication Scheme dialog box opens.
2. For the Name, enter **RUM Scheme**.

3. For the Description, enter **RUM SM Web Agent**.
4. For the Authentication Scheme Type, select **HTML Form Template**.
5. In the Scheme tab, for the Web Server Name enter the hostname of the machine on which the Web Agent performs authentication.
6. Click **OK**.

## Configure the Domain

To configure the domain, perform the following steps:

- ["Create the Realm" below](#)
- ["Create the Response" below](#)
- ["Create the Rules" on the next page](#)
- ["Configure the Policy" on the next page](#)

### Create the Realm

In the SiteMinder Administration console, open the domain of the monitored application as provided by your SiteMinder contact.

1. In the left pane of the SiteMinder Administration console, right-click **Domain**.
2. In the right pane, right-click the relevant domain and select **Properties of Domain** from the menu. The SiteMinder Domain dialog box opens.
3. Select the **Realms** tab.
4. Click **Create**. The SiteMinder Realm dialog box opens.
5. For the Name, enter **RUM Mirror Servlet**.
6. For the Resource Filter, enter **/iam/mirror**.
7. Click **Lookup** to search for and select the agent's hostname.
8. For the Authentication Schema, select the **RUM Authentication Schema** created previously.
9. For the Default Resource Protection, select **Protected**.
10. Click **OK** (in the SiteMinder Realm dialog box).
11. Click **OK** (in the SiteMinder Domain dialog box).

### Create the Response

In the SiteMinder Administration console, open the domain of the monitored application as provided by your SiteMinder contact.

1. In the left pane of the SiteMinder Administration console, right-click **Domain**.
2. In the right pane, right-click the relevant domain and select **Create Response** from the menu. The SiteMinder Response dialog box opens.
3. For the Name, enter **RUM Response**.
4. For the Agent, select **Web Agent**.
5. Click **Create**. The SiteMinder Response Attribute Editor opens.
  - a. For the Attribute, select **WebAgent-HTTP-Header-Variable**.
  - b. For the Attribute Kind, select **User Attribute**.

- c. For the Variable Name, enter **RUM\_SM\_USER**.

**Note:** If you change the Variable Name value, you must also change the value of the **requestHeaderUserNameParamName** tag in the **RUM\conf\configurationmanager\configuration\IAM\_config.xml** file.

- d. Set the Attribute Name as the name of the LDAP attribute that holds the user name value.

**Note:** The Attribute name depends on your specific LDAP implementation. (For example, the **uid** attribute for Sun One LDAP.)

- e. Click **OK** (in the SiteMinder Response Attribute Editor).
6. Click **OK** (in the SiteMinder Response dialog box).

## Create the Rules

1. Create the RUM SMA Authentication rule for the RUM Mirror Servlet realm.
  - a. In the left pane of the SiteMinder Administration console, right-click the **RUM Mirror Servlet** realm and select **Create Rule under Realm** from the menu. The SiteMinder Rule dialog box opens.
  - b. For the Name, enter **RUM SMA Authentication Rule**.
  - c. For the Action, select **Authentication events**.
  - d. In the Action drop-down list, select **onAuthAccept**.
  - e. Click **OK**.
2. Create the RUM SMA Web Action rule for the RUM Mirror Servlet realm.
  - a. In the left pane of the SiteMinder Administration console, right-click the **RUM Mirror Servlet** realm and select **Create Rule under Realm** from the menu. The SiteMinder Rule dialog box opens.
  - b. For the Name, enter **RUM SMA Web Action Rule**.
  - c. For the resource, enter an asterisk (\*).
  - d. For the Action, select **Web Agent actions**.
  - e. In the Action list, select **Get**, **Post**, and **Put**.
  - f. Click **OK**.

## Configure the Policy

In the SiteMinder Administration console, edit the policy of the domain.

**Note:** If there is more than one policy, you must add the rule and response to each of them.

1. In the left pane of the SiteMinder Administration console, click **Policies**.
2. In the right pane, right-click the relevant policy and select **Properties of Policy** from the menu. The SiteMinder Policy dialog box opens.
3. Select the **Rules** tab.
4. Click **Add/Remove Rules**. The Rule Items dialog box opens.
5. Move the **RUM SMA Web Rule** and the **RUM MA Authentication Rule** from Available Members to Current Members.
6. Click **OK**.
7. In the Rules tab of the SiteMinder Policy dialog box, select the **RUM SMA Authentication Rule**.

8. Click **Set Response**. The Set Response dialog box opens.
9. Select **RUM Response**.
10. Click **OK** (in the Set Response dialog box).
11. Click **OK** (in the SiteMinder Policy dialog box).

## Installing and Configuring the SiteMinder Web Agent

This section describes how to install and configure the SiteMinder Web Agent and includes the following topics:

- ["Prerequisites" below](#)
- ["Installing the SiteMinder Web Agent" below](#)
- ["Configuring the SiteMinder Web Agent" below](#)

### Prerequisites

Ensure the following prerequisites before installing the SiteMinder Web Agent:

- The Web Server is installed.
- You have an account with Administrative privileges for your Web Server.
- The Policy Server is configured.
- You have an appropriate version of the Web Agent setup file.
- The setup file is compatible with the host's operating system.

### Installing the SiteMinder Web Agent

To install the SiteMinder Web Agent:

1. If necessary, extract all the files from the ZIP file provided by SiteMinder.
2. Start the Web Agent executable.  
For example: `nete-wa-6qmr6-win64.exe`
3. The CA SiteMinder Web Agent Introduction screen appears. Click **Next**.
4. On the License Agreement screen, scroll down and select **I accept the terms of the License Agreement**, and then click **Next**.
5. On the Important Information screen, click **Next**.
6. On the Choose Install Location screen, accept the default location for installing the Web Agent, or click **Choose** to select a different location. Click **Next**.
7. On the Choose Shortcut Folder screen, click **Next**.
8. On the Pre-Installation Summary screen, click **Install**.
9. On the Install Complete screen, select **Yes, I would like to configure the Agent now** and click **Next**.

### Configuring the SiteMinder Web Agent

To configure the SiteMinder Web Agent:

1. On the Host Registration screen, select **Yes, I would like to do Host Registration now**, but do not select the Enable PKCS11 DLL Cryptographic Hardware check box. Click **Next**.
2. On the Admin Registration screen, type the SiteMinder administrator name and password provided by

- your SiteMinder contact. Do **not** select the Enable Shared Secret Rollover check box. Click **Next**.
3. On the Trusted Host Name and Configuration Object screen, type the trusted hostname and Host Conf Object provided by your SiteMinder contact. Click **Next**.
  4. On the Policy Server IP Address screen, type the SiteMinder Policy Server IP address provided by your SiteMinder contact and click **Add**. Click **Next**.
  5. On the Host Configuration file location screen, accept the default file name and location and click **Next**.
  6. On the Select Web Server(s) screen, select the Web server that you want to configure as a Web Agent and click **Next**.
  7. On the Agent Configuration Object screen, enter the Agent Conf Object provided by the SiteMinder contact and click **Next**. (For details, see "[Create the Agent Conf Object](#)" on page 180)
  8. On the Self Registration screen, select **No, I don't want to configure Self Registration**. Click **Next**.
  9. On the Web Server Configuration Summary screen, click **Install**. The Web Agent configuration process starts and when completed, the Configuration Complete screen is displayed.
  10. Click **Done** to complete the configuration process.

## Configuring the Web Server

This section describes how configure the Web Server and includes the following topics:

- "[Configuring IIS to Work with RUM](#)" below
- "[Configuring IIS to Work with the SiteMinder Web Agent](#)" on page 187

## Configuring IIS to Work with RUM

To configure IIS to work with RUM:

1. Download the ISAPI redirector server plug-in **isapi\_redirect.dll**, which is available at:
  - Win32 i386  
<http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/windows/tomcat-connectors-1.2.37-windows-i386-iis.zip>
  - Win64 x86  
[http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/windows/tomcat-connectors-1.2.37-windows-x86\\_64-iis.zip](http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/windows/tomcat-connectors-1.2.37-windows-x86_64-iis.zip)
  - AMD64  
[http://archive.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/jk-1.2.31/amd64/isapi\\_redirect-1.2.31.dll](http://archive.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/jk-1.2.31/amd64/isapi_redirect-1.2.31.dll)
2. Unzip the zip file and copy the **isapi\_redirect.dll** file to the **/bin/IIS** directory in your RUM Engine installation.

For example: C:\RUM\bin\IIS\isapi\_redirect.dll

**Caution:** If you are installing on a WinNT or Win2k system, make sure IIS runs with a user that can access this directory.

3. Open the **/bin/IIS/isapi\_redirect.properties** file that contains the configuration settings for the redirector



plug-in file.

4. Change **%LOG\_DIR%** to the full path of any directory that is not under the RUM home directory.

**Caution:** Placing the log file in the RUM home directory may cause an automatic uninstallation of the RUM Engine and interference with the re-installation process.

5. Change **%RUM%** to the full path of the installation directory of your RUM Engine.

For example: C:\RUM\bin\IIS\isapi\_redirect.properties

```
# Configuration file for the Jakarta ISAPI Redirector
# The path to the ISAPI Redirector Extension, relative to the website
# This must be in a virtual directory with execute privileges
extension_uri=jakarta/isapi_redirect.dll

# Full path to the log file for the ISAPI Redirector
log_file=C:\Users\johndoe\AppData\Local\Temp\isapi.log

# Log level (debug, info, warn, error or trace)
log_level=error

# Full path to the workers.properties file
worker_file=C:\RUM\conf\workers.properties.minimal

# Full path to the uriworkermapping.properties file
worker_mount_file=C:\RUM\conf\uriworkermapping.properties
```

6. Save your changes.
7. Open Internet Information Services (IIS) Manager. You must be logged on as a member of the Administrators group on the local computer to perform the following procedures, or you must have been delegated the appropriate authority.

To open IIS Manager at a command prompt:

- a. On the Start menu, click **Run**.
- b. In the Open dialog box, type **inetmgr** and then click **OK**.

For more information, see <http://msdn.microsoft.com/en-us/library/bb763170.aspx>.

8. Using the IIS management console, set TCP port **8181** to **Default Web Site**. This port is used for accessing the mirror servlet from the RUM Engine.

**Note:** If you change the port value in this dialog box, you must also change the port value in other places. For details, see "[Changing the Configuration of the TCP Port](#)" on page 188.

- a. Right-click the Default Web Site and select **Properties** from the menu. The Default Web Site Properties dialog box opens.
  - b. On the Web Site tab, click **Advanced** to open the Advanced Web Site Identification dialog box.
  - c. Select the current line with port 80 and click **Edit** to open the Add/Edit Web Site Identification dialog box.
  - d. Select the (All Unassigned) IP address option and set the TCP port to **8181**. Click **OK**. The new configuration appears in the **Multiple identities for this Web site** list in the Advanced Web Site Identification dialog box.
9. Using the IIS management console, add a new virtual directory to Default Web Site. The name of the virtual directory **must** be **jakarta**. Its physical path should be the directory in which you placed **isapi\_redirect.dll** (for example, C:\RUM\bin\IIS). While creating this new virtual directory, assign execute permission to it.

Right-click the Default Web Site and select **New>Virtual Directory** from the menu. The Virtual Directory Creation Wizard opens. In the wizard:

- Enter **jakarta** as an alias of the virtual directory.
- Add a path to the directory that contains **isapi\_redirect.dll** (for example, C:\RUM\bin\IIS).
- Assign execute permission.

**Caution:** The name of the virtual directory must be **jakarta**.

10. Using the IIS management console, grant access to the jakarta resource from the local machine only.
  - a. In the left pane, right-click **jakarta** and select **Properties** from the menu.
  - b. Select the **Directory Security** tab.
  - c. In the **IP address and domain restrictions** panel, click **Edit**. The IP Address and Domain Name Restrictions dialog box opens.
    - Select **Denied Access**.
    - Click **Add**.
    - Select **Single computer**.
    - Enter the **IP address** of the machine on which the RUM SiteMinder Web Agent is installed.
    - Click **OK**.
  - d. Click **OK**.
11. Using the IIS management console, add **isapi\_redirect.dll** as a filter in Default Web Site (DWS). The name of the filter should reflect its task (uses the name tomcat) and its executable must be C:\RUM\bin\IIS\isapi\_redirect.dll.
  - a. In the left pane, right-click **Default Web Site** and select **Properties**. The Default Web Site Properties dialog box opens.
  - b. Select the **ISAPI Filters** tab and click **Add**. The Add/Edit Filter Properties dialog box opens.
  - c. Enter **tomcat** as the filter name
  - d. Add the full path to the **isapi\_redirect.dll** as the executable field (for example, C:\RUM\bin\IIS\isapi\_redirect.dll).
  - e. Click **OK**.

**Note:** At this stage, the status of the added filter is inactive.

12. Using the IIS management console, add the jakarta ISAPI Redirector to the Web Service Extensions.
  - a. In the left pane, right-click **Web Service Extensions** and select **Add a new Web Service extension**. The New Web Service Extension dialog box opens.
  - b. Enter **tomcat** as the Extension Name
  - c. Add the full path to the **isapi\_redirect.dll** to the required files. (for example, C:\RUM\bin\IIS\isapi\_redirect.dll)
  - d. Select the **Set extension status to Allowed** check box.
  - e. Click **OK**.
13. Restart the IIS Web Server.
  - a. On the Start menu, click **Run**.
  - b. In the Open dialog box, type **IISReset** and then click **OK**.

## Configuring IIS to Work with the SiteMinder Web Agent

To configure IIS to work with the SiteMinder Web Agent:

1. Open the IIS management console.
2. In the left pane, ensure that the **siteminderagent** virtual directory has been added under the Default Web Site.
3. Check the status of the ISAPI filter for SiteMinder:
  - a. In the left pane, right-click **Web Sites** and select **Properties**. The Web Sites Properties dialog box opens.
  - b. Select the **ISAPI Filters** tab.
  - c. The status of SiteMinder Web Agent must be green.
4. In the IIS management console, add the **ISAPI6 SiteMinder WEbAgent service** to the Web Service Extensions:
  - a. In the left pane, right-click **Web Service Extensions** and select **Add a new Web Service extension** from the menu. The New Web Service Extension dialog box opens.
  - b. Enter **ISAPI6 WEbAgent** as the Extension Name.
  - c. Add the full path to the **netegrity\webagent\bin\ISAPI6WebAgent.dll** to the required files (for example, C:\Program Files\netegrity\webagent\bin\ISAPI6WebAgent.dll).
  - d. Select the **Set extension status to Allowed** check box.
  - e. Click **OK**.
5. In the IIS management console, add the **SM PW** service to the Web Service Extensions:
  - a. In the left pane, right-click **Web Service Extensions** and select **Add a new Web Service extension** from the menu. The New Web Service Extension dialog box opens.
  - b. Enter **SM PW Services** as the Extension Name.
  - c. Add the full path to the **netegrity\webagent\pw\smpwservicescgi.exe** to the required files (for example, C:\Program Files\netegrity\webagent\pw\smpwservicescgi.exe).
  - d. Select the **Set extension status to Allowed** check box.
  - e. Click **OK**.
6. In the IIS management console, add the **SM PW Default** service to the Web Service Extensions:
  - a. In the left pane, right-click **Web Service Extensions** and select **Add a new Web Service extension** from the menu. The New Web Service Extension dialog box opens.
  - b. Enter **SM PW Default Services** as the Extension Name.
  - c. Add the full path to the **netegrity\webagent\pw\_default\smpwservicescgi.exe** to the required files (for example, C:\Program Files\netegrity\webagent\pw\_default\smpwservicescgi.exe).
  - d. Select the **Set extension status to Allowed** check box.
  - e. Click **OK**.
7. In the IIS management console, allow all unknown CGI and ISAPI Extensions:
  - a. In the left pane, select **Web Service Extensions**.
  - b. In the right pane:
    - o Select **All Unknown CGI Extensions**.
    - o Click **Allow**.

- Select **All Unknown ISAPI Extensions**.
  - Click **Allow**.
8. Enable the SiteMinder Web Agent:
    - a. Edit the **netegrity/webagent/bin/IIS/WebAgent.conf** file (for example, C:\Program Files\netegrity\webagent\bin\IIS\WebAgent.conf).
    - b. Change NO to YES in the **EnableWebAgent** field.
  9. Restart IIS.
  10. Check that SiteMinder is running by selecting **Start > Administrative Tools > Event Viewer**.

## Configuring the RUM Engine

This section describes how to configure the RUM Engine:

1. Open the `\EJBContainer\server\mercury\deploy\jbossweb-tomcat50.sar\server.xml` file in a text editor.  
For example: C:\RUM\EJBContainer\server\mercury\deploy\jbossweb-tomcat50.sar\server.xml
2. Enable the AJP entry by uncommenting it (by default it is commented out).

```
<!-- A J/P 1.3 Connector on port 8009 -->  
<Connector port="8009" address="$jboss.bind.address"  
    emptySessionPath="true" enableLookups="false" redirectPort="8443"  
    protocol="AJP/1.3" URIEncoding="UTF-8"/>
```

3. Save your changes.
4. Open the `\conf\configurationmanager\Beatbox_Default_Const_Configuration.xml` file in a text editor.  
For example: C:\RUM\conf\configurationmanager\Beatbox\_Default\_Const\_Configuration.xml
5. Change the value of **max\_log\_field\_length** from 2048 (the default value) to 10240.  
For example: max\_log\_field\_length 10240
6. Save your changes.
7. Restart the RUM Engine.

## Changing the Configuration of the TCP Port

The deployment of SiteMinder resources (Policy Web agent and RUM Engine mirror servlet) is configured by default to use TCP port **8181**. If you want to change the configured port value, you must also set the port value in the following:

- **Policy server:**
  - Change the **Web agent** name in the SiteMinder Agent dialog box to include the port value. For details, see ["Create an Agent" on page 180](#).
  - Change the **DefaultAgentName** parameter value in the SiteMinder Agent Configuration Object dialog box to the agent's name. For details, see ["Create the Agent Conf Object" on page 180](#).
- **IIS:** Change the **TCP Port** parameter in the Default Web Site Properties dialog box in the IIS Manager. For

details, see ["Configuring IIS to Work with RUM" on page 184](#).

- **RUM Engine:** Change the **http\_settings > port** XML tag in the **RUM\conf\configurationmanager\configuration\IAM\_config.xml** file.

## Testing and Troubleshooting

This section describes various testing and troubleshooting procedures for the following:

- ["RUM Engine" below](#)
- ["SiteMinder Web Agent" on the next page](#)
- ["Mirror Servlet" on the next page](#)

## RUM Engine

**Note:** Before carrying out the following procedures, the SiteMinder Agent must be disabled.

1. Invoke the URL **http://localhost:8180/rumwebconsole**. If the Login page of the RUM Engine is not displayed, check that the RUM Engine is running.
2. Invoke the URL **http://localhost:8181/iam/mirror**. If an Error page is displayed, check if the status of the ISAPI Filter on the Default Web Site is green.
  - a. Right-click **Default Web Site** and select **Properties**. The Default Web Site Properties dialog box opens.
  - b. Select the **ISAPI Filters** tab.
  - c. If the status is red, check the Application Event Log for the W3SVC-WP. To open the Event Viewer, select **Start > Administrative Tools > Event Viewer**.
    - Make sure you use an **isapi\_redirect.dll** that is compatible with for the host's operating system.
    - Make sure IIS runs with a user that can access the C:\RUM\bin\IIS directory.
  - d. If the status is green, examine the last line in the IIS server log file, located in SYSTEM32\LogFiles\W3SVC1. Take the appropriate action according to the error code in the last line:

Error Code	Action
404	Make sure you entered the URL correctly.
505	<ul style="list-style-type: none"><li>○ Make sure the virtual directory created is called <b>jakarta</b>.</li><li>○ Make sure that the <b>extension_uri</b> setting is correct.</li><li>○ Check the <b>workers.properties</b> file and make sure the port setting for <b>worker.ajp13w.port</b> is the same as the port specified in the <b>server.xml</b> for the Apache AJP13 support.</li></ul>
202 or 403	Make sure you have checked <b>Execute Access</b> for the jakarta virtual directory in the Advanced Options of the Personal Web Manager.

## SiteMinder Web Agent

Invoke the URL **http://localhost:8181/iam/mirror**. The SiteMinder Login Page should be displayed. If an Error page is displayed:

1. **Enable logging.** In the SiteMinder Administration console, right-click your Agent Conf Object and select **Properties of Configuration Object**. The SiteMinder Agent Configuration Object dialog box opens.
  - a. Select **LogFileName**.
  - b. Click **Edit**.
  - c. Enter the full log file path as the value (for example, C:\Users\johndoe\AppData\Local\Temp\siteminder.log).

**Caution:** Placing the log file in the RUM home directory may cause an automatic uninstallation of the RUM Engine and interference with the re-installation process.

- d. Click **OK**.
- e. Select **Logfile**.
- f. Click **Edit**.
- g. Enter **yes** as the value.
- h. Click **OK**.

**Note:** No restart is required.

2. **Check Error in the Event Viewer.** Make sure that the **HostConfigFile** parameter in the **WebAgent.conf** file has the path to the host configuration file.

**For example:**

```
C:\Program Files\netegrity\webagent\bin\IIS\WebAgent.conf
```

```
HostConfigFile="C:\Program Files\netegrity\  
webagent\config\SmHost.conf.bk1"
```

## Mirror Servlet

To check that the mirror servlet is alive and operating correctly with the SiteMinder Web agent, invoke the following URL: **http://localhost:8181/iam/mirror?IDENTITY\_PARAM\_USER\_NAME=RUM\_SM\_USER**

The **IDENTITY\_PARAM\_USER\_NAME** parameter indicates the header name that is returned at the Web agent's response and that contains the logged-in user name. The header name **RUM\_SM\_USER** is the same value that was defined in the policy server. For details, see ["Create the Response" on page 181](#).

The result on the page will be the user name that was entered in the login page, followed by the prefix **IAM\_UID=**. For example, **IAM\_UID=JohnSmith**.

If this result is not accepted:

1. Verify that **RUM\_SM\_USER** is the configured value in the Policy server.
2. Test and troubleshooting the RUM Engine. For details, see ["RUM Engine" on the previous page](#).
3. Test and troubleshooting the SiteMinder Web Agent. For details, see ["SiteMinder Web Agent" above](#).

# Chapter 15: RUM Data Export

Data export enables you to extract requested raw data from RUM and provide it to users. You can then use this data to create your own reports, giving you different views than those provided in the standard End User Management reports in APM. Another benefit of exporting data is that you are not dependent on the RUM purging cycle and can save the exported data for as long as you need.

This chapter includes the following topics:

- ["Enable Data Export" below](#)
- ["How Data is Exported" below](#)
- ["Data Export XML File" on the next page](#)
- ["Valid Channel Types and Fields" on page 195](#)

## Enable Data Export

To enable data export, you create and configure an XML file in the **\<RUM root directory>\conf\data\publisher\consumers** directory. This file contains settings such as what data you want extracted, how it should be formatted, where it should be saved, when to close and save a data file and open a new one, and so forth. For details on the XML file, see ["Data Export XML File" on the next page](#).

You can create multiple XML files so that different data can be extracted for different consumers. For convenience, it is recommended that each file name is the same as the relevant consumer name.

A template XML file called **consumer-template.xml** is located in the **\<RUM root directory>\conf\data\publisher** directory. You can copy and edit this file and then save it in the **\<RUM root directory>\conf\data\publisher\consumers** directory.

While a background process checks if configuration files have been changed, you can force an immediate update by synchronizing the configuration in the RUM web console (select **Tools > Monitoring Configuration Data > Sync All Configuration**).

## How Data is Exported

When the RUM Engine is started, it checks to see if there are data export configuration XML files in the **\<RUM root directory>\conf\data\publisher\consumers** directory. For each XML file found, the RUM Engine creates a directory for the configured consumer in the configured output directory, and in the consumer's directory creates further sub-directories for each configured channel type. For example, the following directories are created for a consumer called **XYZ**, with a configured output directory of **C:\MyDataPublishing\DpOutput** and with configured channel types of **Page** and **Transaction**:

- C:\MyDataPublishing\DpOutput\XYZ\Page
- C:\MyDataPublishing\DpOutput\XYZ\Transaction

### Note:

- RUM must have read and write (RW) permissions for the configured output directory.
- The output directory can be a local or remote directory.

Files are opened in the relevant directories and data is saved to them according to the configuration in the XML file. Data is continuously saved to the files.

A file is closed when it reaches a certain size, or a specific timeout is encountered. You configure the maximum file size and/or timeout in the XML file. When a file is closed, a new file is automatically opened when new data is received. File names are made up of the consumer name, channel type, and the time in milliseconds that the file was created (for example, XYZ\_PAGE\_12345678).

You can also limit the output directories by size, or by the number of files in them. When the maximum size or the maximum number of files is reached, no more new files will be opened. You must manually manage the output directories and files to ensure that you have enough space.

To stop the export of data, remove the XML files from the **\<RUM root directory>\conf\data\publisher\consumers** directory. Removing the XML file for a specific consumer stops the export of data for that consumer only.

## Data Export XML File

This section describes the elements and attributes used in the data export configuration XML file.

A template XML file called **consumer-template.xml** is located in the **\<RUM root directory>\conf\data\publisher** directory.

### Elements Table

Element	Description	Attribute For details, see "Attributes Table" below
<b>consumer</b>	Initial element in block containing all the data export configuration.	<ul style="list-style-type: none"> <li>name</li> <li>disable</li> </ul>
<b>consumerDescription</b>	Optional consumer description.	
<b>collector</b>	Initial element for configuration of a specific collector. <b>Note:</b> You can configure only one collector for data export.	
<b>formats</b>	Initial element for configuring the format for common data types for all exported data.	
<b>DOUBLE</b>	Format for double precision numbers. <b>Default value:</b> <DOUBLE>{#.000}</DOUBLE>	
<b>DATE</b>	Format for dates. <b>Default value:</b> <DATE>{MM-dd-yyyy hh:mm:ss:SS}</DATE>	



Element	Description	Attribute For details, see "Attributes Table" below
<b>appTierIds</b>	Application Filter. <b>Note:</b> You can specify comma separated application tier IDs. If you do not specify any IDs, data is displayed for all the applications.	
<b>channels</b>	Initial element for configuring what data to export.	
<b>channel</b>	Initial element for configuring a specific type of data for export. <b>Note:</b> <ul style="list-style-type: none"> <li>• For each channel type, you configure separate fields and field elements.</li> <li>• If you declare a channel type, but do not declare any fields for that type, all fields are exported by default.</li> </ul>	type
<b>fields</b>	The initial element for configuring the specific fields to export for each channel type. <b>Note:</b> For details on the available fields for each channel type, see " <a href="#">Valid Channel Types and Fields</a> " on page 195.	
<b>field</b>	Specific data field to export for the configured channel type.	<ul style="list-style-type: none"> <li>• name</li> <li>• title</li> </ul>
<b>publisher</b>	Configuration for the actual export of the data.	
<b>type</b>	The type of output in which to export the data. <b>Note:</b> The only valid option is <b>FILE</b> .	
<b>outputDirectory</b>	The directory path in which to save the output files. <b>Caution:</b> Do not locate the output directory on the same disk used by the MySQL database.	
<b>maxDirectorySizeMb</b>	The maximum size of the output directory. After this limit is reached, no more output files are saved.	
<b>maxFilesInDirectory</b>	The maximum number of saved output files that can exist in the output directory. After this limit is reached, no more output files are saved until old files are removed.	
<b>maxFileSizeMb</b>	The maximum size for the open data export file. After this limit is reached, the file is closed and saved and a new file is opened when new data is received.	

Element	Description	Attribute For details, see "Attributes Table" below
<b>timeoutInSec</b>	The maximum timeout that triggers the closing of the data export file. After this limit is reached, the file is closed and saved and a new file is opened when new data is received.	
<b>publisherFileType</b>	The exported data file type. <b>Note:</b> The only valid option is CSV.	
<b>readyFileExtension</b>	The extension to add to the output file when it is closed and saved.	
<b>useHeaders</b>	If set to <b>true</b> , a line of field headers (or alternate names if configured) is added to the saved output file.	
<b>fieldDelimiter</b>	The delimiter to use for separating fields in the output file.	
<b>newLineDelimiter</b>	The delimiter between records (lines) in a file. Valid options are: <ul style="list-style-type: none"> <li>• WINDOW</li> <li>• UNIX</li> <li>• MAC</li> </ul>	
<b>useZip</b>	If set to <b>true</b> , the output file is zipped.	
<b>comment</b>	The sign to use to denote a comment in the output file. <b>Note:</b> This is limited to a single character.	

### Attributes Table

Attribute	Parent Element	Description	Example
<b>name</b>	consumer	The consumer name for whom data is exported. <b>Note:</b> <ul style="list-style-type: none"> <li>• The consumer name is also used in the exported data file name.</li> <li>• The consumer name must be unique within all the configured XML files.</li> </ul>	<consumer name="consumer_XYZ">
<b>disable</b>	consumer	When set to <b>true</b> , data publishing for the consumer is disabled. <b>Default value:</b> false	<consumer name="consumer_XYZ" disable="false">

Attribute	Parent Element	Description	Example
<b>type</b>	channel	The type of data to export. Valid options are: <ul style="list-style-type: none"> <li>• <b>Page</b></li> <li>• <b>Session</b></li> <li>• <b>Transaction</b></li> <li>• <b>Action</b></li> <li>• <b>Event</b></li> </ul>	<channel type="Page">
<b>name</b>	field	The name of the field to be exported. <b>Note:</b> For details on the available fields for each channel type, see " <a href="#">Valid Channel Types and Fields</a> " below.	<field name="x-end-user-id" title="x-end-user-id" />
<b>title</b>	field	An alternate title for the field name. <b>Note:</b> For details on the available fields for each channel type, see " <a href="#">Valid Channel Types and Fields</a> " below.	<field name="x-end-user-id" title="x-end-user-id" />

## Valid Channel Types and Fields

The tables in the following topics list the valid fields for each channel for which you can export data:

- "[Page](#)" below
- "[Transaction](#)" on page 199
- "[Session](#)" on page 201
- "[Action](#)" on page 204

### Page

Field Name	Type	Units	Description
all-login-names	string		Login name of end user
c-browser-name	string		Describes the web browser used by the visitor
c-host-id	object		The APM host ID associated with client
c-host-name	string		The host name associated with client
c-os-name	string		Describes the operating system used by the visitor
cs-app-bytes	int	byte	The number of bytes received by the software element
cs-version	string		HTTP version used for the action
referrer	string		Entire raw referrer string sent in the action

Field Name	Type	Units	Description
s-host-id	object		The APM server ID
s-host-name	string		The server name
s-sw-element-id	object		The APM software element ID
s-sw-element-name	string		The software element name
sc-app-bytes	int	byte	The number of bytes sent by the software element
sc-server-firstbut-time-ms	long	ms	Time taken for the server to process the request
sc-status	int		Status or code sent by the server in response to the action
server-time-threshold-ms	long	ms	Server time threshold for the action
timestamp	date	date	Action start time
x-action-descriptor	string		Descriptor for given action
x-action-download-threshold-time-ms	long	ms	Download time threshold for the action
x-action-download-time-ms	long	ms	Total download of the action, from the beginning of the first request until the end of the last request
x-action-external-time-ms	long	ms	Sum totaling the gaps of time within loading of a page during which there are no components being transferred
x-action-id	long		The internal ID of the action
x-action-name	string		The configured name of the action
x-action-requests	int		Total number of component requests for this action
x-application-id	object		The APM application ID number
x-application-name	string		The APM application name
x-application-tier-id	object		The APM application tier ID number
x-available	boolean		Indicates if the action was available
x-cancelled	boolean		Page request that was prematurely interrupted
x-classify	boolean		Indicates that the page was classified
x-connect-time-ms	long	ms	Time taken for the client and server to initialize a TCP connection
x-end-user-id	object		The APM end-user group ID
x-end-user-packet-latency-time-threshold-ms	long	ms	End user packet latency threshold

Field Name	Type	Units	Description
x-end-user-subnet-id	object		The APM end-user subnet ID
x-end-user-username	string		The APM end-user group name
x-errors-events-num	int		Total number of application error events on page
x-event-id1	int		The event ID that has occurred within a particular visitor session on the action
x-event-id2	int		The event ID that has occurred within a particular visitor session on the action
x-event-id3	int		The event ID that has occurred within a particular visitor session on the action
x-geo-ip-num	string		IP Address
x-geo-net-end-num	string		Last IP Address of the client's network block
x-geo-net-start-num	string		First IP Address of the client's network block
x-host-parameterization	string		The host name
x-info-event-num	int		Total number of information (non error) events on page
x-is-backend-tier	boolean		Indicates if the action belongs to back-end tier
x-is-encrypted	boolean		Indicates if the action was encrypted
x-is-over-server-time-threshold	boolean		Indicates if the action was over server time threshold
x-location-id	object		The APM end-user location ID
x-location-name	string		The APM end-user location name
x-location-packet-latency-time-threshold-ms	long	ms	Location packet latency threshold
x-location-parent-id1	object		The APM location ID
x-location-parent-id2	object		The APM location ID
x-location-parent-id3	object		The APM location ID
x-location-parent-id4	object		The APM location ID
x-location-parent-id5	object		The APM location ID
x-location-parent-name1	string		The APM location name
x-location-parent-name2	string		The APM location name
x-location-parent-name3	string		The APM location name

Field Name	Type	Units	Description
x-location-parent-name4	string		The APM location name
x-location-parent-name5	string		The APM location name
x-network-time-ms		ms	Network time
x-packet-latency-time-threshold-ms	long	ms	Packet latency threshold
x-page-title	string		Title of the web page, which is normally displayed along the top of a visitor's web browser window
x-parent-action-seq-id	int		This field is used to correlate frames of the frame sets or other dependent pages
x-performance-event-num	int		Total number of performance (non error) events on page
x-retransmission-time-ms	long	ms	Time spent on retransmitting packets
x-rum-probe-id	int		Internal ID of the RUM Probe
x-server-time-ms	long	ms	Time taken for the server to respond to the request
x-server-time-to-firstbuf-threshold-ms	long	ms	Time to first buffer threshold for the action
x-session-action-seq	int		Number of action views (such as page views) associated with the session
x-session-application-id	string		The internal ID of the session application
x-session-id	string		Universally unique identifier (UUID) automatically assigned to each unique visitor session
x-session-property-tag1	string		The application session property was tagged by RUM
x-session-property-tag2	string		The application session property was tagged by RUM
x-session-property-tag3	string		The application session property was tagged by RUM
x-session-property-tag4	string		The application session property was tagged by RUM
x-session-property-tag5	string		The application session property was tagged by RUM
x-session-start-time	date	date	The session start time
x-ssl-time-ms	long	ms	Time taken for the client and server to initialize an SSL connection
x-total-packets	int		Total number of packets in the request and response
x-uri-parameterization	string		The URI
x-url-extracted-data	string		The URL extracted data

Field Name	Type	Units	Description
x-url-host	string		Name of the host requested by the client
x-url-http-method	string		HTTP request method used
x-url-port	int		HTTP request port
x-url-post-data	string		Query string data sent by a POST request
x-url-protocol	string		Identifier of the protocol
x-url-query-original	string		Query string data sent by a GET request
x-url-query-parameterization	string		URL query string data sent by a GET request
x-url-uri	string		URI string data sent by a GET request

## Transaction

Field Name	Type	Units	Description
all-login-names	string		Login name of end user
c-browser-name	string		Web browser used by the visitor
c-host-id	object		The APM host ID associated with client
c-host-name	string		The host name associated with client
c-os-name	string		Operating system used by the visitor
c-session-start	date	date	Session start time
c-transaction-client-time-ms	long	ms	Time of total processing time between components
c-transaction-gross-download-time-ms	long	ms	Gross download time
c-transaction-net-download-time-ms	long	ms	Net download time
s-host-id	object		The APM server ID
s-host-name	string		The APM server name
s-sw-element-id	object		The APM software element ID
s-sw-element-name	string		The software element name
s-transaction-server-firstbuf-time-ms	long	ms	Time taken for the server to process the transaction

Field Name	Type	Units	Description
s-transaction-server-time-ms	long	ms	Time taken for the server to respond to the transaction
timestamp	date	ms	Transaction start time
x-application-id	object		The APM application ID number
x-application-name	string		The APM application name
x-application-tier-id	object		The APM application tier ID number
x-end-user-id	object		The APM end-user group ID
x-end-user-subnet-id	object		The APM end-user subnet ID
x-end-user-user-name	string		The APM end-user group name
x-geo-ip-num	string		IP Address
x-geo-net-end-num	string		Last IP Address of the client's network block
x-geo-net-start-num	string		First IP Address of the client's network block
x-is-backend-tier	boolean		Indicates if the action belongs to back end tier
x-is-transaction-available	boolean		Indicates if the transaction was available
x-is-transaction-complete	boolean		Indicates if the transaction was completed
x-location-id	object		The APM end-user location ID
x-location-name	string		The APM end-user location name
x-location-parent-id1	object		The APM location ID
x-location-parent-id2	object		The APM location ID
x-location-parent-id3	object		The APM location ID
x-location-parent-id4	object		The APM location ID
x-location-parent-id5	object		The APM location ID
x-location-parent-name1	string		The APM location name
x-location-parent-name2	string		The APM location name
x-location-parent-name3	string		The APM location name
x-location-parent-name4	string		The APM location name
x-location-parent-name5	string		The APM location name
x-rum-probe-id	int		Internal ID of the RUM Probe
x-session-application-id	string		Internal ID of the session application



Field Name	Type	Units	Description
x-session-id	string		Universally unique identifier (UUID) automatically assigned to each unique visitor session
x-threshold-offset-percent			The location threshold offset in percent
x-transaction-bytes	long		Total number of bytes sent and received for the transaction
x-transaction-components	int		Number of components associated with the transaction
x-transaction-connect-time-ms	long	ms	Time taken for the client and server to initialize a TCP connection
x-transaction-errors-events-num	int		Total number of application error events associated with the transaction
x-transaction-id	object		The APM transaction ID
x-transaction-info-events-num	int		Total number of information (non error) events on transaction
x-transaction-name	string		The APM transaction name
x-transaction-network-time-ms	long	ms	Network time
x-transaction-performance-events-num	int		Total number of performance (non error) events on transaction
x-transaction-retransmission-time-ms	long	ms	Time spent on retransmitting packets
x-transaction-ssl-time-ms	long	ms	Time taken for the client and server to initialize an SSL connection

## Session

Field Name	Type	Units	Description
all-login-names	string		Login name of end user
c-browser-name	string		Web browser used by the visitor
c-host-id	object		The APM host ID associated with client
c-host-name	string		The host name associated with client
c-os-name	string		Operating system used by the visitor
cs-session-bytes	long	byte	Total number of bytes received for the session
s-host-id	object		The APM server ID
s-host-name	string		The server name

Field Name	Type	Units	Description
s-sw-element-id	object		The APM software element ID
s-sw-element-name	string		The software element name
sc-session-bytes	long	byte	Total number of bytes sent for the session
timestamp	date	date	Session start time
x-application-id	object		The APM application ID number
x-application-name	string		The APM application name
x-application-tier-id	int		The internal ID of the tier
x-avg-download-time-ms	long	ms	Average download time for all actions associated with the session
x-end-user-id	object		The APM end-user group ID
x-end-user-subnet-id	object		The APM end-user subnet ID
x-end-user-username	string		The APM end-user group name
x-expected-actions-count	int		Expected number of action hits associated with the session
x-geo-ip-num	string		IP Address
x-geo-net-end-num	string		Last IP Address of the client's network block
x-geo-net-start-num	string		First IP Address of the client's network block
x-is-backend-tier	boolean		Indicates the session associated with a back-end tier
x-is-session-available	boolean		Indicates if the session was available
x-is-session-ssl	boolean		Indicates that the session was over SSL connection
x-location-id	object		The APM end-user location ID
x-location-name	string		The APM end-user location name
x-location-parent-id1	object		The APM location ID
x-location-parent-id2	object		The APM location ID
x-location-parent-id3	object		The APM location ID
x-location-parent-id4	object		The APM location ID
x-location-parent-id5	object		The APM location ID
x-location-parent-name1	string		The APM location name
x-location-parent-name2	string		The APM location name
x-location-parent-name3	string		The APM location name

Field Name	Type	Units	Description
x-location-parent-name4	string		The APM location name
x-location-parent-name5	string		The APM location name
x-rum-probe-id	int		Internal ID of the RUM Probe
x-session-application-id	string		The internal ID of the session application
x-session-duration-ms	long	ms	Duration time of the session
x-session-dwell-time-ms	long	ms	Session's total dwell time, or the total number of milliseconds the visitor spent looking at pages during the current session
x-session-error-events-num	int		Total number of application error events associated with the session
x-session-failed-actions	long		Number of failed actions on the session
x-session-id	string		This is a universally unique identifier (UUID) automatically assigned to each unique visitor session
x-session-info-events-num	int		The total number of information (non error) events associated with the session
x-session-last-page	date	date	Time of last page associated with the session
x-session-latency-time-ms	long	ms	Total session latency
x-session-packets	long		Total number of packets sent and received for the session
x-session-pageviews-num	int		Number of page views associated with the session
x-session-performance-events-num	int		The total number of performance (non error) events associated with the session
x-session-property-tag1	string		The application session property was tagged by RUM
x-session-property-tag2	string		The application session property was tagged by RUM
x-session-property-tag3	string		The application session property was tagged by RUM
x-session-property-tag4	string		The application session property was tagged by RUM
x-session-property-tag5	string		The application session property was tagged by RUM
x-session-referrer	string		Entire raw referrer string sent in the session's first request
x-session-requests-num	int		Number of hits or HTTP requests associated with the session
x-total-download-time-for-available-actions-ms	long	ms	Total download time of available action associated with the session

Field Name	Type	Units	Description
x-total-download-time-for-unavailable-actions-ms	long	ms	Total download time of unavailable action associated with the session

## Action

Field Name	Type	Units	Description
x-action-id	int		Action ID
x-action-id-as-integer	int		Action ID as an integer
x-action-name	string		Action name
x-additional-properties	string		A string containing all additional properties of an action relevant for the specific protocol
x-action-requests	string		Total number of component requests for this action
x-action-seq-id	int		The sequential number of the action from the total actions for the entire session
x-availability-threshold	long		Availability threshold
x-available	boolean		Indicates if the action was available
x-bytes-in	int		Number of received bytes
x-bytes-out	int		Number of sent bytes
x-client-time-MS	long	ms	Action client time
x-conditional-follower-time-diff-threshold	int		Relevant for Seibel protocol only
x-connect-time-MS	long	ms	The time taken for the client and server to initialize a TCP connection, in microseconds.
x-download-threshold-offset-percent	int		Download threshold offset percent
x-download-time-threshold-MS	long	ms	Download time threshold
x-download-time-MS	long	ms	Time taken from page first packet to page last packet
x-dynamic-download-time-Th	long		If true - download time threshold is computed dynamically from historical data

Field Name	Type	Units	Description
x-dynamic-server-time-Th	long		If true - server time threshold is computed dynamically from historical data
x-end-time-micros	long	ms	Action end time
x-event-app-error-count	int		Number of event application errors
x-event-info-count	int		Number of info events
x-event-string	string		String contains event IDs
x-events	int		Number of events
x-extracted-parameters	string		A string containing all extracted parameters for an action</description
x-extracted-parametersMap	string		A string containing a map of all extracted parameters for an action
x-event-category-protocol-count	int		Number of category protocol events
x-event-performance-count	int		Number of performance events
x-generic-descriptor	string		Descriptor for a given action
x-generic-parameters	string		A string containing generic parameters for the specific protocol
x-hierarchy-tag	string		Relevant for Seibel protocol only
x-integration-diag	string		Data from Diagnostics integration
x-is-backend-tier	boolean		Indicates if the action belongs to a back-end tier
x-is-classify	boolean		Action has been classified
x-is-SSL	boolean		Indicates that the action was over an SSL connection
x-network-time-MS	long	ms	Action network time
x-orig-action-properties-as-string	string		A string containing all the original properties of an action for the specific protocol
x-parameters	string		String contains protocol parameters
x-parent-action-seq-id	int		This field is used to correlate frames of the frame sets or other dependent pages
x-retransmission-time-MS	long	ms	The time spent on retransmitting packets

Field Name	Type	Units	Description
x-server-availability-threshold	int		Server availability threshold
x-server-time-threshold-MS	long	ms	Server time threshold
x-server-time-MS	long	ms	Time taken for the server to respond to the request
x-server-time-to-first-buf-MS	long	ms	Server time to first buffer
x-server-time-to-first-buf-threshold-MS	long	ms	Server time to first buffer
x-session-property-tag1	string		The application session property was tagged by RUM
x-session-property-tag2	string		The application session property was tagged by RUM
x-session-property-tag3	string		The application session property was tagged by RUM
x-session-property-tag4	string		The application session property was tagged by RUM
x-session-property-tag5	string		The application session property was tagged by RUM
x-session-start-time	long		The session start time
x-specific-descriptor	string		The APM action name
x-specific-parameters	string		A string containing specific extracted parameters
x-ssl-time-MS	long	ms	The time taken for the client and server to initialize a TCP connection, in microseconds.
x-start-time-micros	long	ms	Action start time
x-status-code	int		Protocol status code
x-stopped	long		The number of page requests that were prematurely interrupted, including the page itself and all subsequent non-page or image transactions.
x-template-parameters	string		A string containing all action parameters relevant for the specific protocol
x-time-stamp	date		Action start time
x-total-latency-MS	long	ms	Total action latency

Field Name	Type	Units	Description
x-total-packets	int		Number of packets

## Event

Field Name	Type	Units	Description
c-client-host	string		Client host name
c-client-host-cmdb-id	object		Client host - APM ID
c-client-ip	string		Client IP
x-action-generic-descriptor	string		Generic descriptor of the action containing the event (for non session events)
x-action-id	int		ID of the action containing the event (for non session events)
x-action-name	string		Name of the action containing the event (for non session events)
x-application-cmdb-id	object		APM application ID
x-application-id	object		APM application configuration ID
x-application-name	string		APM application configuration name
x-application-tier-id	object		APM application tier ID
x-eu-cmdb-id	object		End user group - APM ID
x-eu-rule-id	int		End user group configuration ID
x-eu-subnet-id	object		End user group subnet - APM ID
x-eu-user-name	string		End user group name
x-event-category	string		Event Category - ERROR/INFO/PERFORMANCE
x-event-data	string		Event extra data. For example, extracted data for text pattern events (limited to 1024 chars)
x-event-id	int		Event ID
x-event-name	string		Event name
x-event-type	string		Event Type - HTTP/TEXT-PATTERN/GLOBAL/DL-TIME/PAGES/SOAP/SESSSION-PAGES/SESSION-FAILED-PAGES

Field Name	Type	Units	Description
x-location-id	object		APM location ID
x-location-name	string		APM end-user location name
x-location-parent-name1	string		APM location name
x-location-parent-name2	string		APM location name
x-location-parent-name3	string		APM location name
x-location-parent-name4	string		APM location name
x-location-parent-name5	string		APM location name
x-session-comp-seq	int		Session action sequence
x-session-guid	string		Session GUID
x-session-id	string		Value of the application session ID (for example, JSESSIONID)
x-session-start-time	date	date	Session start time
x-swe-cmdb-id	obj		APM software element ID
x-swe-display-name	string		Software element name
x-swe-host-cmdb-id	object		Software element host - APM ID
x-swe-host-name	string		Software element host name
x-swe-id	int		Software element ID
x-swe-ips	string		Software element IPs
x-timestamp	date	date	Event time



# Chapter 16: RUM Integrations

RUM integrations enable you to export data gathered by the RUM Sniffer Probe into the following tools for analysis:

- ["RUM Integration with Operations Analytics" below](#)
- ["RUM Integration with Performance Center" below](#)

## RUM Integration with Operations Analytics

Integrating RUM with Micro Focus Operations Analytics allows you to use the forensic root cause analysis tools in Operations Analytics on data exported from the RUM Sniffer Probe.

The RUM data export function is used to export the data from the RUM Sniffer Probe. For information about the RUM data export function, see ["RUM Data Export" on page 191](#).

To configure RUM to export data to Operations Analytics, you need to access the content pack from Operations Analytics and modify setting on the RUM Engine. For details, see the Operations Analytics documentation.

## RUM Integration with Performance Center

The data that is exported in the RUM integration with Micro Focus Performance Center (PC) is used to enrich PC with real data from production.

The data export file is located in:

```
<install dir>\conf\datapublisher\pc_integration.xml.
```

The data export file defines the default output folder (C:/RUM\_Export\pc\_integration) and the maximum default folder size (2 Gb) among other information.

For information about the RUM data export function, see ["RUM Data Export" on page 191](#).

### To enable integration with PC:

1. Copy the data export configuration file from  

```
<install dir>\conf\datapublisher\pc_integration.xml
```

to  

```
<install dir>\conf\datapublisher\consumers\pc_integration.xml
```
2. From the RUM web console, click **Tools > Monitoring configuration information**.
3. Click **Sync all configuration**.

# Part 4: Supporting Specific Protocols

# Chapter 17: Parsing Supported Protocols

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

**Note:** The supported protocols are for standard implementation. For specific custom protocol implementation support contact Support.

The following table lists the parsing supported protocols. Additional information for each protocol appears in the following sections.

	Applications
<b>HTTP</b>	"HTTP" on page 213
	"Flash/ActionScript AMF — HTTP Based" on page 215
<b>SOA</b>	"SOA" on page 217
	"WCF — HTTP Based" on page 217
<b>Databases</b>	"Microsoft SQL Server" on page 218
	"Oracle DB [+]" on page 218
	"MySQL" on page 219
	"DB2" on page 220
	"SSDB" on page 220
<b>Application Servers</b>	"Citrix XenApp (ICA) [+]" on page 223
	"XenApp Application configured as a VDI tier under the main General Web Application" on page 223
	"Oracle Forms NCA [+]" on page 227
	"WMQ" on page 228
	"SAPGUI" on page 229
<b>Mailing Applications</b>	"IMAP" on page 231
	"SMTP" on page 231
	"POP3" on page 231
<b>Generically Supported Protocols</b>	"DNS — Generic UDP" on page 233
	"Microsoft Terminals Services (RDP) — Generic Streaming TCP" on page 233

	Applications
	<a href="#">"RMI Registry — Generic TCP" on page 234</a>
	<a href="#">"SSH — Generic Streaming TCP" on page 235</a>
<b>Financial Protocols</b>	<a href="#">"NDC" on page 236</a>
	<a href="#">Diebold</a>
	<a href="#">"ISO 8583" on page 237</a>
	<a href="#">"TCS BaNCS" on page 237</a>
<b>Additional Applications</b>	<a href="#">"FTP" on page 239</a>
	<a href="#">"LDAP" on page 239</a>
	<a href="#">"SHVA" on page 240</a>
	<a href="#">"AMF" on page 240</a>
	<a href="#">"UDP" on page 241</a>

**Note:** For applications monitored with RUM versions prior to 9.0, only Slow Requests report is provided. However, full support is available for Oracle Forms NCA over HTTP starting from 8.02.

## TCP Level Information

RUM supports deep content analysis for the application types listed in this document. The Action Summary Report and Transaction Summary Report display the information for these application types. The basic TCP Level information (Connection Availability, network quality) is also available for these applications.

You can also use RUM to create general TCP level reports for all TCP-based applications which are not listed in this document .

# HTTP

- HTTP/S
  - **Versions:** 1.0, 1.1
  - **APM Template Name:** General Web Application
  - **Sample Snapshots:**

## Session Details

The screenshot displays the 'Session Details' window in the RUM Session Analyzer. It provides a comprehensive overview of a session, including properties, general events, and a detailed actions table.

**Properties:**

- Start time: 8/12/2015 11:04 AM
- Client IP: 2020.0a17.e081.c0b4.7750.5776.994
- Application: HTTPS
- Client host name: N/A
- End user: Others [...]
- User name: N/A
- Webpage: ...
- Server IP: 2020.0a17.e081.c0f1.12b7.36a7.8622
- Location: UNKNOWN
- Arrived from: N/A
- Total Traffic (KB): 127.1
- Client type: Chrome 43.0
- Duration (hh:mm:ss): 00:01:26
- HTTP Version: HTTP/1.1
- Operating system: Windows
- Latency (ms): 4.66
- Total action hits: 127

**General Events:** No data was found.

**Actions:** There are 127 actions in the session with 127 frame units, of which 127 units are for the selected application.

Action	Start Time	Application	Events	Total Time (sec)	Server Time (sec)	Network Time (sec)	Client Time (sec)	Think Time (sec)	Total Traffic (KB)	Snapshot	
https://my5-vml06122.hps.wlabs.../OpenSana00.worff	8/12/2015 11:04:16 AM	HTTPS	-	0.001	0.001	0.000	0.000	0.000	31.782	0.7	No
https://my5-vml06122.hps.wlabs.../443/ocsa/security-howto.html	8/12/2015 11:04:48 AM	HTTPS	-	0.239	0.000	0.000	0.239	0.000	0.000	2.1	No
https://my5-vml06122.hps.wlabs.../OpenSana00.worff	8/12/2015 11:04:48 AM	HTTPS	-	0.000	0.000	0.000	0.000	0.000	0.000	0.5	No
https://my5-vml06122.hps.wlabs.../OpenSana700.worff	8/12/2015 11:04:48 AM	HTTPS	-	0.000	0.000	0.000	0.000	0.000	2.278	0.5	No
https://my5-vml06122.hps.wlabs.../443/ocsa/manager-howto.html	8/12/2015 11:04:49 AM	HTTPS	-	0.187	0.000	0.000	0.187	0.000	0.000	0.9	No
https://my5-vml06122.hps.wlabs.../OpenSana700.worff	8/12/2015 11:04:49 AM	HTTPS	-	0.000	0.000	0.000	0.000	0.000	0.000	0.5	No
https://my5-vml06122.hps.wlabs.../OpenSana00.worff	8/12/2015 11:04:16 AM	HTTPS	-	0.001	0.001	0.000	0.000	0.000	0.002	0.7	No
https://my5-vml06122.hps.wlabs.../OpenSana700.worff	8/12/2015 11:04:19 AM	HTTPS	-	0.001	0.001	0.000	0.000	0.000	0.472	0.7	No
howto	8/12/2015 11:04:18 AM	HTTPS	-	33.708	0.000	0.000	33.708	0.000	0.000	4.3	No
https://my5-vml06122.hps.wlabs.../OpenSana400.worff	8/12/2015 11:04:18 AM	HTTPS	-	0.000	0.000	0.000	0.000	0.000	0.003	0.5	No
https://my5-vml06122.hps.wlabs.../OpenSana400.worff	8/12/2015 11:04:18 AM	HTTPS	-	0.000	0.000	0.000	0.000	0.000	1.751	0.5	No
man?r	8/12/2015 11:04:19 AM	HTTPS	-	0.139	0.000	0.000	0.139	0.000	1.872	0.9	No
https://my5-vml06122.hps.wlabs.../OpenSana400.worff	8/12/2015 11:04:21 AM	HTTPS	-	0.000	0.000	0.000	0.000	0.000	1.284	0.5	No
https://my5-vml06122.hps.wlabs.../OpenSana00.worff	8/12/2015 11:04:23 AM	HTTPS	-	0.000	0.000	0.000	0.000	0.000	0.004	0.5	No
https://my5-vml06122.hps.wlabs.../OpenSana700.worff	8/12/2015 11:04:23 AM	HTTPS	-	0.000	0.000	0.000	0.000	0.000	4.458	0.5	No
https://my5-vml06122.hps.wlabs.../OpenSana700.worff	8/12/2015 11:04:27 AM	HTTPS	-	0.000	0.000	0.000	0.000	0.000	1.993	0.5	No

## Action Summary

The screenshot displays the 'RUM Action Summary' window. It provides a high-level overview of actions, categorized by tier and type, with key performance indicators.

Action	Tier	Type	Total Action Hits	Availability (%)	Total Time (sec)	Server Time (sec)	Requests per Action Hit	Total Traffic (KB)
man?r	HTTP-Web	Page	367	100.00	0.95	0.02	3.31	1.6
howto	HTTP-Web	Page	301	100.00	1.46	0.00	5.09	2.7
			<b>668</b>	<b>100.00</b>	<b>1.02</b>	<b>0.01</b>	<b>4.11</b>	<b>2.1</b>

## Tier Summary

The screenshot displays the 'RUM Tier Summary' window. It provides a high-level overview of tiers, categorized by application and network, with key performance indicators.

Tier	Tier Availability (%)	Total Action Hits	Slow Action Hits	Total Time (sec)	Total Requests	Connection Availability (%)	Total Connection Attempts	Total Traffic (MB)
SDM	99.99	6,577	0	0.50	6,527	100.00	1,947	115.5
auto-discovered-See-MySQL	99.99	547,528	0	0.00	547,526	100.00	49	995.9
auto-discovered-See-Microsoft SQL datab	99.99	467,573	0	0.01	467,573	100.00	837	180.5
auto-discovered-See-General_WWB	100.00	467	0	0.09	467	99.78	463	74.4

### App Infrastructure

Analysis Reports > RUM Application Infrastructure Summary

Status Reports Analysis Reports Alerts Production Analysis Business Process Recognition Mobile Reports

RUM Application Infrastructure Summary 06/06/2015 10:00:00 AM-05/13/2015 10:00:00 AM (GMT+02:00) Jerusalem

Highlights Application Network

Running Servers

Item	IP	Group By	Server	Availability	Response Time	Total Actions	Slow	Connection Availability	Total	Total Traffic	Actions with Slow Server
2020-0-17-e081-cct12b7-36a7-802	2020-a17-e081-cct12b7-36a7-802			100.00	0.18	6,343	48	99.95	6,504	6,504	10.1
mys4-vin06122.jpawiba.adppp.hp	16.60.183.86			-	-	-	-	100.00	33	0.0	0.0

Clients

Client	Running Software	Availability (%)	Response Time (sec)	Total Actions Hits	Slow Actions	Connection Availability (%)	Total Connections	Total Traffic (MB)	Actions with Slow Server Time
2020-0-17-e081-cct12b7-36a7-802	Web Server	100.00	0.18	6,343	48	99.95	6,504	10.1	10.1

Topology Map

### Session Summary

Analysis Reports > RUM Session Summary

Status Reports Analysis Reports Alerts Production Analysis Business Process Recognition Mobile Reports

RUM Session Summary 06/06/2015 10:00:00 AM-06/13/2015 10:00:00 AM (GMT+02:00) Jerusalem

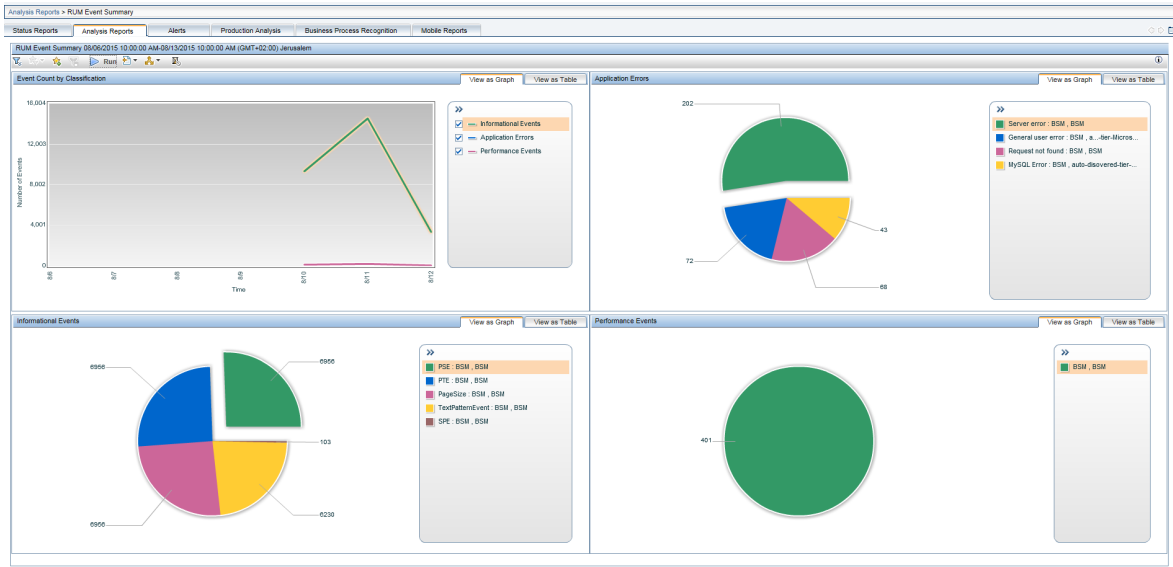
Session Overview

Value	Number of Sessions	Number of Subgroups	Error Events	Info Events	Performance Events	Total Actions	Unavailable Actions	Latency (ms)	Total Traffic (KB)
Thu, 21 Jan 2010 14:21:05 GMT	9	1	28	312	0	83	26	153.89	154.6
Thu, 21 Jan 2010 14:21:05 GMT	1	1	0	3	0	1	0	167.00	1.6
Thu, 21 Jan 2010 14:20:55 GMT	10	1	0	2,521	0	628	0	107.26	1,840.5
Thu, 21 Jan 2010 14:18:07 GMT	10	1	0	101	0	25	0	101.89	171.7
Thu, 21 Jan 2010 14:20:46 GMT	2	1	32	2,017	47	515	32	33.74	8,353.6
Thu, 21 Jan 2010 14:21:15 GMT	9	1	0	2,033	0	506	0	62.08	47,838.8
Thu, 21 Jan 2010 14:17:52 GMT	2	1	38	2,367	59	604	36	33.68	9,843.1
Thu, 21 Jan 2010 14:16:36 GMT	10	1	0	1,390	0	305	0	65.04	502.6
Thu, 21 Jan 2010 14:19:43 GMT	10	1	0	1,018	0	252	0	40.89	610.0
Thu, 21 Jan 2010 14:20:15 GMT	10	1	0	771	0	197	0	52.34	393.6
Thu, 21 Jan 2010 14:20:49 GMT	10	1	0	1,146	0	284	0	36.29	235.7
Thu, 21 Jan 2010 14:21:06 GMT	9	1	27	507	0	157	27	196.36	251.9
Thu, 21 Jan 2010 14:20:31 GMT	10	1	0	974	0	241	0	124.21	437.2
Thu, 21 Jan 2010 14:15:41 GMT	1	1	32	1,945	51	497	32	24.86	8,064.9
Thu, 21 Jan 2010 14:16:36 GMT	1	1	0	4	0	1	0	0.50	2.2
Thu, 21 Jan 2010 14:21:16 GMT	7	1	109	7,568	178	1,929	109	32.99	31,847.6
Thu, 21 Jan 2010 14:20:08 GMT	10	1	0	204	0	66	0	186.37	80.9
Thu, 21 Jan 2010 14:20:25 GMT	10	1	54	8,516	131	1,877	54	127.57	9,309.3
Undefined Value	10	0	0	73	0	24	318	66.41	38.3
	141		318	31,478	466	8,052	636	66.43	120,149.2

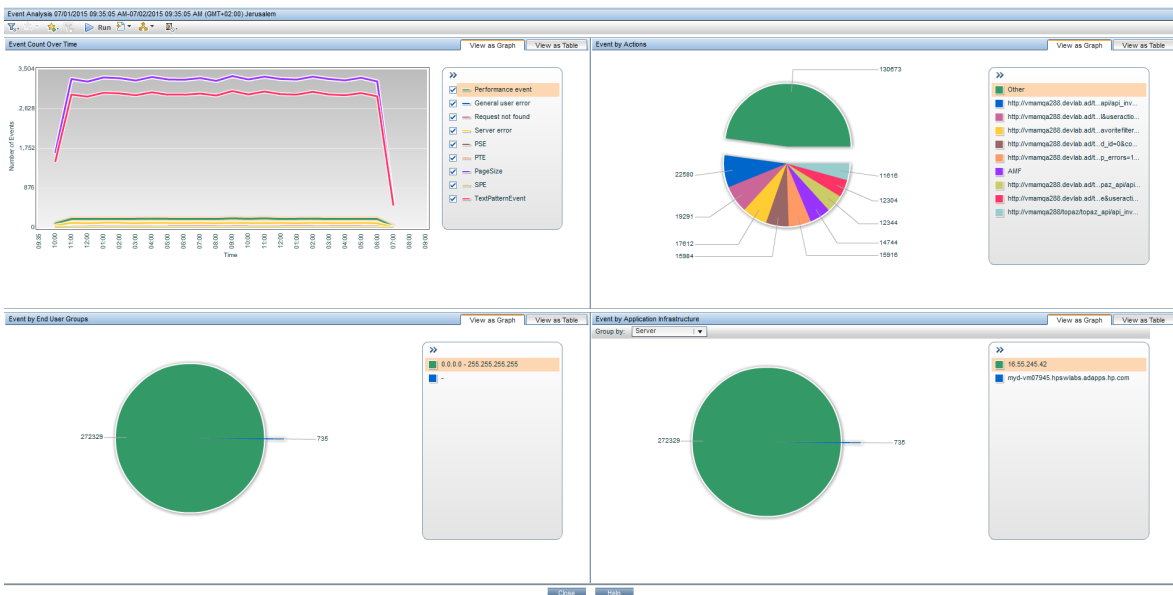
Detailed Subgroups

Value	Number of Sessions	Error Events	Info Events	Performance Events	Total Actions	Unavailable Actions	Latency (ms)	Total Traffic (KB)
vrmapa398	10	0	1,146	0	284	0	36.29	235.7
	10	0	1,146	0	284	0	36.29	235.7

## Event Summary



## Event Analysis



- **Flash/ActionScript AMF — HTTP Based**
  - **Versions:** AMF0, AMF3
  - **APM Template Name:** Flash

• **Sample Snapshots:**

**Session Analyzer**

Actions

There are 24 actions in the session with 24 frame units, of which 24 units are for the selected application. Session Replay    Session VuGen Script

Action	Start Time	Application	Events	Total Time (sec)	Server Time (sec)	Network Time (sec)	Client Time (sec)	Total Traffic (KB)
http://valletta_old.devlab.a...choAMF EchoAMF EchoAny([:0])	10/12/11 10:46:03 AM	Flex_for_Yan	-	0.37	0.20	0.16	0.00	
http://valletta_old.devlab.a...EchoAny([yy & amp; sss])	10/12/11 10:46:05 AM	Flex_for_Yan	TPE	0.31	0.17	0.14	0.00	
http://valletta_old.devlab.a...hoAny(11968-03-09 16:59:59!)	10/12/11 10:46:07 AM	Flex_for_Yan	-	0.39	0.20	0.19	0.00	
http://valletta_old.devlab.a...AMF EchoAMF /gateway.aspx?request=EchoAMF EchoAny([<?xml version=%221.0?><encoding=%22ISO-8859-1?><?guestbook-entry date=%224/1/2002?><name=11?><name=<email=22?<email=<date=4/21/2002?<date=<comment=33333333...])	10/12/11 10:46:12 AM	Flex_for_Yan	TPE	0.45	0.31	0.18	0.00	
http://valletta_old.devlab.a...Assemier, preter: c++]]]]	10/12/11 10:46:12 AM	Flex_for_Yan	TPE	0.39	0.21	0.18	0.00	
http://valletta_old.devlab.a...Object(prefs: VB.MET]]]]	10/12/11 10:46:14 AM	Flex_for_Yan	TPE	0.35	0.16	0.20	0.00	
http://valletta_old.devlab.a...Object(prefs: VB.MET]]]]	10/12/11 10:46:14 AM	Flex_for_Yan	TPE	0.48	0.22	0.27	0.00	

**Action Summary**

Analysis Reports > RUM Action Summary

Status Reports    Analysis Reports    Alerts    Production Analysis    Business Process Recognition    Mobile Reports

RUM Action Summary 04/09/2015 11:40:20 AM-04/10/2015 11:40:20 AM (GMT+02:00) Jerusalem

Highlights    Availability and Events    Performance

Action	Tier	Type	Total Action Hits	Availability (%)	Total Time (sec)	Server Time (sec)	Requests per Action Hit	Total Traffic (KB)
client_ping	AMF	Page	26	100.00	0.27	0.07	1.00	1.3
ProbAMF_errro[Test](\$faultCode=Server.Processing	AMF	Page	25	100.00	0.26	0.07	1.00	0.0
ProbAMF_echo[Test]	AMF	Page	25	100.00	0.21	0.01	1.00	1.2
ProbAMF_sendComplexObjects()	AMF	Page	25	100.00	0.20	0.00	1.00	1.6
ProbAMF_sendParam[Test]	AMF	Page	25	100.00	0.21	0.00	1.00	1.2
ProbAMF_getComplexObjects()	AMF	Page	25	100.00	0.27	0.07	1.00	1.8
			152	83.33	0.23	0.03	1.00	1.4

■ Critical   
 ■ OK   
 ■ Minor   
 ■ No data   
 ■ Downtime   
 ■ Unknown



# SOA

- **SOAP — HTTP Based**
  - **Versions:** 1.1, 1.2
  - **APM Template Name:** General SOAP Application
  - **Sample Snapshots:** Session Details

Analysis Reports > RUM Session Analyzer > Session Details

Session Details 4/9/2015 2:48 PM-2:51 PM (GMT+02:00) Jerusalem

Refresh

**Properties**

Start time:	4/9/2015 2:48 PM	Client IP:	16.55.245.32
Application:	SOAP	Client host name:	N/A
End user:	Others	User name:	N/A
urlgroup:	[0,0,0-255,255,255,255]	Server IP:	16.55.240.84
Location:	Palo Alto	Arrived from:	N/A
Total Traffic (KB):	3.9	Client type:	Commons-RtpClient 3.0
Duration (Minutes:Seconds):	00:00:39	HTTP version:	HTTP/1.1
Operating system:	N/A	Total action hits:	4
Latency (ms):	137.79		

**General Events**

No data was found.

**Actions**

There are 4 actions in the session with 4 frame units, of which 4 units are for the selected application.

Action	Start Time	Application	Events	Total Time (sec)	Server Time (sec)	Network Time (sec)	Client Time (sec)	Think Time (sec)	Total Traffic (KB)	Snapshot
http://16.55.246.84:8080/mcc...ex.net/GetWeatherByPlaceName	4/9/2015 02:49:54 PM	SOAP	-	0.138	0.003	0.136	0.000	0.000	4.123	1.2 No
http://16.55.246.84:8080/mcc...ex.net/GetWeatherByPlaceName	4/9/2015 02:49:59 PM	SOAP	-	0.143	0.007	0.136	0.000	0.000	9.208	1.2 No
http://16.55.246.84:8080/mcc...ex.net/GetWeatherByPlaceName	4/9/2015 02:50:08 PM	SOAP	Multiple events	0.202	0.006	0.196	0.000	0.000	25.505	1.0 Yes
http://16.55.246.84:8080/mcc...ex.net/GetWeatherByPlaceName	4/9/2015 02:50:34 PM	SOAP	-	0.090	0.005	0.085	0.000	0.000	6.000	0.6 No

- **WCF — HTTP Based**
  - **Versions:** any (NetTcpBinding binding is the only supported version)
  - **APM Template Name:** WCF TCP
  - **Sample Snapshots:** App Infrastructure

Analysis Reports > RUM Application Infrastructure Summary

RUM Application Infrastructure Summary [1/3/2015 2:10 PM-3:10 PM (GMT+02:00) Jerusalem

Refresh

**Running Software**

Name	IP Address	Availability (%)	Response Time (sec)	Total Actions Hits	Slow Actions	Connection Availability (%)	Total Connections	Total Traffic (MB)	Actions with Slow Server Time
153.88.171.27	153.88.171.27	64.71	0.28	255	0	100.00	34	1.6	0
WCF Service	153.88.171.27	64.71	0.28	255	0	100.00	34	1.6	0

**Clients**

Client	Running Software	Availability (%)	Response Time (sec)	Total Actions Hits	Slow Actions	Connection Availability (%)	Total Connections	Total Traffic (MB)	Actions with Slow Server Time
0.0.0.0-255.255.255.255	WCF Service	64.71	0.28	255	0	100.00	34	1.6	0

**Topology Map**

153.88.171.27

WCF Service

## Session Details

Analysis Reports > RUM Session Analyzer > Session Details

Status Reports Analysis Reports Alerts Production Analysis Business Process Recognition Mobile Reports

Session Details 8/13/2015 02:52:00 PM-08/16/2015 02:54:00 PM (GMT+02:00) Jerusalem

Refresh

Properties

Start time: 8/13/2015 2:53 PM Client IP: 150.236.177.61  
 Application: wcf4ftp Client host name: N/A  
 End user: Others Client host name: N/A  
 subgroup: [0.0.0.0-255.255.255.255] User name: N/A  
 Location: Sweden Server IP: 153.88.171.27  
 Total Traffic (KB): 27.9 Arrived from: N/A  
 Duration (hh:mm:ss): 00:16:07 Client type: N/A  
 Operating system: N/A HTTP version: HTTP/1.1  
 Latency (ms): 265.58 Total action hits: 9

General Events

No data was found.

Actions

There are 11 actions displayed with 11 frame units.

Action	Start Time	Application	Events	Total Time (sec)	Server Time (sec)	Network Time (sec)	Client Time (sec)	Think Time (sec)	Total Traffic (KB)	Snapshot
Authorization request	8/13/2015 03:06:28 PM	wcf4ftp	-	0.137	0.137	0.000	0.000	0.000	1.1	Yes
WCF Call to ProposaService.SavelserProfile	8/13/2015 03:06:28 PM	wcf4ftp	-	0.366	0.000	0.366	0.000	0.263	3.4	Yes
WCF Call to ProposaService.SavelserProfile	8/13/2015 03:03:35 PM	wcf4ftp	-	1.487	0.238	1.257	0.000	171.149	4.8	No
Authorization request	8/13/2015 03:03:35 PM	wcf4ftp	Request refused	0.137	0.137	0.000	0.000	0.284	1.1	Yes
WCF Call to ProposaService.SavelserProfile	8/13/2015 03:03:34 PM	wcf4ftp	Request refused	0.366	0.000	0.366	0.000	0.284	3.4	Yes

## Tier Summary

Analysis Reports > RUM Tier Summary

Status Reports Analysis Reports Alerts Production Analysis Business Process Recognition Mobile Reports

RUM Tier Summary 8/13/2015 2:11 PM-3:11 PM (GMT+02:00) Jerusalem

Refresh

Highlights Application Network

Tier	Tier Availability (%)	Total Action Hits	Available Action Hits	Slow Action Hits	Action Hits with Slow Server Time	Total Requests	Error Events	Info Events	Total Time (sec)	Server Time (sec)	Server Time to First Buffer (sec)	Network Time (sec)	Connect Time (sec)	SSL Handshake Time (sec)	Retransmit Time (sec)	Client Time (sec)
WCF over HTTP	0.00	255	165	0	0	255	90	0	0.26	0.06	0.07	0.20	0.00	0.00	0.00	0.00

Legend: Critical (Red), OK (Green), Minor (Yellow), No data (Grey), Downtime (Blue), Unknown (Black)

## Databases

- **Microsoft SQL Server**
  - **Versions:** 2000 and higher
  - **APM Template Name:** MS SQL
  - **Sample Snapshots:** Session Analyzer

Action	Start Time	Application	Events	Total Time (sec.)	Server Time (sec.)	Network Time (sec.)	Client Time (sec.)	Total Traffic (KB)
Prelogin	12:17:08 16/11/10	rotem_mssql	-	0.00	0.00	0.00	0.00	0.7
Prelogin SQL Server 2005 SP1+	12:17:08 16/11/10	rotem_mssql	-	0.00	0.00	0.00	0.00	0.1
Batch SET LOCK_TIMEOUT 30000	12:17:08 16/11/10	rotem_mssql	-	0.19	0.00	0.19	0.00	0.1
Batch SELECT @@LOCK_TIMEOUT	12:17:09 16/11/10	rotem_mssql	-	0.11	0.00	0.11	0.00	0.1
Batch SELECT @@LOCK_TIMEOUT	12:17:10 16/11/10	rotem_mssql	-	0.00	0.00	0.00	0.00	0.1
Batch SELECT s.physical_name... ON (s.type = 0 and s.databa	12:17:10 16/11/10	rotem_mssql	-	0.09	0.09	0.00	0.00	0.9
Batch SELECT @@LOCK_TIMEOUT	12:17:10 16/11/10	rotem_mssql	-	0.21	0.00	0.21	0.00	0.1
Batch SELECT CAST(serverprop...S sysname) AS [InstanceName]	12:17:10 16/11/10	rotem_mssql	-	0.00	0.00	0.00	0.00	0.4
Batch use [profile_1796_vmam...me = user_name()] AS [Defaul	12:17:10 16/11/10	rotem_mssql	-	0.18	0.18	0.00	0.00	1.2
Batch use [profile_1796_vmamrmd39]	12:17:10 16/11/10	rotem_mssql	-	0.00	0.00	0.00	0.00	0.3
Batch SELECT dtb.name AS [Na...ROPERTYEX](dtb.name, 'Col	12:17:10 16/11/10	rotem_mssql	-	0.02	0.02	0.00	0.00	2.2
Batch SELECT sch.name, sn.na... THEN 3 WHEN ObjectPropertyE	12:17:11 16/11/10	rotem_mssql	-	0.39	0.19	0.20	0.00	1.5
Batch SELECT CONVERT(bit, CH...on') AS nvarchar(255))	12:17:11 16/11/10	rotem_mssql	-	0.00	0.00	0.00	0.00	0.3
Batch SELECT CONVERT(bit, CH...on') AS nvarchar(255))	12:17:11 16/11/10	rotem_mssql	-	0.00	0.00	0.00	0.00	0.2

- **Oracle DB [+]**
  - **Versions:** Thin Client (JDBC): 10g R2, 11g
  - **APM Template Name:** Oracle DB

• **Sample Snapshots:**

**Action Summary**

Analysis Reports > RUM Action Summary

Status Reports | Analysis Reports | Utilities | Alerts | Production Analysis | Business Process Recognition

RUM Action Summary 02/22/2011 12:00:00 AM-03/01/2011 12:00:00 AM (GMT+02:00) Jerusalem

Highlights | Availability and Events | Performance

Application	Action	Type	Total Action Hits	Availability (%)	Total Time (sec)	Server Time (sec)	Requests per Action Hit	Total Traffic (KB)
Oracle_DB	Close Statement	Action	185	100.00	0.01	0.00	1.00	0.5
Oracle_DB	Disconnected/Logout	Action	1	100.00	0.00	0.00	1.00	0.0
Oracle_DB	DTY-Set Data Representations	Action	26	100.00	0.00	0.00	1.00	1.9
Oracle_DB	Logon(auth-password)	Action	16	100.00	0.00	0.00	1.00	1.1
Oracle_DB	Logon(auth-seskey)	Action	1	100.00	0.00	0.00	1.00	0.2
Oracle_DB	New Describe	Action	208	100.00	0.00	0.00	1.00	0.2
Oracle_DB	Query alter session set isolation_level = read committed	Action	2,341	100.00	0.00	0.00	1.00	0.2
Oracle_DB	Query SELECT '1' FROM DUAL	Action	2,803	100.00	0.01	0.00	1.00	0.2
Oracle_DB	RXD-Row Transfer Data Follows	Action	703	100.00	0.00	0.00	1.00	0.2
Oracle_DB	SNS-Secure Network Services Negotiation	Action	4	100.00	0.00	0.00	1.00	0.3
Oracle_DB	Rollback	Action	6,157	100.00	0.03	0.00	1.00	0.0
Oracle_DB	Commit	Action	15,638	100.00	0.03	0.00	1.00	0.0
			28,083	100.00	0.02	0.00	1.00	0.1

■ Critical   
 ■ OK   
 ■ Minor   
 ■ No data   
 ■ Downtime

**Session Analyzer**

Actions

Action	Start Time	Application	Events	Total Time (sec)	Server Time (sec)	Network Time (sec)	Client Time (sec)	Total Traffic (KB)
Version	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.2
Connect	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.2
DTY-Set Data Representations	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	2.0
Logon(auth-password)	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	1.3
Logon(auth-seskey)	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.3
PRO-Set Protocol	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.3
Query ALTER SESSION SET NLS_... HH24.MI.SS.FF TZH:TZM'	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.5
Query ALTER SESSION SET TIME_ZONE = '3:0'	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.2
Query SELECT '1' FROM DUAL	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.2
Query SELECT '1' FROM DUAL	2/28/11 01:40:22 PM	Oracle_DB	-	0.16	0.00	0.16	0.00	0.2
Query select A.CUSTOMER_ID,S... (sysdate-P.LAST_PING)*86400	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.9
Query select USER from DUAL	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.2
Query select TZ_OFFSET(DBTIMEZONE) from dual	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.3
Query select A.CUSTOMER_ID,S... (sysdate-P.LAST_PING)*86400	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	1.1
Version	2/28/11 01:40:22 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.1
Connect	2/28/11 01:40:22 PM	Oracle_DB	-	0.03	0.02	0.00	0.00	0.2
Query SELECT '1' FROM DUAL	2/28/11 01:40:27 PM	Oracle_DB	-	0.19	0.00	0.19	0.00	0.2
Query SELECT '1' FROM DUAL	2/28/11 01:40:27 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.2
Query SELECT '1' FROM DUAL	2/28/11 01:40:27 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.2
Query select SERVICE_ID,CUST... HA_TASKS where PROCESS_ID=4	2/28/11 01:40:27 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.2
Query update HA_PROCESSES set LAST_PING=sysdate where ID=4	2/28/11 01:40:27 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.2
Query SELECT '1' FROM DUAL	2/28/11 01:40:27 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.2
Query select SERVICE_ID,CUST... HA_TASKS where PROCESS_ID=4	2/28/11 01:40:27 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.6
Query SELECT '1' FROM DUAL	2/28/11 01:40:32 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.2
Query SELECT '1' FROM DUAL	2/28/11 01:40:32 PM	Oracle_DB	-	0.16	0.00	0.16	0.00	0.2
Query select A.CUSTOMER_ID,S... (sysdate-P.LAST_PING)*86400	2/28/11 01:40:32 PM	Oracle_DB	-	0.00	0.00	0.00	0.00	0.9

■ Critical   
 ■ OK   
 ■ Downtime   
 ■ Actions included in the ...

- **Comments:** JDBC thin driver is a software component that allows the Java application to connect the Oracle server without SQL\*Net installed. It is widespread in Java applets. There are other categories of JDBC drivers (JDBC OCI and JDBC KPRB) which require SQL\*Net to be installed. JDBC OCI and JDBC KPRB are not yet supported by RUM Monitoring. JDBC Thin connections allow RUM to report SQL queries and bound parameters (if any). The Oracle JDBC Thin driver uses TCP/IP connections.

- **MySQL**
  - **Versions:** 5.X and higher
  - **APM Template Name:** MySQL

- **Sample Snapshots: Session Analyzer**

Action	Start Time	Application	Total Time (sec.)	Server Time (sec.)	Network Time (sec.)	Client Time (sec.)	Total Traffic (KB)
Query: SET NAMES utf8	17:09:54 15/11/10	rotem_mysql	0.18	0.00	0.18	0.00	0.0
Query: SELECT @@sql_mode	17:09:54 15/11/10	rotem_mysql	0.00	0.00	0.00	0.00	0.1
Query: SET SESSION sql_mode=""	17:09:54 15/11/10	rotem_mysql	0.00	0.00	0.00	0.00	0.0
Query: show databases	17:09:56 15/11/10	rotem_mysql	0.14	0.00	0.14	0.00	0.2
Query: SHOW COLUMNS FROM `tables_priv`	17:10:01 15/11/10	rotem_mysql	0.01	0.01	0.00	0.00	0.8
Query: SHOW COLUMNS FROM `help_category`	17:10:01 15/11/10	rotem_mysql	0.05	0.05	0.00	0.00	0.5
Query: SHOW COLUMNS FROM `help_keyword`	17:10:01 15/11/10	rotem_mysql	0.02	0.02	0.00	0.00	0.4
Query: SHOW COLUMNS FROM `help_relati`	17:10:01 15/11/10	rotem_mysql	0.02	0.02	0.00	0.00	0.4
Query: SHOW COLUMNS FROM `help_topi`	17:10:01 15/11/10	rotem_mysql	0.02	0.02	0.00	0.00	0.5
Query: SHOW COLUMNS FROM `host`	17:10:01 15/11/10	rotem_mysql	0.01	0.01	0.00	0.00	1.1
Query: SHOW COLUMNS FROM `func`	17:10:01 15/11/10	rotem_mysql	0.01	0.01	0.00	0.00	0.4
Query: SHOW COLUMNS FROM `ndb_binlog_index`	17:10:01 15/11/10	rotem_mysql	0.01	0.01	0.00	0.00	0.6
Query: SHOW COLUMNS FROM `plugin`	17:10:01 15/11/10	rotem_mysql	0.01	0.01	0.00	0.00	0.4
Query: SHOW COLUMNS FROM `proc`	17:10:01 15/11/10	rotem_mysql	0.01	0.01	0.00	0.00	1.6

- **DB2**

- **Versions:** Type 4 driver (DRDA)

- **APM Template Name:** DB2

- **Sample Snapshots: Session Analyzer**

Action	Start Time	Application	Events	Total Time (sec.)	Server Time (sec.)	Network Time (sec.)	Client Time (sec.)	Total Traffic (KB)
EXCSQLSTT - Execute SQL Stat... an example</example>	12/2/10 02:01:31 PM	db2_yan	-	0.00	0.00	0.00	0.00	0.4
EXCSQLMIM - Execute Immediat..._est_stored WHERE ID = 1; END	12/2/10 02:01:31 PM	db2_yan	-	0.14	0.14	0.00	0.00	0.3
EXCSQLMIM - Execute Immediat..._est_stored WHERE ID = 1; END	12/2/10 02:01:31 PM	db2_yan	-	0.05	0.05	0.00	0.00	0.3
PRPSQLSTT - Prepare SQL Statement CALL EXCSQLMIM - Execute Immediate SQL Statement CREATE PROCEDURE processint(OUT risorsa int) LANGUAGE SQL BEGIN SELECT age INTO risorsa FROM test_stored WHERE ID = 1; END	12/2/10 02:01:31 PM	db2_yan	-	0.00	0.00	0.00	0.00	0.3
SECCHK - Security Check for ...069C17780601746F1D009A17A	12/2/10 02:01:31 PM	db2_yan	-	0.00	0.00	0.00	0.00	0.4
EXCSQLSTT - Execute SQL Statement CALL PROCESSINT( 0 )	12/2/10 02:01:31 PM	db2_yan	-	0.00	0.00	0.00	0.00	0.2
RDBCMM - RDB Commit Unit of Work	12/2/10 02:01:31 PM	db2_yan	-	0.00	0.00	0.00	0.00	0.1
PRPSQLSTT - Prepare SQL Statement CALL PROCESSVAR( ? )	12/2/10 02:01:31 PM	db2_yan	-	0.00	0.00	0.00	0.00	0.3
RDBCMM - RDB Commit Unit of Work	12/2/10 02:01:31 PM	db2_yan	-	0.00	0.00	0.00	0.00	0.1

- **Comments:** DRDA (Distributed Relational Database Architecture) is the only architecture (not an implementation) that enables different platforms to interchange relational data. JDBC Driver type 4 for DB2 implements DRDA to communicate with the DB2 server. It was first introduced in DB2 v.8.1. It does not require any additional middleware software to be installed. There is also DB2 CLI protocol which is used by Type 2, Type 3 to communicate to DB2 server. DB2 CLI is not yet supported by RUM. Monitoring DRDA connections allow RUM to report SQL queries and bound parameters (if any). DB2 JDBC Driver Type 4 usually uses TCP/IP connections.

- **SSDB**

- **APM Template Name:** SSDB
- **Sample Snapshots:**

### Session Details

The screenshot displays the 'Session Details' page in the Real User Monitor interface. The page is titled 'Session Details 5/25/2017 12:52 PM-12:54 PM (GMT+02:00) Jerusalem'. It features a navigation bar with tabs for 'Status Reports', 'Analysis Reports', 'Alerts', 'Production Analysis', 'Business Process Recognition', and 'Mobile Reports'. The main content area is divided into three sections: 'Properties', 'General Events', and 'Actions'.

**Properties:**

Start time:	5/25/2017 12:53 PM	Latency (ms):	0.00
Application:	ssdb-test	Client IP:	10.129.3.132
End user:	Others	Client host name:	N/A
subgroup:	[0.0.0.0.255.255.255.255]	User name:	N/A
Location:	UNKNOWN	Server IP:	10.120.16.205
Total Traffic (KB):	0.4	Total action hits:	1
Duration (hh:mm:ss):	00:00:00		
Operating system:	N/A		



**General Events:**

No data was found.

**Actions:**

Action	Start Time	Application	Events	Total Time (sec)	Server Time (sec)	Network Time (sec)	Client Time (sec)	Think Time (sec)	Total Traffic (KB)
200 AT06 IS00140000500 B23A8...190000000000000000000005 012000	5/25/2017 12:53:26 PM	ssdb-test	-	0.000	0.000	0.000	0.000	0.000	0.000

### Action Details

Action Details			
 			
Action Description			
<input type="button" value="Copy Description"/>			
<b>Action description:</b>	200 AT06 ISO0140000500 B23A840128E190000000000005000005 012000		
<b>Action name:</b>	N/A		
Action Parameters			
<b>Bitmap:</b>	B23A840128E190000000000005000005		
<b>Canal:</b>	AT06		
<b>CodigoProceso:</b>	012000		
<b>Command:</b>	ATH		
<b>ISO:</b>	ISO0140000500		
<b>TipoMensaje:</b>	200		
Connection Details			
<b>Server IP:</b>	10.120.16.205	<b>Client IP:</b>	10.129.3.132
<b>Server name:</b>	10.120.16.205	<b>Client name:</b>	N/A
<b>Server port:</b>	2135	<b>Client port:</b>	2159
<b>Running software:</b>	Unknown		
General			
<b>Stopped action hit:</b>	No	<b>Received traffic (KB):</b>	0.4
<b>Total requests:</b>	1	<b>Total traffic (KB):</b>	0.4
<b>Start time:</b>	5/25/2017 12:53:26 PM	<b>End user subgroup:</b>	Others [0.0.0.0-255.255.255.255]
<b>Sent traffic (KB):</b>	0.0		
Performance			
<b>Total time (sec):</b>	0.00	<b>Connect time (sec):</b>	0.00
<b>Server time (sec):</b>	0.00	<b>SSL handshake time (sec):</b>	0.00
<b>Server time to first buffer (sec):</b>	0.00	<b>Retransmit time (sec):</b>	0.00
<b>Network time (sec):</b>	0.00	<b>Client time (sec):</b>	0.00
Events			

- **Comments:** SSDB is a text based custom protocol supported by RUM.  
 For detailed information about configuring textual protocols, see "[RUM Probe Textual Protocol Configuration](#)" on page 246.

# Application Servers

- **Citrix XenApp (ICA) [+]**
  - **Versions:** 4.5 - 6.5
  - **APM Template Name:** Citrix ICA
  - **Sample Snapshots:** Session Summary

RUM Session Summary 16/11/2010 16:01-17:01 (GMT+02:00)Israel Standard Time

Session Groups

Group session by: Username

Value	Number of Sessions	Number of sub-groups	Error Events	Latency	Total Traffic(KB)
WL_LHJvu1k\InD-CFtu	4	1	0	0	350.2
	4		0	0.02	350.2

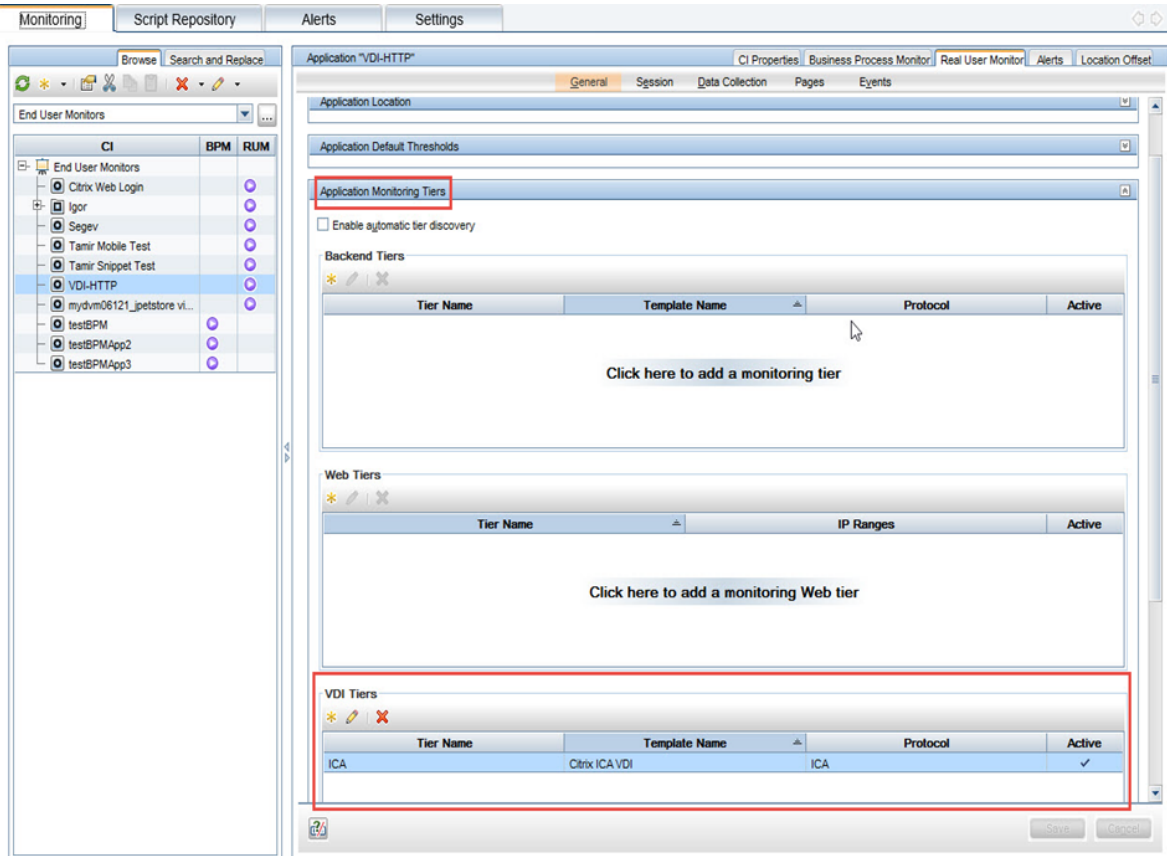
Detailed Sub Groups

Group session by: Published Application

Value	Number of Sessions	Error Events	Latency	Total Traffic(KB)
Sap Logon	4	0	0.02	350.2
	4	0	0.02	350.2

- **XenApp Application configured as a VDI tier under the main General Web Application**
  - **Versions:** 6.5
  - **APM Template Name:** Citrix ICA VDI

• **Sample Snapshots:**





### New Monitoring VDI Tier

#### Monitoring Settings

Configure the application's monitoring setting

Status:  Active  Inactive

Protocol: ICA

Template name: Citrix ICA VDI

\* Tier name:

Profile database: myd\_vm01185\_Prddb

[Engines](#) MYD-VM00088 - All probes

Assign Application 360 license \* AppOS count for this application:

#### Application Location

Use **both** host IP ranges and filters to determine the application location

IP Range	Port	SSL
0.0.0.0-255.255.255.255	1494	-
0.0.0.0-255.255.255.255	2598	-

#### Filter

Click here to add a filter (Mandatory)

#### Monitoring

Monitoring | Script Repository | Alerts | Settings

Browse Search and Replace

End User Monitors

- CI
- BPM
- RUM
- End User Monitors
  - Citrix Web Login
  - Igor
  - Segev
  - Tamir Mobile Test
  - Tamir Snippet Test
  - VDI-HTTP
  - mydvm06121\_petstore v1...
  - testBPM
  - testBPMApp2
  - testBPMApp3

Application "VDI-HTTP"

General | **Session** | Data Collection | Pages | Events

Session Identification

Session Reset

Session Properties

Active	Name	Search	Content	Removable
✓	VDI User Name	HTTP Header	Header name: RUM_AGENT, All content	-
✓	VDI Server IP	HTTP Header	Header name: RUM_AGENT, All content	-

#### RUM Session Analyzer

Start Time	Tier	End User Subgroup	Client	VDI Server IP	User Name	VDI User Name	Locatio	Active	Duration (hh:mm:ss)	Latenc (ms)	VDI Latency (ms)	Error Events	Informational Events	Slow Actions	Actions	Has Data for VuGen Scripts
1/7/2015 10:05 PM	HTTP-Web	Others [0.0.0.0-255.255.255.255]	16.60.153.192	16.60.153.192	-	hpsvlab01auid	Palo Alto	No	00:01:45	64.45	360.38	15	0	0	34	No
1/7/2015 3:53 PM	HTTP-Web	Others [0.0.0.0-255.255.255.255]	16.60.153.192	16.60.153.192	-	hpsvlab01auid	Palo Alto	No	00:01:11	60.5	360.38	14	0	0	35	No
1/7/2015 3:17 PM	HTTP-Web	Others [0.0.0.0-255.255.255.255]	16.60.153.192	16.60.153.192	-	hpsvlab01ahkrun	Palo Alto	No	00:01:14	64.02	175.68	17	0	0	40	No
1/7/2015 3:14 PM	HTTP-Web	Others [0.0.0.0-255.255.255.255]	16.60.153.192	16.60.153.192	-	hpsvlab01auid	Palo Alto	No	00:01:04	64.13	197.36	27	0	0	58	No
1/7/2015 2:41 PM	HTTP-Web	Others [0.0.0.0-255.255.255.255]	16.60.153.192	16.60.153.192	-	hpsvlab01auid	Palo Alto	No	00:01:17	64.93	197.36	8	0	0	16	No
1/7/2015 2:32 PM	HTTP-Web	Others [0.0.0.0-255.255.255.255]	16.60.153.192	16.60.153.192	-	hpsvlab01auid	Palo Alto	No	00:00:44	60.15	197.36	11	0	0	28	No
1/7/2015 1:54 PM	HTTP-Web	Others [0.0.0.0-255.255.255.255]	16.60.153.192	16.60.153.192	-	hpsvlab01ahkrun	Palo Alto	No	00:05:12	58.48	175.9	6	0	0	18	No
					0/7					62.74	308.86	98	0	0	229	

### Active Filters

- Session Properties
- End User Groups
- Transactions
- Servers
- Locations
- User Properties
- Actions
- Events
- Tiers

Application	Tier	Session Property	Operator	Value
VDI-HTTP	HTTP-Web	VDI Server IP	ignore	
VDI-HTTP	HTTP-Web	VDI User Name	ignore	

Session status:  All  Active  Closed

Show only sessions with data for generating VuGen scripts

Only show sessions accessed via VDI tier

Only show sessions accessed directly from application

### Session Details 1/7/2015 10:04 PM-10:08 PM (GMT+02:00) Jerusalem

Refresh

Properties

Start time:	1/7/2015 10:05 PM	Client IP:	16.60.153.192
Application:	VDI-HTTP	Client host name:	N/A
End user subgroup:	Others [0.0.0.0-255.255.255.255]	User name:	N/A
Location:	Palo Alto	Server IP:	16.60.183.85
Total Traffic (KB):	793.9	Arrived from:	N/A
Duration (hh:mm:ss):	00:01:45	Client type:	Internet Explorer 8.0
Operating system:	Windows	HTTP version:	HTTP/1.1
Latency (ms):	64.45	Total action hits:	34

### VDI Session Properties

Duration (hh:mm:ss):	06:36:14	VDI Latency (ms):	360.38	VDI Server IP:	16.60.153.192
Start time:	1/7/2015 3:52 PM	VDI User Name:	hpsvblabs\taubd		

### General Events

No data was found.

### Actions

There are 34 actions in the session with 34 frame units, of which 34 units are for the selected application.

Action	Start Time	Application	Events	Total Time (sec)	Server Time (sec)	Network Time (sec)	Client Time (sec)	Think Time (sec)	Total Traffic (KB)	Snapshot
http://myd-vm06121.hpsvblabs.../min/getApplicationStatusAjax	1/7/2015 10:05:54 PM	VDI-HTTP	Request refused	0.122	0.017	0.105	0.000	0.001	1.9	Yes
http://myd-vm06121.hpsvblabs.../om:0080/cyclos/oa/admin/home	1/7/2015 10:05:54 PM	VDI-HTTP	-	0.012	0.012	0.000	0.000	0.000	1.0	No
http://myd-vm06121.hpsvblabs.../hp.com:0080/cyclos/oa/login	1/7/2015 10:05:54 PM	VDI-HTTP	-	0.409	0.049	0.420	0.000	8.954	55.0	No
http://myd-vm06121.hpsvblabs.../cpal-admin?passwdrds=***	1/7/2015 10:06:04 PM	VDI-HTTP	-	0.225	0.007	0.213	0.000	2.805	1.3	No

### Session Groups

Group session by: VDI User Name

Value	Number of Sessions	Number of Subgroups	Error Events	Info Events	Performance Events	Total Actions	Unavailable Actions	Latency (ms)	Total Traffic (KB)	VDI Latency (ms)
hpsvblabs\shukrun	2	1	23	0	0	58	23	62.31	1,403.4	175.74
hpsvblabs\taubd	5	1	75	0	0	171	75	62.88	4,053.7	320.92
	7		98	0	0	229	98	62.74	5,457.1	308.86

### Detailed Subgroups

Group session by: VDI Server IP

Value	Number of Sessions	Error Events	Info Events	Performance Events	Total Actions	Unavailable Actions	Latency (ms)	Total Traffic (KB)	VDI Latency (ms)
16.60.153.192	2	23	0	0	58	23	62.31	1,403.4	175.74
	2	23	0	0	58	23	62.31	1,403.4	175.74

#### VDI Connectivity and Number of Sessions over time

#### VDI Performance (latency) and Number of Sessions over time

### RUM Tier Summary 01/07/2015 10:54:30 AM-01/08/2015 10:54:30 AM (GMT+02:00) Jerusalem

View: [Past day] From: 1/7/15 10:54 AM To: 1/8/15 10:54 AM (GMT+02:00) Jerusalem

Applications: VDI-HTTP

Active Filters: None (Restore Default Settings)

Tier	Tier Availability (%)	Total Action Hits	Slow Action Hits	Total Time (sec)	Total Requests	Connection Availability (%)	Total Connection Attempts	Total Traffic (MB)	Latency (ms)
HTTP-Web	100.00	300	0	0.44	3,183	100.00	117	7.6	73.45
ICA	-	-	-	-	-	100.00	16	1.2	198.80

RUM Application Infrastructure Summary 01/13/2015 07:35:00 PM-01/14/2015 07:35:00 PM (GMT+02:00) Jerusalem

Highlights Application Network

Running Software

Name	IP Address	Connection Availability (%)	Total Connections	Total Timed-out Connections	Total Refused Connections	Connect Time (sec)	SSL Handshake Time (sec)	Packets With Network Errors (%)	Packets With Server Errors (%)	Throughput (bit/sec)	Total Traffic (MB)	Application Traffic (MB)	Latency (ms)
mys-vn06121.hps.wiabs.adapps.hp.com	16.60.183.85	100.00	235	0	0	0.06	0.00	0.05	0.00	2,124.63	21.9	21.0	80.93

- **Oracle Forms NCA [+]**
  - **Versions:** 11g
  - **APM Template Name:** Oracle Forms over HTTP/TCP
  - **Sample Snapshots:** Session Analyzer (v.8.02), Auto-discovered RUM Actions for Oracle Forms, RUM Actions matching Oracle Forms traffic

1-15 of 15

Page	Start Time	Application	Page Time (sec.)	Server Time (sec.)	Network Time (sec.)	
Oracle Applications 11i	3/30/09 04:48:20 PM	Oracle_Forms_8000_9000	0.04	0.01	0.00	
Oracle Forms Handshake	3/30/09 04:48:26 PM	Oracle_Forms_8000_9000	0.00	0.00	0.00	
Connect: server module=/opt/applvis/visappl/fnd/11.5.0/forms/US/FNDSCSG N userid=APPLSYS/PUB@VIS fndnam=APPS record=names	3/30/09 04:48:26 PM	Oracle_Forms_8000_9000	0.14	0.14	0.00	
Oracle Applications: Form updates	3/30/09 04:48:27 PM	Oracle_Forms_8000_9000	1.11	0.75	0.36	
Oracle Applications - ADS Vision LM0001: Form updates	3/30/09 04:48:30 PM	Oracle_Forms_8000_9000	0.30	0.30	0.00	
Oracle Applications: Form updates	3/30/09 04:48:30 PM	Oracle_Forms_8000_9000	0.01	0.01	0.00	
Navigator - Payables, Vision Operations (USA): Form updates	3/30/09 04:48:30 PM	Oracle_Forms_8000_9000	0.07	0.07	0.00	
Oracle Applications: Connect.event: NAVIGATOR_TYPE_0.event; NAVIGATOR_TYPE_0.event; NAVIGATOR_TYPE_0.change_cursor_position	3/30/09 04:48:30 PM	Oracle_Forms_8000_9000	0.00	0.00	0.00	
Navigator - Payables, Vision Operations (USA): NAVIGATOR_TYPE_0.event; NAVIGATOR_LIST_0.event	3/30/09 04:48:30 PM	Oracle_Forms_8000_9000	0.55	0.41	0.14	
Suppliers (Vision Operations: USD): VNR_VENDOR_NAME_MIR_0.set_text(M); VNR_VENDOR_NAME_MIR_0.event; VNR_VENDOR_NAME_MIR_0...	3/30/09 04:48:32 PM	Oracle_Forms_8000_9000	0.45	0.12	0.34	
Calendar: CALENDAR_NEXT_MONTH_0.event; CALENDAR_NEXT_MONTH_0.event; CALENDAR_NEXT_MONTH_0.event; OK.event; CALENDAR_NEXT...	3/30/09 04:48:35 PM	Oracle_Forms_8000_9000	0.51	0.16	0.35	
Suppliers (Vision Operations: USD): window.function_activate	3/30/09 04:48:38 PM	Oracle_Forms_8000_9000	0.02	0.02	0.00	
Calendar: OK.event; VNR_PARENT_VENDOR_NAME_MIR_0.event; VNR_PARENT_VENDOR_NAME_MIR_0.event; VNR_PARENT_VEN...	3/30/09 04:48:38 PM	Oracle_Forms_8000_9000	0.13	0.00	0.13	
Suppliers (Vision Operations: USD): VNR_PARENT_VENDOR_NAME_MIR_0.event; VNR_VENDOR_NAME_MIR_0.event	3/30/09 04:48:39 PM	Oracle_Forms_8000_9000	0.61	0.43	0.18	
Oracle Applications - ADS Vision LM0001: Oracle Applications - ADS Vision LM0001.event	3/30/09 04:48:41 PM	Oracle_Forms_8000_9000	0.00	0.00	0.00	

Pages included in the selected application session

Application: Ora Forms™

CI Properties Business Process Monitor Real User Monitor Alerts Location Offset

General Session Data Collection Pages Events

Browse Search

Root Auto discovered

Auto discovered Folder Content

Name	Active	In Use	URL	Parameters	Auto Discov...
zsa change cursor position	✓	–	/zsa_(unb.zsa)	*change_cur...	✓
znk2.promics change cursor posi...	✓	–	/znk2.promics...	*change_cur...	✓
wizzard	✓	–	/wizzard_for_...		✓
wizzard change cursor position	✓	–	/wizzard_for_...	*change_cur...	✓
wizzard event	✓	–	/wizzard_for_...	*event=	✓
wichtige informationen resize	✓	–	/wichtige_info...	*resize=	✓
webutil	✓	–	/webutil_infor...		✓
webutil change cursor position	✓	–	/webutil_infor...	*change_cur...	✓
webutil event	✓	–	/webutil_infor...	*event=	✓
vua.sigma	✓	–	/vua.sigma_v...		✓
vua.sigma change cursor position	✓	–	/vua.sigma_v...	*change_cur...	✓
vua.sigma event	✓	–	/vua.sigma_v...	*event=	✓
vhm.vf event	✓	–	/vhm.vf_verb...	*event=	✓
vf	✓	–	/vf_(ttb.vf)		✓
vf change cursor position	✓	–	/vf_(ttb.vf)	*change_cur...	✓
vf event	✓	–	/vf_(ttb.vf)	*event=	✓
vf.vf	✓	–	/vf.vf_verbots...		✓
vf.vf event	✓	–	/vf.vf_release...	*event=	✓
user event	✓	–	/user_settings	*event=	✓
user	✓	–	/user_profile		✓
ubk	✓	–	/ubk_ _msp_p...		✓
ubk change cursor position	✓	–	/ubk_ _msp_p...	*change_cur...	✓
ubk event	✓	–	/ubk_ _msp_p...	*event=	✓
ubk-nimbus	✓	–	/ubk-nimbus_l...		✓
ubk-nimbus change cursor position	✓	–	/ubk-nimbus_l...	*change_cur...	✓
ubk-nimbus event	✓	–	/ubk-nimbus_l...	*event=	✓
ubk-nimbus resize	✓	–	/ubk-nimbus_l...	*resize=	✓
ubk-msp	✓	–	/ubk-msp_log...		✓
ubk-msp change cursor position	✓	–	/ubk-msp_log...	*change_cur...	✓
ubk-msp event	✓	–	/ubk-msp_log...	*event=	✓
ubk-msp resize	✓	–	/ubk-msp_log...	*resize=	✓

MyBSM Applications Admin Help Site Map

Analysis Reports > RUMAction Summary

Status Reports Analysis Reports Utilities Alerts Production Analysis Business Process Recognition Mobile Reports

RUM Action Summary 10/08/2014 05:09:57 PM-10/09/2014 05:09:57 PM (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Highlights Availability and Events Performance

Action	Tier	Type	Total Action Hits	Availability (%)	Total Time (sec)	Server Time (sec)	Requests per Action Hit	Total Traffic (KB)
forms-java	NCA Over HTTP	Page	15,984	0.18	0.03	0.00	1.23	0.3
ang.angebote event	NCA Over HTTP	Page	1	100.00	0.02	0.00	1.00	0.7
sigma	NCA Over HTTP	Page	8	100.00	0.18	0.00	1.00	0.7
alsb.erzeugnisse change cursor position	NCA Over HTTP	Page	2	100.00	0.11	0.00	1.00	0.7
ang.angebote ch...	http://*.4445/ALSB.ERZEUGNISSE_Applications_for_LS_B-number_order_sheet_BSP2NU?134.change_cursor_pos...				0.02	0.00	1.00	0.7
standard resize					0.13	0.00	1.00	0.7
ubk-msp resize	NCA Over HTTP	Page	345	100.00	0.05	0.00	1.00	0.7
pms.pms event	NCA Over HTTP	Page	16	100.00	0.17	0.00	1.00	0.7
gs-is-prod resize	NCA Over HTTP	Page	5,497	100.00	0.08	0.00	1.00	0.7
sv.pms event	NCA Over HTTP	Page	34	100.00	0.19	0.00	1.00	0.7
wichtige informationen resize	NCA Over HTTP	Page	145	100.00	0.05	0.00	1.00	0.7
keine	NCA Over HTTP	Page	3	100.00	0.23	0.00	1.00	0.9
service resize	NCA Over HTTP	Page	56	100.00	0.22	0.00	1.00	0.7
fmea.fmea change cursor position	NCA Over HTTP	Page	5	100.00	0.13	0.00	1.00	0.7
erzeugnisse: event	NCA Over HTTP	Page	2	100.00	0.20	0.00	1.00	0.7
per.permes change cursor position	NCA Over HTTP	Page	2	100.00	0.01	0.00	1.00	0.7
important resize	NCA Over HTTP	Page	25	100.00	0.18	0.00	1.00	0.7

- WMQ
  - Versions: WMQ6, WMQ7, WMQ8
  - APM Template Name: MQ



## Session Details

Analysis Reports > RUM Session Analyzer > Session Details

Status Reports Analysis Reports Alerts Production Analysis Business Process Recognition Mobile Reports

Session Details: 4/9/2015 4:40 PM-4:47 PM (GMT+02:00) Jerusalem

Refresh

Properties

Start time: 4/9/2015 4:41 PM Latency (ms): 110.52  
 Application: SAP\_demo Client IP: 16.59.61.27  
 End user: Others [0.0.0.0-255.255.255.255] Client host name: N/A  
 subgroups: 255.255.255.255  
 Location: Palo Alto User name: GA01  
 Total Traffic (KB): 106.2 Server IP: 16.44.49.44  
 Duration (minutes): 00:05:20 Total action hits: 20  
 Operating system: N/A

General Events

No data was found.

Actions

Action	Start Time	Application	Events	Total Time (sec)	Server Time (sec)	Network Time (sec)	Client Time (sec)	Think Time (sec)	Total Traffic (KB)
SESSION_MANAGER	4/9/2015 04:41:14 PM	SAP_demo	Multiple events	22.241	0.037	0.634	21.570	24.438	5.4
SESSION_MANAGER	4/9/2015 04:42:00 PM	SAP_demo	ASE	0.145	0.003	0.142	0.000	6.434	4.0
ABAP Function Modules (SE37)	4/9/2015 04:42:07 PM	SAP_demo	ASE	0.024	0.024	0.000	0.000	65.027	4.6
ABAP Function Modules (SE37)	4/9/2015 04:43:12 PM	SAP_demo	Multiple events	149.132	12.602	0.919	135.526	2.910	24.4
ABAP Function Modules (SE37)	4/9/2015 04:45:43 PM	SAP_demo	ASE	0.012	0.012	0.000	0.000	2.100	4.3
SESSION_MANAGER	4/9/2015 04:45:45 PM	SAP_demo	ASE	0.207	0.002	0.205	0.000	3.797	3.4
Create Sales Order (VA01)	4/9/2015 04:45:49 PM	SAP_demo	Multiple events	2.963	0.422	0.627	1.913	2.294	5.0
SESSION_MANAGER	4/9/2015 04:45:54 PM	SAP_demo	ASE	0.208	0.002	0.204	0.000	1.696	3.5
Change Sales Order (VA02)	4/9/2015 04:45:56 PM	SAP_demo	Multiple events	2.835	0.163	0.204	2.468	3.040	5.3
SESSION_MANAGER	4/9/2015 04:46:02 PM	SAP_demo	ASE	0.208	0.002	0.207	0.000	2.230	3.5
Display Sales Order (VA03)	4/9/2015 04:46:05 PM	SAP_demo	Multiple events	3.662	0.055	0.221	3.386	3.020	5.3
SESSION_MANAGER	4/9/2015 04:46:11 PM	SAP_demo	ASE	0.205	0.002	0.203	0.000	1.945	3.5
Archive Administration (SARA)	4/9/2015 04:46:13 PM	SAP_demo	ASE	0.212	0.003	0.199	0.000	2.221	3.4

Analysis Reports > RUM Session Analyzer > Session Details

Status Reports Analysis Reports Alerts Production Analysis Business Process Recognition Mobile Reports

Session Details: 4/9/2015 3:54 PM-4:02 PM (GMT+02:00) Jerusalem

Refresh

Properties

Start time: 4/9/2015 3:55 PM Latency (ms): 110.52  
 Application: SAP\_demo Client IP: 16.59.61.27  
 End user: Others [0.0.0.0-255.255.255.255] Client host name: N/A  
 Location: Palo Alto User name: GA01  
 Total Traffic (KB): 106.2 Server IP: 16.44.49.44  
 Duration (minutes): 00:05:20 Total action hits: 20  
 Operating system: N/A

General Events

No data was found.

Actions

Action	Start Time	Application	Events	Total Time (sec)	Server Time (sec)	Network Time (sec)	Client Time (sec)	Think Time (sec)	Total Traffic (KB)
SESSION_MANAGER	4/9/2015 03:55:55 PM	SAP_demo	Multiple events	22.241	0.037	0.634	21.570	24.438	5.4
SESSION_MANAGER	4/9/2015 03:56:42 PM	SAP_demo	ASE	0.145	0.003	0.142	0.000	6.434	4.0
ABAP Function Modules (SE37)	4/9/2015 03:56:49 PM	SAP_demo	ASE	0.024	0.024	0.000	0.000	65.027	4.6
ABAP Function Modules (SE37)	4/9/2015 03:57:54 PM	SAP_demo	Multiple events	149.132	12.602	0.919	135.526	2.910	24.4
ABAP Function Modules (SE37)	4/9/2015 04:00:25 PM	SAP_demo	ASE	0.012	0.012	0.000	0.000	2.100	4.3
SESSION_MANAGER	4/9/2015 04:00:27 PM	SAP_demo	ASE	0.207	0.002	0.205	0.000	3.797	3.4
Create Sales Order (VA01)	4/9/2015 04:00:31 PM	SAP_demo	Multiple events	2.963	0.422	0.627	1.913	2.294	5.0
SESSION_MANAGER	4/9/2015 04:00:36 PM	SAP_demo	ASE	0.208	0.002	0.204	0.000	1.697	3.5
Change Sales Order (VA02)	4/9/2015 04:00:35 PM	SAP_demo	Multiple events	2.835	0.163	0.204	2.468	3.040	5.3
SESSION_MANAGER	4/9/2015 04:00:43 PM	SAP_demo	ASE	0.209	0.002	0.207	0.000	2.229	3.5
Display Sales Order (VA03)	4/9/2015 04:00:46 PM	SAP_demo	Multiple events	3.662	0.055	0.221	3.386	3.020	5.3
SESSION_MANAGER	4/9/2015 04:00:53 PM	SAP_demo	ASE	0.205	0.002	0.203	0.000	1.944	3.5
Archive Administration (SARA)	4/9/2015 04:00:55 PM	SAP_demo	ASE	0.212	0.003	0.199	0.000	2.221	3.4
SESSION_MANAGER	4/9/2015 04:00:57 PM	SAP_demo	ASE	0.201	0.002	0.199	0.000	1.483	3.5
Extended Computer Aided Test Tool (SECAT)	4/9/2015 04:00:59 PM	SAP_demo	ASE	0.365	0.005	0.254	0.107	1.528	6.8
SESSION_MANAGER	4/9/2015 04:01:01 PM	SAP_demo	ASE	0.206	0.001	0.205	0.000	6.300	3.5
Development Workbench Demos (DWDM)	4/9/2015 04:01:07 PM	SAP_demo	ASE	0.002	0.002	0.000	0.000	2.927	3.1
Development Workbench Demos (DWDM)	4/9/2015 04:01:10 PM	SAP_demo	ASE	0.038	0.038	0.000	0.000	4.246	2.9
Development Workbench Demos (DWDM)	4/9/2015 04:01:15 PM	SAP_demo	ASE	0.005	0.005	0.000	0.000	0.979	3.4

# Mailing Applications

- **IMAP**
  - **Versions:** Any
  - **APM Template Name:** IMAP
  - **Sample Snapshots:** Tier Summary

The top screenshot shows the following data for the IMAP tier:

Tier	Connection Availability (%)	Total Connection Attempts	Timed-out Connections	Refused Connections	Connect Time (sec)	SSL Handshake Time (sec)	Packets with Network Errors (%)	Packets with Server Errors (%)	Throughput (bits/sec)	Total Traffic (MB)	Application Traffic (MB)
IMAP	100.00	5	0	0	0.00	0.00	0.00	0.00	52.88	0.5	0.5

The bottom screenshot shows the following data for the IMAP tier:

Tier	Tier Availability (%)	Total Action Hits	Available Action Hits	Slow Action Hits	Action Hits with Slow Server Time	Total Requests	Error Events	Info Events	Total Time (sec)	Server Time (sec)	Server Time to First Buffer (sec)	Network Time (sec)	Connect Time (sec)	SSL Handshake Time (sec)	Retransmit Time (sec)	Client Time (sec)
IMAP	100.00	72	72	0	0	72	0	0	0.15	0.87	0.03	0.06	0.00	0.00	0.00	0.00

- **SMTP**
  - **Versions:** Any
  - **APM Template Name:** SMTP
  - **Sample Snapshots:** Session Analyzer

Action	Start Time	Application	Events	Total Time (sec.)	Server Time (sec.)	Network Time (sec.)	Client Time (sec.)	Total Traffic (KB)
Set sender address: qatest1@devlab.ad	15:39:11 15/11/10	SMTP	-	0.00	0.00	0.00	0.00	0.1
Mail content	15:39:11 15/11/10	SMTP	-	0.03	0.00	0.03	0.00	544.1
Quit	15:39:11 15/11/10	SMTP	-	0.00	0.00	0.00	0.00	0.1
Authentication	15:39:11 15/11/10	SMTP	-	0.00	0.00	0.00	0.00	0.0
Authentication	15:39:11 15/11/10	SMTP	-	0.00	0.00	0.00	0.00	0.1
Session initiation LABM2AM264	15:39:11 15/11/10	SMTP	-	0.00	0.00	0.00	0.00	0.3
Set recipient: qatest1@devlab.ad	15:39:11 15/11/10	SMTP	-	0.00	0.00	0.00	0.00	0.1
Set recipient: qatest1@devlab.ad	15:39:11 15/11/10	SMTP	-	0.00	0.00	0.00	0.00	0.1
Set recipient: qatest1@devlab.ad	15:39:11 15/11/10	SMTP	-	0.00	0.00	0.00	0.00	0.1
Set recipient: qatest1@devlab.ad	15:39:11 15/11/10	SMTP	-	0.00	0.00	0.00	0.00	0.1
Mail content	15:39:11 15/11/10	SMTP	-	0.00	0.00	0.00	0.00	0.1

- **POP3**
  - **Versions:** Any
  - **APM Template Name:** POP3

- **Sample Snapshots: Tier Summary**

Analysis Reports > RUM Tier Summary

Status Reports Analysis Reports Alerts Production Analysis Business Process Recognition Mobile Reports

RUM Tier Summary 04/09/2015 04:54:36 PM-04/10/2015 04:54:36 PM (GMT+02:00) Jerusalem

Highlights Application Network

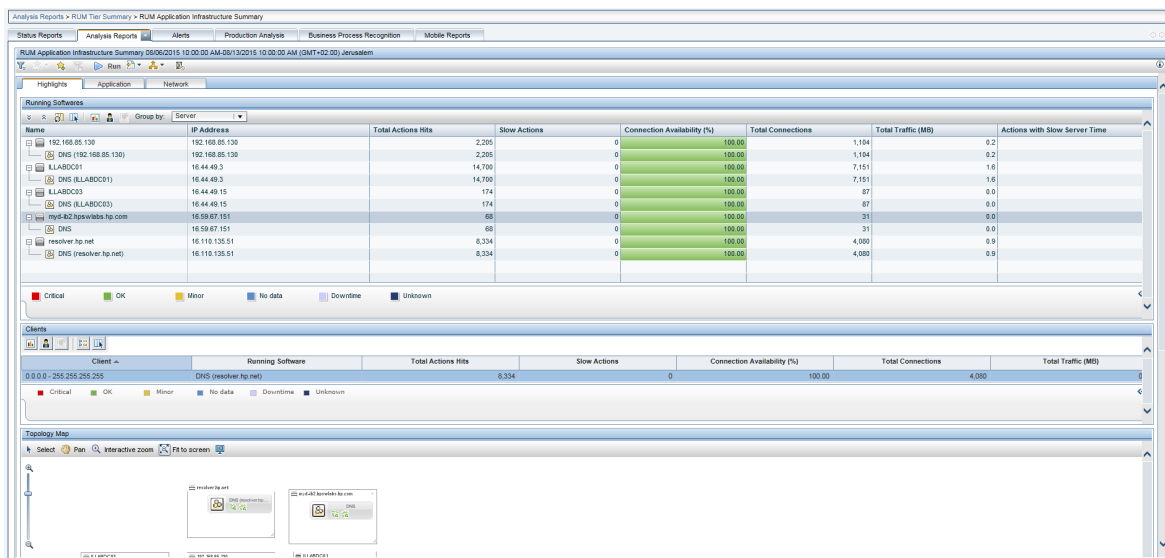
Tier	Tier Availability (%)	Total Action Hits	Slow Action Hits	Total Time (sec)	Total Requests	Connection Availability (%)	Total Connection Attempts	Total Traffic (MB)
POP3	100.00	32	0	5.00	32	100.00	6	0.0

■ Critical ■ OK ■ Minor ■ No data ■ Downtime ■ Unknown



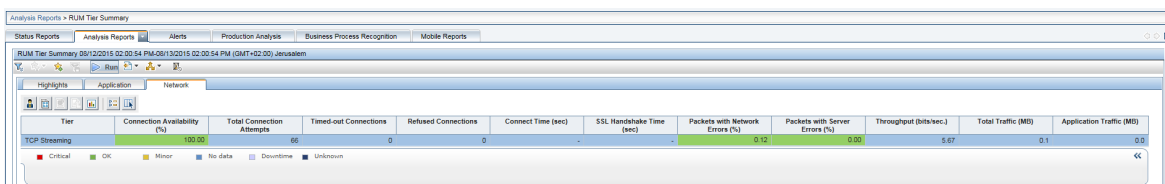
# Generically Supported Protocols

- **DNS — Generic UDP**
  - **Versions:** Any (UDP only)
  - **APM Template Name:** DNS
  - **Sample Snapshots:** App Infrastructure

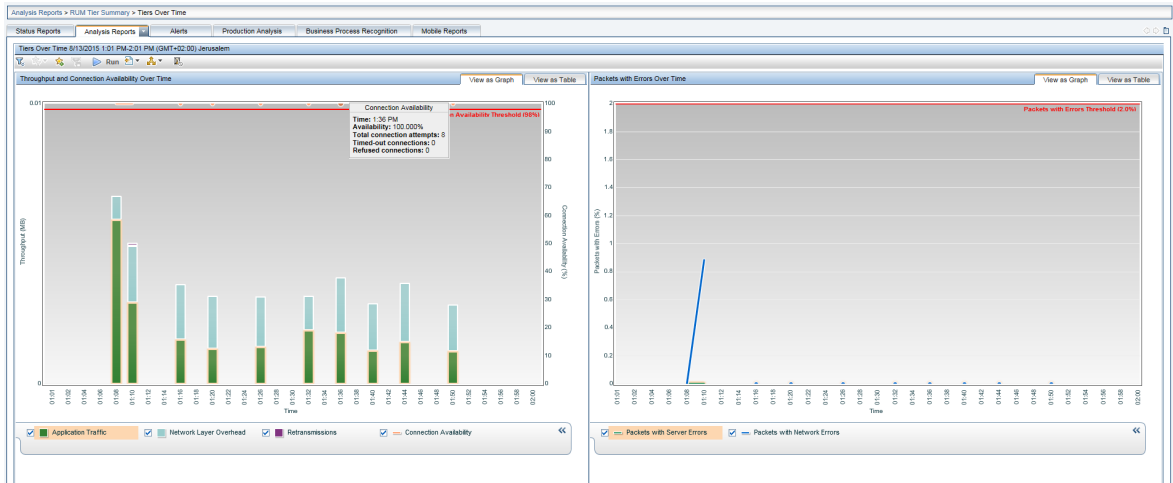


- **Microsoft Terminals Services (RDP) — Generic Streaming TCP**
  - **Versions:** Any
  - **APM Template Name:** Microsoft Terminal Service (RDP)
  - **Sample Snapshots:**

## Tier Summary



### Tiers Over Time



- **RMI Registry — Generic TCP**
  - **Versions:** Any
  - **APM Template Name:** RMI Registry
  - **Sample Snapshots:**  
Tier Summary

Analysis Reports > RUM Tier Summary

RUM Tier Summary 04/09/2015 04:58:18 PM-04/10/2015 04:58:18 PM (GMT+12:00) Jerusalem

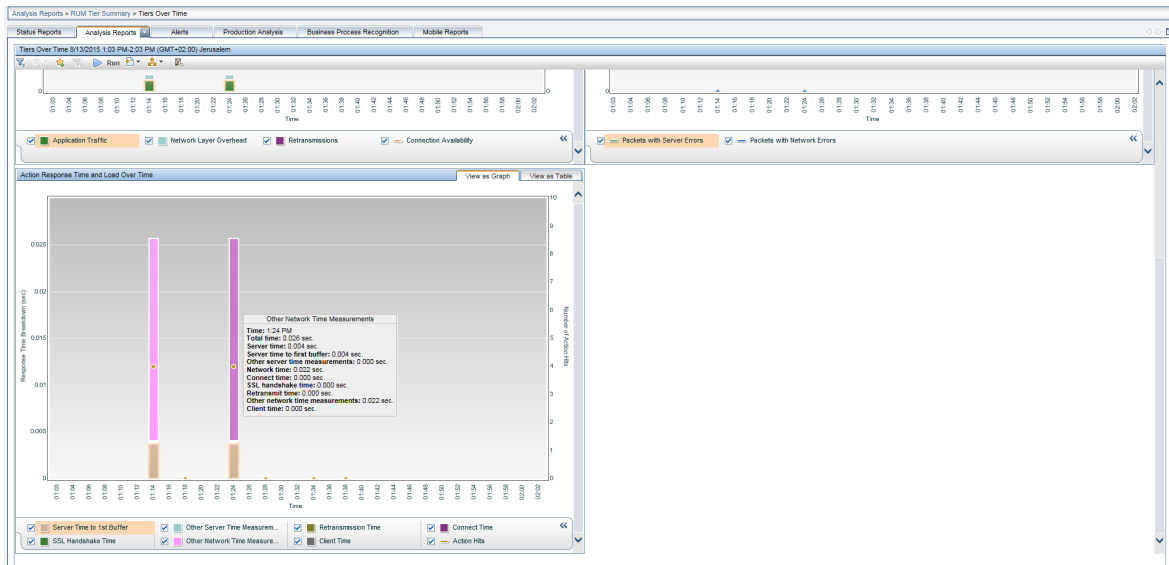
Tier	Tier Availability (%)	Total Action Hits	Slow Action Hits	Total Time (sec)	Total Requests	Connection Availability (%)	Total Connection Attempts	Total Traffic (MB)
TCP Request-Response	100.00	20	0	0.01	20	100.00	5	0.0

Analysis Reports > RUM Tier Summary

RUM Tier Summary 04/09/2015 04:58:18 PM-04/10/2015 04:58:18 PM (GMT+12:00) Jerusalem

Tier	Connection Availability (%)	Total Connection Attempts	Timed-out Connections	Refused Connections	Connect Time (sec)	SSL Handshake Time (sec)	Packets with Network Errors (%)	Packets with Server Errors (%)	Throughput (bits/sec)	Total Traffic (MB)	Application Traffic (MB)
TCP Request-Response	100.00	5	0	0	0.00	0.00	0.00	0.00	0.52	0.0	0.0

## Tiers Over Time



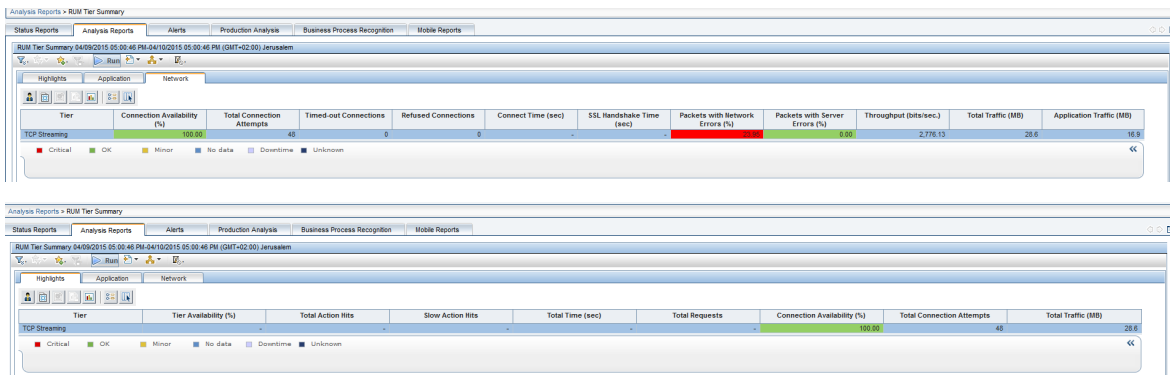
- **SSH — Generic Streaming TCP**
  - **Versions:** Any
  - **APM Template Name:** SSH
  - **Sample Snapshots:**  
App Infrastructure

Running Software												
Name	IP Address	Connection Availability (%)	Total Connections	Total Timed-out Connections	Total Refused Connections	Connect Time (sec)	SSL Handshake Time (sec)	Packets With Network Errors (%)	Packets With Server Errors (%)	Throughput (bit/sec.)	Total Traffic (MB)	Application Traffic (MB)
myapp0211.hpswebs.adapps.hp.com	16.69.154.173	100.00	5	0	0	0.00	0.00	0.00	0.00	6.91	0.5	0.5
Unknown	16.69.154.173	100.00	5	0	0	0.00	0.00	0.00	0.00	6.91	0.5	0.5

Clients												
Client	Running Software	Connection Availability (%)	Total Connections	Total Timed-out Connections	Total Refused Connections	Connect Time (sec)	SSL Handshake Time (sec)	Packets With Network Errors (%)	Packets With Server Errors (%)	Throughput (bit/sec.)	Total Traffic (MB)	Application Traffic (MB)
0.0.0.0-255.255.255.255	Unknown	100.00	5	0	0	0.00	0.00	0.00	0.00	6.91	0.5	0.5

## Tier Summary



## Financial Protocols

- **NDC**
  - **Versions:**
    - **Certified with version:** 03.02.01 conforming to B006-6180-J000, Issue 2, February 2008 Aprta Advance NDC Reference Manual
    - **Supported with version:** 04.02.01 conforming to B006-6180-P000, Issue 1, January 2013 Aprta Advance NDC Reference Manual
  - **APM Template Name:** Aprta Advance NDC
  - **Sample Snapshots**

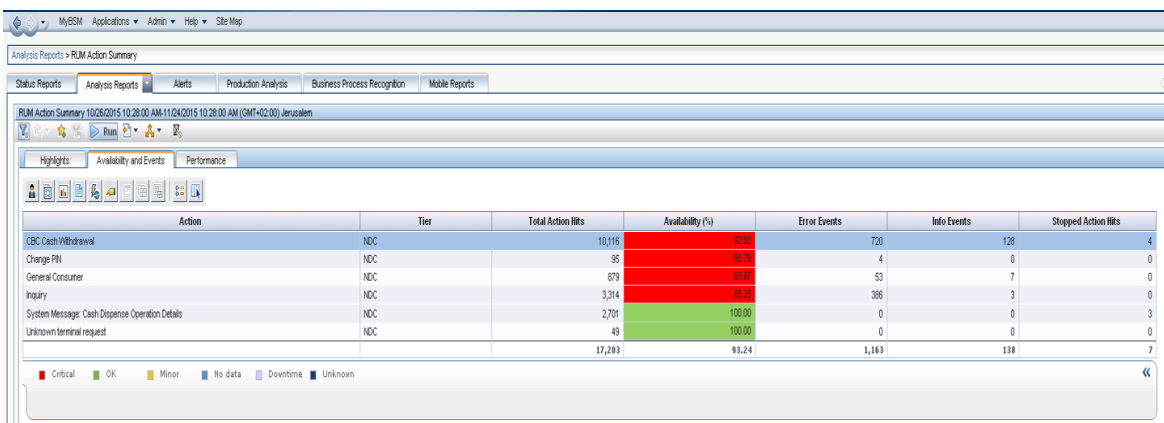
### RUM Session Summary Report

Value	Number of Sessions	Number of Unique Users	Error Events	Info Events	Performance Events	Total Actions	Unavailable Actions	Latency (ms)	Total Traffic (KB)
4010003	135	53	2	0	0	161	2	0.00	0.0
4010048	143	52	24	0	0	182	24	0.00	0.0
4010040	104	26	20	26	0	126	20	0.00	0.0
4010054	26	7	3	0	0	32	3	0.00	0.0
CBA04001	46	23	10	0	0	72	10	0.00	0.0
4010002	196	80	9	0	0	259	9	0.00	0.0
4010013	142	57	8	0	0	186	8	0.00	0.0
4010007	238	106	51	0	0	344	51	0.00	0.0
4010014	42	7	3	0	0	52	3	0.00	0.0
4010008	122	38	13	1	0	128	13	0.00	0.0

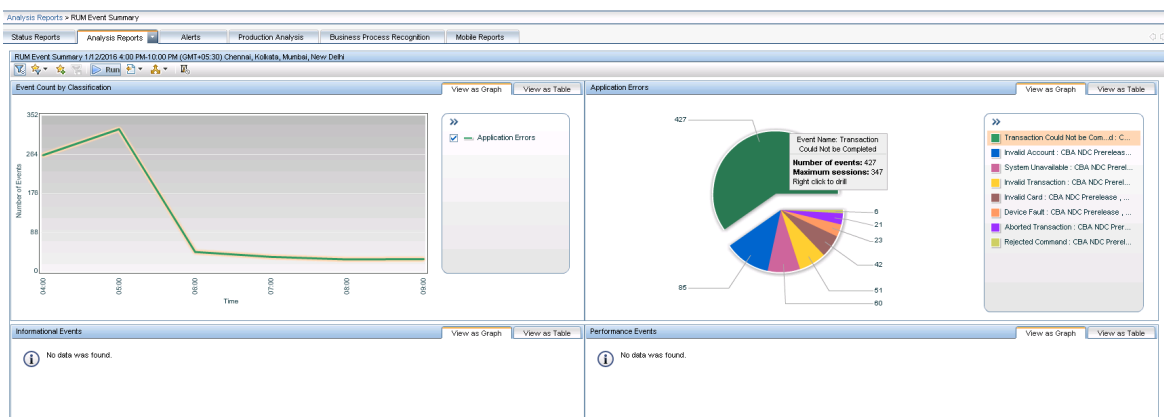
  

Value	Number of Sessions	Error Events	Info Events	Performance Events	Total Actions	Unavailable Actions	Latency (ms)	Total Traffic (KB)
4180..7186	1	2	0	0	2	2	0.00	0.0
4239..5887	1	0	0	0	2	0	0.00	0.0
4239..8703	1	1	0	0	3	1	0.00	0.0
4251..5490	1	0	0	0	1	0	0.00	0.0
4790..2392	1	0	0	0	1	0	0.00	0.0
4890..2195	1	0	0	0	1	0	0.00	0.0
Not Applicable (System Message)	36	0	0	0	42	0	0.00	0.0
<b>Total</b>	<b>42</b>	<b>3</b>	<b>0</b>	<b>0</b>	<b>52</b>	<b>3</b>	<b>0.00</b>	<b>0.0</b>

### RUM Action Summary



### RUM Event Summary

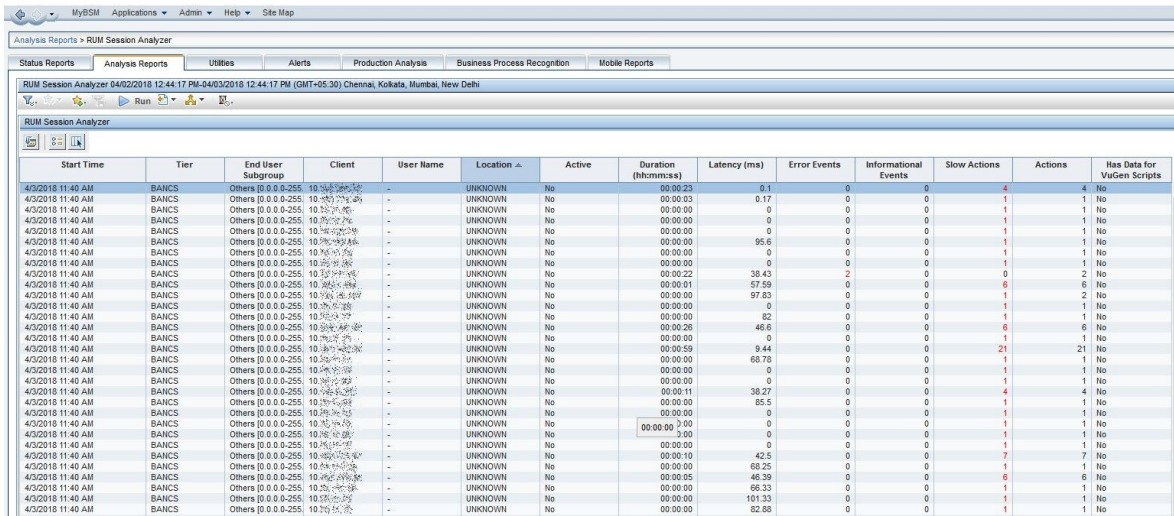


- **Comments:** For detailed information about configuring the NDC protocol, see "[NDC Protocol Configuration](#)" on page 245.
- **ISO 8583**
  - **Versions:** VISA BASE I, MasterCard CIS
  - **APM Template Name:** N/A
  - **Sample Snapshots:** Session Analyzer

Action	Start Time	Application	Events	Total Time (sec.)	Server Time (sec.)	Network Time (sec.)	Client Time (sec.)	Total Traffic (KB)
0302-Card issuer file update Request	12/3/10 06:34:07 PM	iso8583 visa base i	-	0.03	0.00	0.03	0.00	0.0
0800-Network Management Request	12/3/10 06:34:07 PM	iso8583 visa base i	-	0.03	0.00	0.03	0.00	0.0
0302-Card issuer file update Request	12/3/10 06:34:07 PM	iso8583 visa base i	-	0.04	0.00	0.04	0.00	0.0
0302-Card issuer file update Request	12/3/10 06:34:07 PM	iso8583 visa base i	-	0.04	0.00	0.04	0.00	0.0
0800-Network Management Request	12/3/10 06:34:07 PM	iso8583 visa base i	-	0.01	0.00	0.01	0.00	0.0
0302-Card issuer file update Request	12/3/10 06:34:07 PM	iso8583 visa base i	-	0.04	0.00	0.04	0.00	0.0
0100-Authorization Request	12/3/10 06:34:12 PM	iso8583 visa base i	-	0.04	0.00	0.04	0.00	0.0
0100-Authorization Request	12/3/10 06:34:12 PM	iso8583 visa base i	-	0.04	0.00	0.04	0.00	0.0

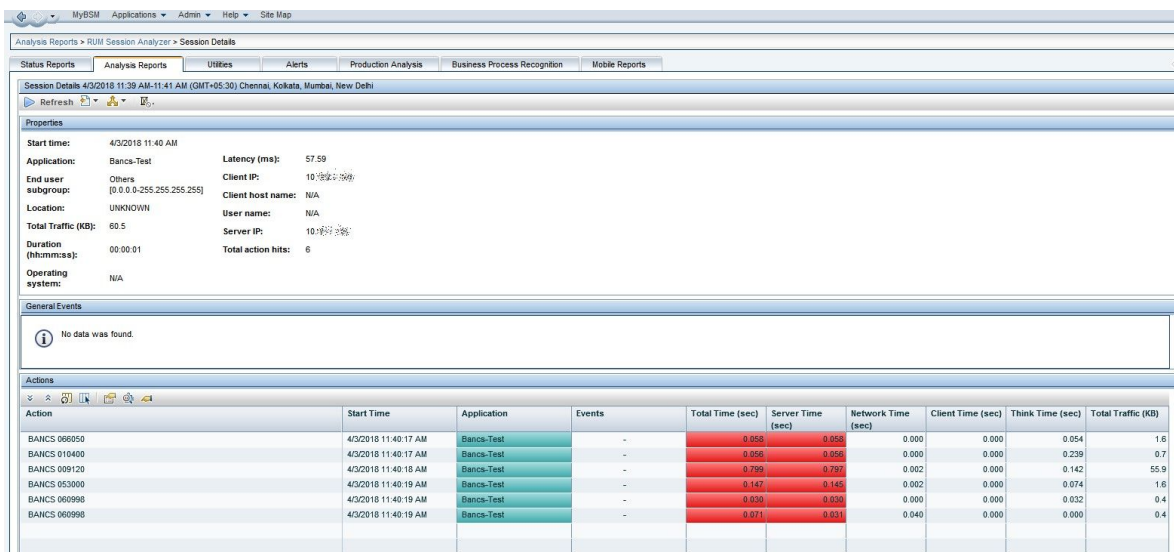
- **TCS BaNCS**
  - **Versions:** Any
  - **APM Template Name:** BaNCS

## Sample Snapshots: Session Analyzer



The screenshot shows the 'Session Analyzer' report interface. At the top, there are navigation tabs: 'Status Reports', 'Analysis Reports', 'Utilities', 'Alerts', 'Production Analysis', 'Business Process Recognition', and 'Mobile Reports'. The current report is titled 'RUM Session Analyzer 04/02/2018 12:44:17 PM-04/03/2018 12:44:17 PM (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi'. Below the title, there is a table with the following columns: Start Time, Tier, End User Subgroup, Client, User Name, Location, Active, Duration (hh:mm:ss), Latency (ms), Error Events, Informational Events, Slow Actions, Actions, and Has Data for VuGen Scripts. The table contains 20 rows of session data, all for the application 'BANCS' and tier 'Others'. The 'Active' column is set to 'No' for all entries. The 'Duration' and 'Latency' columns show various values for each session, such as 00:00:23 with a latency of 0.17 ms, and 00:00:01 with a latency of 57.59 ms.

## Session Details



The screenshot shows the 'Session Details' view for a specific session. The interface includes navigation tabs: 'Status Reports', 'Analysis Reports', 'Utilities', 'Alerts', 'Production Analysis', 'Business Process Recognition', and 'Mobile Reports'. The report title is 'Session Details 4/3/2018 11:39 AM-11:41 AM (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi'. Below the title, there is a 'Properties' section with the following information: Start time: 4/3/2018 11:40 AM, Application: Bancs-Test, Latency (ms): 57.59, End user subgroup: Others, Client IP: 10.26.30.10, Location: UNKNOWN, Total Traffic (KB): 60.5, Duration (hh:mm:ss): 00:00:01, Operating system: NIA, and User name: NIA. Below the properties, there is a 'General Events' section with a message: 'No data was found.' At the bottom, there is an 'Actions' section with a table showing details for various actions. The table has columns: Action, Start Time, Application, Events, Total Time (sec), Server Time (sec), Network Time (sec), Client Time (sec), Think Time (sec), and Total Traffic (KB). The actions listed are all for the application 'BANCS-Test' and occurred between 11:40:17 AM and 11:40:19 AM on 4/3/2018.

**Comments:** TCS BaNCS is a core banking software suite. It includes functionality for universal banking actions, core banking, wealth management, forex, money markets, compliance, the processing of securities, financial inclusion, and other miscellaneous operations. There are also modules that handle capital markets and insurance. For details, see the [TCS BaNCS website](#).



## Session Details

Session Details 4/9/2015 4:51 PM-4:53 PM (GMT+02:00) Jerusalem

**Properties**

Start time:	4/9/2015 4:52 PM	Latency (ms):	0.00
Application:	LDAP	Client IP:	192.168.54.134
End user subgroup:	Others (0.0.0-255.255.255.255)	Client host name:	N/A
Location:	UNKNOWN	User name:	Chk-Taylor, jacob@himmangepart.DIH-GAL-DC-R
Total Traffic (KB):	8.7	Server IP:	12.185.86.63
Duration (hh:mm:ss):	00:00:00	Total action hits:	5
Operating system:	N/A		

**General Events**

No data was found.

**Actions**

Action	Start Time	Application	Events	Total Time (sec)	Server Time (sec)	Network Time (sec)	Client Time (sec)	Think Time (sec)	Total Traffic (KB)
bind_req_d=1 version=3 username=Mercury-auth=smtp_auth	4/9/2015 04:52:39 PM	LDAP	-	0.000	0.000	0.000	0.000	0.000	0.1
search_req_d=2 baseObject=D._name equalityMatch Taylor(1)	4/9/2015 04:52:39 PM	LDAP	-	0.000	0.000	0.000	0.000	0.000	8.4
bind_req_d=3 version=3 user_RUC-DC=NET-auth=smtp_auth	4/9/2015 04:52:39 PM	LDAP	-	0.000	0.000	0.000	0.000	0.000	0.1
search_req_d=4 baseObject=C._uid (present objectClass)	4/9/2015 04:52:39 PM	LDAP	-	0.000	0.000	0.000	0.000	0.000	8.2
unbind_req_d=5	4/9/2015 04:52:39 PM	LDAP	-	0.000	0.000	0.000	0.000	0.000	0.0

- **SHVA**
  - **Versions:** Based on spec by CAL
  - **APM Template Name:** <private>
  - **Sample Snapshots:** N/A
  - **Comments:** Based on the spec provided by customer: CAL

- **AMF**
  - **Versions:** AMF0, AMF3
  - **APM Template Name:** Flash
  - **Sample Snapshots:**
    - Session Analyzer

There are 24 actions in the session with 24 frame units, of which 24 units are for the selected application.

Action	Start Time	Application	Events	Total Time (sec)	Server Time (sec)	Network Time (sec)	Client Time (sec)	Think Time (sec)	Total Traffic (KB)
http://valletta_oid.devlab.a...choAMFEchoAMF.EchoAny[...]	10/12/11 10:46:03 AM	Flex_for_Yan	-	0.37	0.20	0.16	0.16	0.00	0.00
http://valletta_oid.devlab.a...EchoAny[...]&amp;=sss]	10/12/11 10:46:05 AM	Flex_for_Yan	TPE	0.31	0.17	0.14	0.14	0.00	0.00
http://valletta_oid.devlab.a...hoAny[11965-03-09 16:59:59])	10/12/11 10:46:07 AM	Flex_for_Yan	-	0.39	0.20	0.19	0.19	0.00	0.00
http://valletta_oid.devlab.a...AMFEchoAMFEchoAMF.EchoAny[<?xml version='1.0' encoding='utf-8'><requestEchoAMF EchoAMF EchoAny[<?xml date='4/22/21/2002'><name='11'><email='22'><email-date='4/21/2002'><date='4/21/2002'><comment='333333333...']	10/12/11 10:46:12 AM	Flex_for_Yan	TPE	0.45	0.31	0.14	0.14	0.00	0.00
http://valletta_oid.devlab.a...:assembler, prefers: C+]]]]]	10/12/11 10:46:12 AM	Flex_for_Yan	TPE	0.39	0.21	0.18	0.18	0.00	0.00
http://valletta_oid.devlab.a...:Object(prefs: VB NET]]]]]	10/12/11 10:46:14 AM	Flex_for_Yan	TPE	0.35	0.16	0.20	0.20	0.00	0.00

- Action Summary

RUM Action Summary 04/09/2015 11:40:20 AM-04/09/2015 11:40:20 AM (GMT+02:00) Jerusalem

Action	Tier	Type	Total Action Hits	Availability (%)	Total Time (sec)	Server Time (sec)	Requests per Action Hit	Total Traffic (KB)
chrf_req	AMF	Page	26	100.00	0.27	0.07	1.00	1.3
ProbaAMF_echoTest()&=Server:Processing	AMF	Page	25	100.00	0.26	0.06	1.00	0.9
ProbaAMF_echoTest()	AMF	Page	26	100.00	0.21	0.01	1.00	1.2
ProbaAMF_sendComplexObject()	AMF	Page	25	100.00	0.26	0.06	1.00	1.8
ProbaAMF_sendSimpleText()	AMF	Page	25	100.00	0.21	0.00	1.00	1.2
ProbaAMF_getComplexObject()	AMF	Page	25	100.00	0.27	0.07	1.00	1.8
			132	83.33	0.23	0.04	1.00	1.4

Legend: Critical (red), OK (green), Minor (yellow), No data (blue), Downtime (dark blue), Unknown (grey)

- **Comments:** Flash is a client side technology. It can be used for many different things, from playing movies to creating a completely client side application that may never access the server. Flex is a specific framework for developing applications over Flash. A part of the Flex framework is using the AMF protocol which is an Adobe protocol for communication between a Flash client and server. AMF in



Flex usually runs over HTTP. Monitoring AMF protocol allows RUM to report remote method invocations and their parameters. RUM supports versions AMF0 and AMF3.

- **UDP**
  - **Versions:** N/A
  - **APM Template Name:** Generic UDP

## Application Suites

### Oracle E-Business

- **Siebel (CRM):** HTTP-based. When defining an application in APM, use one of the Siebel X.X types.
- **PeopleSoft:** Regular HTTP-Web application
- **Oracle Database:** There are two types of protocols used for Oracle DB: OCI and Thin Client (JDBC). Only Thin Client (JDBC) is currently supported (see "[Databases](#)" on page 218).
- **Oracle Forms:** Can be implemented as a regular HTTP-Web application, or using Oracle NCA client (runs integrated in the Web browser). Oracle NCA client may communicate with the server over HTTP or raw TCP sockets. For each type of communication, RUM provides a separate application template: Oracle Forms over HTTP or Oracle Forms over TCP.

These protocol types may be combined in a single RUM application as different tiers.

### Citrix Solutions

- **XenApp (successor of MetaFrame):** A user connects to XenApp using a special Citrix Client, and runs certain applications on the server, while getting the look-and-feel of the local application. Uses Citrix ICA protocol for communication.
- **XenDesktop:** Similar to XenApp, only that whole desktop is virtualized.
- **Citrix Portal:** A Web interface which provides access to XenApp applications. You have to select the **Citrix HTTP** application template when monitoring a Citrix portal.
- **XenServer:** Server virtualization, each virtual server runs it's own Operatins System.

With RUM you can monitor XenApp and XenDesktop from two angles:

- **Monitoring Citrix ICA protocol:** You can have all TCP-level measurements (including network quality parameters) for each user session via the Session Summary report, which shows the breakdown of the data by username or/and application which runs on Citrix Server;
- **Monitoring outgoing traffic:** When RUM monitors an HTTP-Web application which is accessed by users via XenAll or XenDesktop, this virtualization layer hides the real client's properties (IP address, username). These parameters may be recovered if the RUM HTTP Agent is installed on the Citrix Server.

### View Data for Citrix Sessions

In the RUM Session Analyzer report, you can view the number of sessions configured for Citrix-based apps. RUM identifies the apps that were started by a user and collects the metrics for the user session on that app. This information is shown in the Session Summary and Session Analyzer reports. However, specific information about the user's interaction with that particular app, is not visible to RUM.

The following image shows a Session Analyzer report for the Citrix ICA application:

Start Time	Tier	End User Subgroup	Client	User Name	Location	Active	Duration (hh:mm:ss)	Latency (ms)	Error Events	Informational Events	Slow Actions	Actions	Rise Data for Values Sample
4/18/2018 1:12 PM	ICA	Others [0.0.0.0-255.255.255.255]		devlab/Calcut1		Yes	00:00:25	0.54	-	-	-	-	No
4/18/2018 1:12 PM	ICA	Others [0.0.0.0-255.255.255.255]		Wl_spu09-09bvm		Yes	00:00:48	26.14	-	-	-	-	No
4/18/2018 1:11 PM	ICA	Others [0.0.0.0-255.255.255.255]		devlab/Calcut1		Yes	00:01:30	43.39	-	-	-	-	No
4/18/2018 1:10 PM	ICA	Others [0.0.0.0-255.255.255.255]		devlab/Calcut1		Yes	00:02:37	13.4	-	-	-	-	No
4/18/2018 1:10 PM	ICA	Others [0.0.0.0-255.255.255.255]		Wl_spu09-09bvm		Yes	00:02:51	24.11	-	-	-	-	No
4/18/2018 1:09 PM	ICA	Others [0.0.0.0-255.255.255.255]		devlab/Calcut1		Yes	00:03:28	32.03	-	-	-	-	No

When you click on a session in order to view its details, the report shows additional information for the published app, as shown below.

Refresh [Icons]

**Properties**

Start time:	4/18/2018 1:12 PM	Latency (ms):	14.98
Application:	Demo-Citrix_ICA	Client IP:	[Redacted]
End user subgroup:	Others [0.0.0.0-255.255.255.255]	Client host name:	N/A
Location:	[Redacted]	User name:	devlab/Calcut1
Total Traffic (KB):	762.6	Server IP:	[Redacted]
Duration (hh:mm:ss):	00:25:13	Published Application:	Calc
Operating system:	N/A		

The RUM Session Summary report shows the number of session for a specific user, and the number of times the user has accessed the app. The image below shows that the **Calc** application has been accessed 24 times.

RUM Session Summary 04/18/2018 01:11:00 PM-04/21/2018 01:13:00 PM (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi

Session Groups

Value	Number of Sessions	Number of Subgroups	Error Events	Info Events	Latency (ms)	Total Traffic (KB)
Wl_spu09-09bvmCDV7	9	2	0	0	23.45	2,145.2
devlab/Calcut1	24	1	0	0	12.44	4,919.8
3	33		0	0	14.53	7,063.1

Detailed Subgroups

Value	Number of Sessions	Error Events	Info Events	Latency (ms)	Total Traffic (KB)
Calc	24	0	0	12.44	4,919.8
3	34	0	0	12.44	4,919.8

## Extending Protocol Coverage

RUM ships with an SDK which allows you to add support for new protocols to RUM. For some application types, the support can be easily added; for some it requires more work. If you encounter a customer's request for an unsupported protocol/application, we recommend that you contact Product Marketing or R&D for assistance.

# Chapter 18: Customizing Error Codes for SAPGUI

Error capturing is based on matching status messages against a template list. Out-of-the-box, RUM is configured to match only some of the SAPGUI error messages. You can add additional error messages (predefined or custom) to the list for matching.

To add additional error messages, on the RUM Probe machine edit the `<RUMProbe>/etc/rum_probe/protocols/sapgui.def` file and under the `[sapgui_custom]` section add a line for each error code in the following format:

```
status_code <CODE> <MESSAGE_REGEX>
```

For example, the line **status\_code 1 Function module \w\* does not exist** means that an action is reported as having a status code of 1 if it results in a status message that matches the regular expression 'Function module \w\* does not exist'.

APM uses the SAPGUI status codes to create predefined events for applications configured with the SAPGUI template. By default, only error codes 1 (Object not found) and 2 (Invalid function) are predefined in APM and are both included in an event called **SAPGUI error**. To add additional predefined events for SAPGUI applications using other codes, on the APM Gateway Server edit the `<APM root>\conf\rum_templates\SapGui.xml` file and under the `<events>` tag, create a new, single event in the following format:

```
<event>
  <active>true</active>
  <snapshot>true</snapshot>
  <name>Unique event name</name>
  <report_as_error>true</report_as_error>
  <category>error</category>
  <collect_session_snapshot>>false</collect_session_snapshot>
  <scope>GLOBAL</scope>
  <type>0</type>
  <error_codes>
    <code>Unique error code number</code>
  </error_codes>
  <actions/>
</event>
```

**Note:** The event name and the error code number must be unique within the template. That is, they cannot be used in any other event configured in the template.

## Example

To report actions that contain an 'Invalid key specified' message:

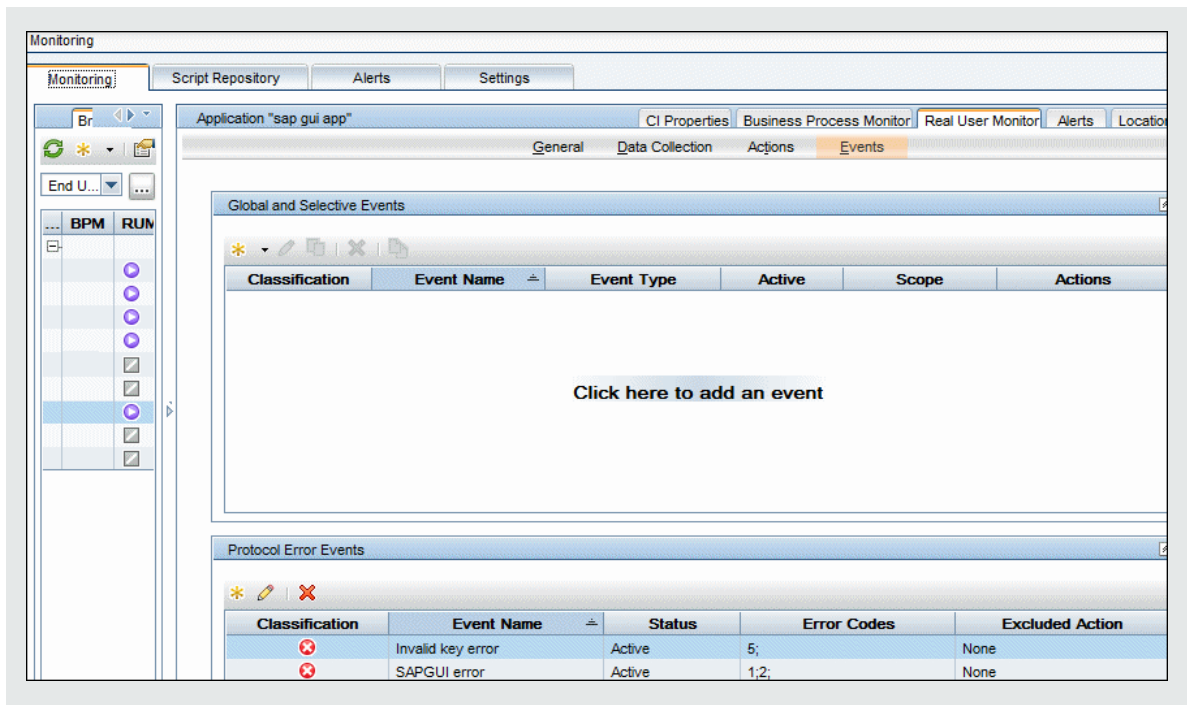
1. On the RUM Probe machine, add the following line under the `[sapgui_custom]` section in the `<RUMProbe>/etc/rum_probe/protocols/sapgui.def` file:

```
status_code 5 Invalid key specified
```

2. On the APM Gateway Server, add the following event to the SAPGUI template (<APM root>\conf\rum\_templates\SapGui.xml):

```
<event>
  <active>true</active>
  <snapshot>true</snapshot>
  <name>Invalid key error</name>
  <report_as_error>true</report_as_error>
  <category>error</category>
  <collect_session_snapshot>false</collect_session_snapshot>
  <scope>GLOBAL</scope>
  <type>0</type>
  <error_codes>
    <code>5</code>
  </error_codes>
  <actions/>
</event>
```

3. In APM, an 'Invalid key error' event is added as a default Protocol Error Event for applications configured with the SAPGUI template:



# Chapter 19: NDC Protocol Configuration

The following provides the information required to configure the NDC protocol parser. To access the NDC template, contact customer support.

The NDC configuration files come with a sample configuration. Replace the **NdcOperationInfo.csv** and **NdcTerminalInfo.csv** files with your deployment configuration so the reports display the correct data. **Ndc.def** may also need to be modified.

The NDC configuration files can be found at: **/etc/rum\_probe/protocols/**

## NdcOperationInfo.csv

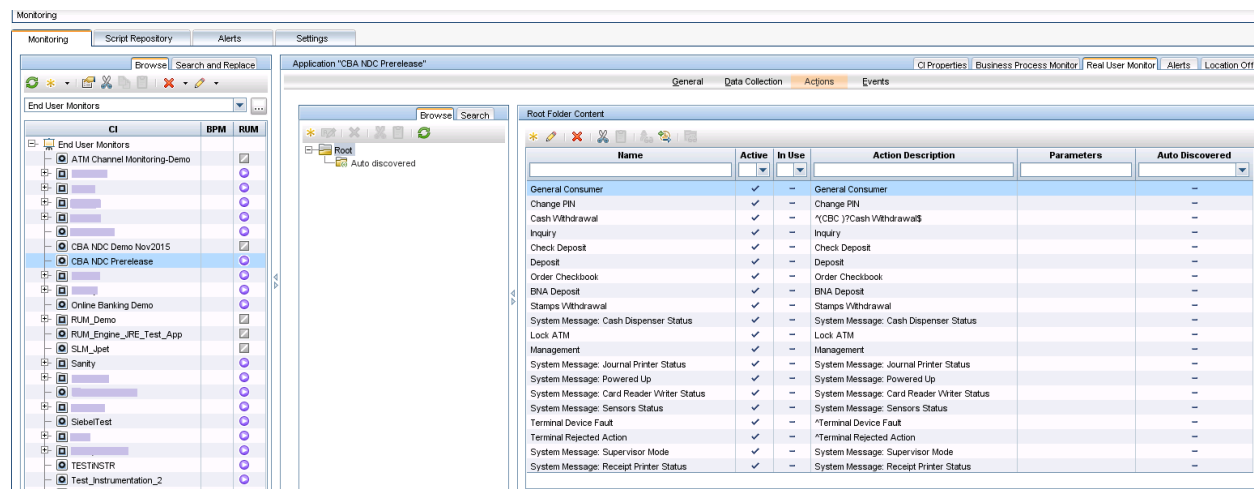
The end user of the ATM presses function keys at an ATM to perform an operation such as Cash Withdrawal. The **NdcOperationInfo.csv** file provides a mapping from the end user key sequence to the operation.

The following is an example line in this file:

```
"Profile 1", "ABCDEFGF", "Cash Withdrawal"
```

Each line in this file contains comma separated values for the Profile name, Operation code, and the Operation. Each ATM may have different hardware and software running on it. This information is categorized by the ATM profiles. Each ATM has a unique profile associated with it. The Operation code is a sequence of keys pressed at the ATM. By pressing an OperationCode key sequence the end user is able to perform an operation.

If you update, add, or remove Actions from the sample configuration file, you need to correspondingly update the defined Actions. You can update the defined Action in the APM UI by clicking **Admin > End User Management**. Select the NDC application in the left pane, and update the Actions tab in the right pane.



Name	Active	In Use	Action Description	Parameters	Auto Discovered
General Consumer	✓	–	General Consumer		–
Change PIN	✓	–	Change PIN		–
Cash Withdrawal	✓	–	*(CBC ?)Cash Withdrawal		–
Inquiry	✓	–	Inquiry		–
Check Deposit	✓	–	Check Deposit		–
Deposit	✓	–	Deposit		–
Order Checkbook	✓	–	Order Checkbook		–
BNM Deposit	✓	–	BNM Deposit		–
Stamps Withdrawal	✓	–	Stamps Withdrawal		–
System Message: Cash Dispenser Status	✓	–	System Message: Cash Dispenser Status		–
Lock ATM	✓	–	Lock ATM		–
Management	✓	–	Management		–
System Message: Journal Printer Status	✓	–	System Message: Journal Printer Status		–
System Message: Powered Up	✓	–	System Message: Powered Up		–
System Message: Card Reader Writer Status	✓	–	System Message: Card Reader Writer Status		–
System Message: Sensors Status	✓	–	System Message: Sensors Status		–
Terminal Device Fault	✓	–	*Terminal Device Fault		–
Terminal Rejected Action	✓	–	*Terminal Rejected Action		–
System Message: Supervisor Mode	✓	–	System Message: Supervisor Mode		–
System Message: Receipt Printer Status	✓	–	System Message: Receipt Printer Status		–

## NdcTerminalInfo.csv

To provide the mapping from the **NdcOperationInfo.csv** file, you need to know the ATM profile. The RUM Probe only sees the data coming from the ATM, so it is only aware of the IP address of the ATM. The

**NdcTerminalInfo.csv** file helps determine the ATM profile and the ATM user friendly name based on the ATM IP address.

The following is an example line in this file. Each terminal, characterized by the user friendly terminal name, has a unique profile.

```
192.168.1.2,Terminal1,"Profile1"
```

Each line in the file contains comma separated values for the ATM IP address, ATM user friendly name, and ATM profile.

## ndc.def

The `ndc_custom` section of the **ndc.def** file provides additional configuration options for the NDC protocol parser.

The NDC Server response to ATM requests contains a clear text part. It is possible to match regular expressions in this clear text to set status codes. In the Events tab of the APM Admin UI for the NDC application you can map these status codes to informational, warning, or error events.

The following is an example line in this file:

```
status_code 1 TRANSACTION ABORTED
```

TRANSACTION ABORTED is the string that is searched in the clear text response in the server. If the string is found, a `status_code` of 1 is set on the Action. In the APM UI for this protocol, this code was mapped to signal an error, so an error event is triggered when this occurs.

It is also possible to extract text in a server response matching a regular expression pattern and display that field in the Action details page for that Action. For example, some transactions might contain **Ledger** followed by the ledger balance amount followed by either KES or TZS as the currency.

This following example matches this pattern. When it is found, the Action Details report for that Action will contain the field `LedgerBalance` with its value and currency.

```
pattern LedgerBalance.*LEDGER.*([K|T][E|Z]S.*)
```

# Chapter 19: RUM Probe Textual Protocol Configuration

The RUM Probe supports textual protocols like FTP, SSDB, IMAP, POP3, SMTP, and TCS BaNCS. It uses an inline generic protocol parser that parses textual "Shell Like" protocols.

For textual protocols, the client request packets are in the form of "commands" and the server response packets are in the form of "feedback".

## Textual Protocol Parser Configuration

A typical request will be in the following form:

```
[optional-prefix] command-keyword [optional-parameters]
```

The textual protocol parser is configured according to a configuration file. This enables the addition of a new textual parser for a given probe, without the need to compile the probe again.

You edit the protocol definition in the configuration files (*/etc/rum\_probe/protocols*).

### Example: SSDB textual protocol:

There is no action descriptor with TCP applications, so actions are given the default name **SSDB Command**, as shown in the report picture below. The name can be configured in the **ssdb.conf** file on the probe machine (*/etc/rum\_probe/protocols*):

```

1 [command SomeCommand]
2 template                .*
3 title                   SSDB command
4 response                display-raw
5 response-summary       display-raw
6
7 [global]
8 protocol-title         SSDB
9 unrecognized-command  ignore
10 max-buff-size         2048
11 default-tag           ssdb-raw
12 command-parameter-key param
13
    
```

The default name is given for every action, but the field can be configured to extract something dynamically from the action content (using regex), and to use it as the action name in the report.

Below are some example SSDB commands included in **ssdb.conf**.

#### [command ATH]

template	<code>^(.?(AT[\d]{2})(ISO[\w]{10})([\d]{3})(B23[\w]{29})([\d]{6})(.)*\$</code>
title	<code>{{Title1}} {{Canal}} {{ISO}} {{Bitmap}} {{Title2}}</code>
parameter	Canal display template \$2
parameter	ISO display template \$3
parameter	Title1 display template \$4
parameter	Bitmap display template \$5
parameter	Title2 display template \$6
response	display-raw
response-summary	display-raw

### [command RDBN]

template	^(.?(RDBN)(ISO[\w]{10})([\d]{3})(B23[\w]{29})([\d]{6})(.*)\$
title	{{Title1}} {{Canal}} {{ISO}} {{Bitmap}} {{Title2}}
parameter	Canal display template \$2
parameter	ISO display template \$3
parameter	Title1 display template \$4
parameter	Bitmap display template \$5
parameter	Title2 display template \$6
response	display-raw
response-summary	display-raw

## Chapter 19: Diebold ATM Protocol Configuration

Diebold is a widely used protocol used between ATM terminals and the ATM Switch. With Diebold ATM protocol support in RUM, an application owner can monitor and isolate the cause of performance and availability issues for Diebold applications using RUM.

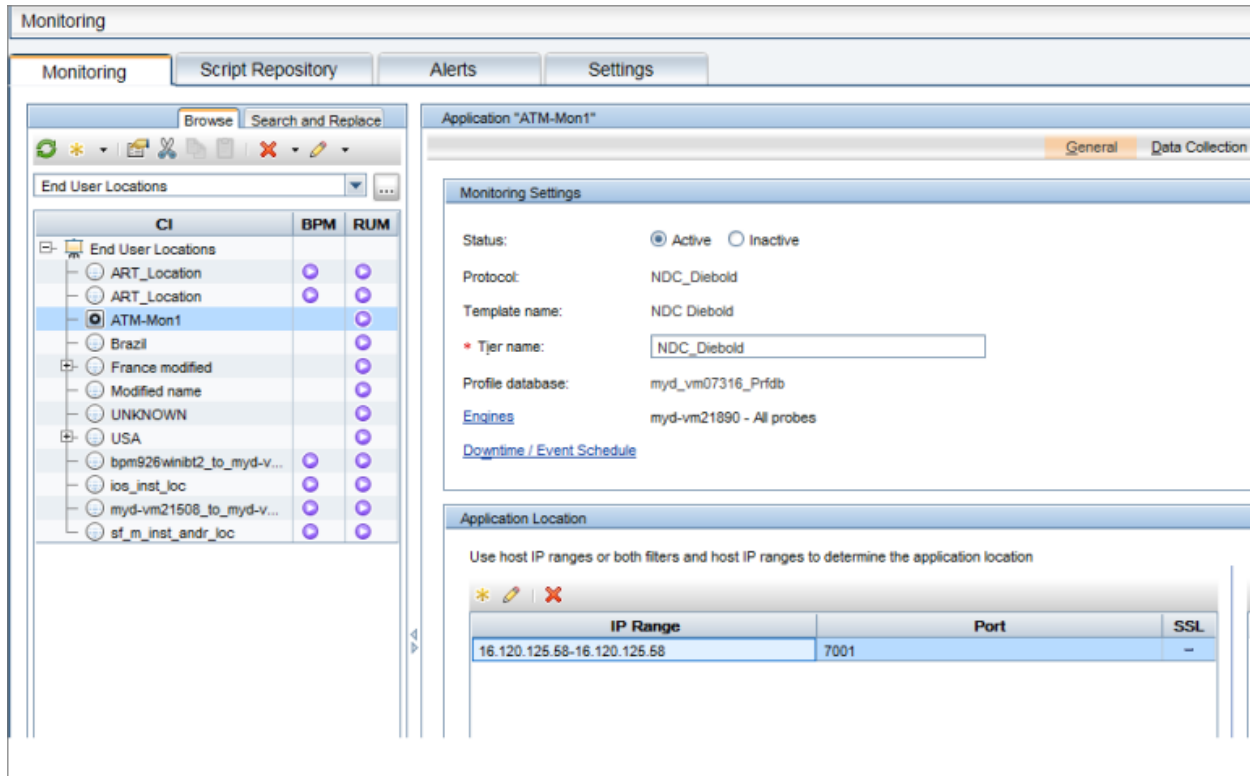
RUM supports three types of customer deployments, where the ATM server supports:

- Diebold ATM protocol only
- Both NDC and Diebold ATM protocols. In this case, the same End User Monitoring (EUM) Application can be used to monitor both protocols.
- NDC ATM protocol only

This can be achieved by setting the protocol definition in the **ndc.def** file as described below.

The template to use while configuring the application in the EUM is **NDC\_Diebold**.





Parsing the Diebold ATM main transactions is currently supported using the RUM sniffer probe monitoring. As ATM implementations are often customized, you may encounter some limited monitoring capability. The current release of RUM provides Beta support for parsing the Diebold ATM protocol. **Note:** Parsing of maintenance messages is currently not supported.

This chapter provides the information required to configure the Diebold's ATM protocol parser.

## NdcOperationInfo.csv

A detailed description of the purpose and contents of this file can be found in "[NDC Protocol Configuration](#)" on [page 245](#). Configuration for Diebold operations needs to be done similarly to the NDC operation as shown in the following example:

```
"DieboldProfile1", "ABCEDFGH", "Cash Withdrawal"
```

Adding the prefix "Diebold" before the Diebold profile can help distinguish between NDC and Diebold actions if both protocols are being monitored by the same application.

## NdcTerminalInfo.csv

Ensure that the Diebold profiles defined in **NdcTerminalInfo.csv** and **NdcOperationInfo.csv** use the same profile name. For details, see "[NDC Protocol Configuration](#)" on [page 245](#).

## ndc.def

The protocol definition file needs to be updated to configure the deployment scenario.

**is\_diebold:** A boolean flag indicating whether Diebold-specific processing needs to be enabled for this application. “true” enables the processing and “false” disables it.

**is\_diebold\_only:** A boolean flag indicating if the application has Diebold only. Setting the value “true” disables NDC-specific processing for this application.

The default value for both these flags is “false”. For example if you want to configure an application used to monitor Diebold data and is not expected to monitor NDC data, you can add the following lines in the **ndc.def** file.

```
is_diebold true  
is_diebold_only true
```

# Chapter 20: Monitoring Citrix with RUM

You can use RUM's VDI agent to monitor Citrix traffic.

This chapter includes the following topics:

- ["Overview of Citrix Monitoring with RUM" below](#)
- ["Overview of the RUM VDI Agent" on the next page](#)
- ["Configurations for Working with the RUM VDI Agent for HTTP Traffic" on page 253](#)
- ["Advanced Configuration for HTTP Traffic" on page 255](#)
- ["Using the RUM VDI Agent with Terminal Services for HTTP Traffic" on page 257](#)

## Overview of Citrix Monitoring with RUM

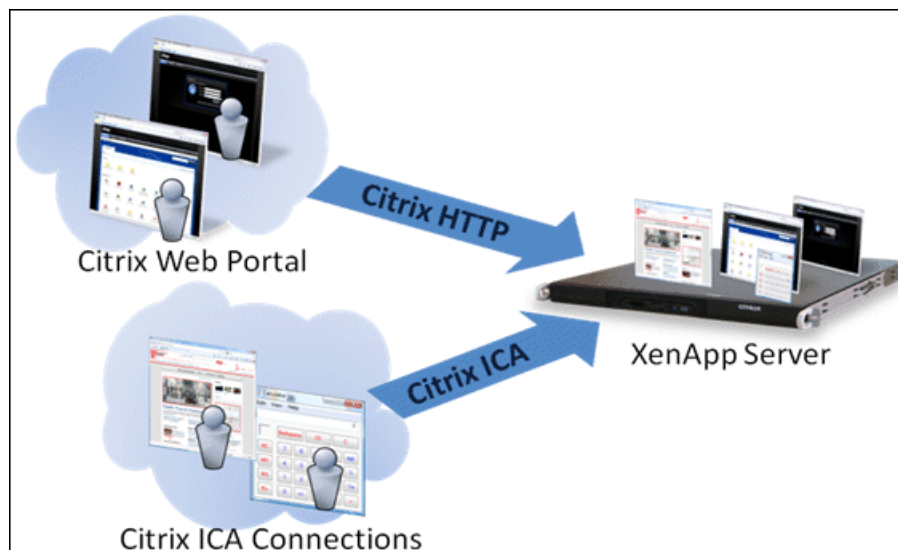
End users can connect to a Citrix XenApp server via a web portal or a direct ICA connection. When multiple users connect to the same XenApp server, requests sent from the XenApp server all originate from the same client, regardless of the originating end user.

This section includes:

- ["Monitoring Traffic Between End Users and a XenApp Server" below](#)
- ["Monitoring Outgoing Traffic from a XenApp Server" on the next page](#)

### Monitoring Traffic Between End Users and a XenApp Server

The following diagram shows typical traffic between end users and a Citrix XenApp server:



An end user starts by opening a Citrix web portal and selecting one of the published applications. An ICA session is created, in which the selected application runs on the XenApp server, and the user uses the application remotely.

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

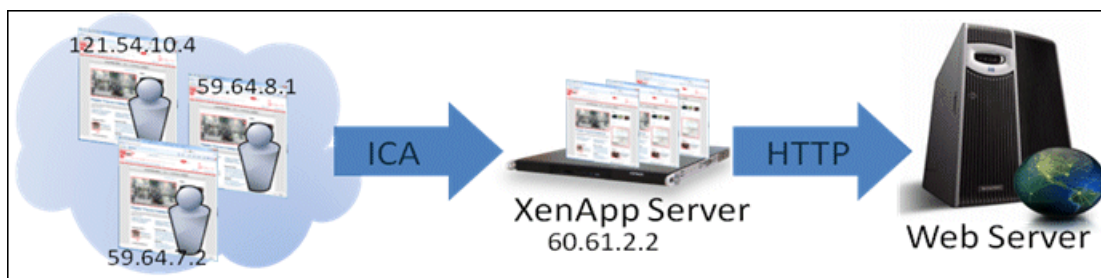
To monitor this traffic with RUM 9.x or later, no agent installation is required. You simply configure the following applications in APM, using specific templates:

- The XenApp application, using the **Citrix ICA** template.
- The Login application, using the **Citrix Http** template.

For user interface details on creating RUM applications in APM, see "RUM Application Configuration Wizard" in the APM Application Administration Guide.

## Monitoring Outgoing Traffic from a XenApp Server

The following diagram shows multiple users connected to the same XenApp server, each running an instance of the Internet Explorer browser to connect to a web server. In this scenario, all connections opened to the web server originate from the same client, which is the XenApp server.



To monitor this, you must define the web application (web servers) using the **General Web Application** template.

When monitoring this scenario with RUM, it is desirable to see the real end users as the clients, rather than having a single client combining all the traffic. To achieve such functionality, you must install the RUM VDI Agent on the XenApp server.

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

Request URL	Without RUM VDI Agent		With RUM VDI Agent	
	Client IP	User Name	Client IP	User Name
/index.html	60.61.2.2	-	121.54.10.4	John
/index.html	60.61.2.2	-	59.64.8.1	Rosetta
/search?q=agent	60.61.2.2	-	121.54.10.4	John
/checkout.jsp	60.61.2.2	-	59.64.8.1	Rosetta
/index.html	60.61.2.2	-	59.64.7.2	Steve
/view?item=agent	60.61.2.2	-	121.54.10.5	Peter

## Overview of the RUM VDI Agent

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

This section includes:

- ["Supported Browsers for HTTP Traffic" below](#)
- ["How the RUM VDI Agent Works for HTTP Protocol" below](#)

## Supported Browsers for HTTP Traffic

For details on the supported browsers and ActiveX components, see the *RUM VDI Agent Requirements* in the Real User Monitor Installation and Upgrade Guide.

## How the RUM VDI Agent Works for HTTP Protocol

The RUM VDI Agent tags outgoing HTTP traffic with the IP address and user name of the real end user (connected to the XenApp server). This information is added to the preconfigured HTTP header.

The new configuration mode (which is the default mode) adds the following HTTP headers:

- RUM\_USER\_NAME
- RUM\_CLIENT\_ADDRESS

In compatibility mode, the information is added to the **UserAgent HTTP** header

For more information see ["Advanced Configuration for HTTP Traffic" on page 255](#).

**Note:** Tagging the user agent HTTP header may slow down the browser. However, you can assume that the browser and website are on the same network (or at least geographically near each other), so any slow down is not significant.

# Configurations for Working with the RUM VDI Agent for HTTP Traffic

You must configure user name detection in the applications you want monitored using the RUM VDI Agent. Additionally, you can configure RUM to use the IP of the real user connected to a XenApp server as the client IP in the web application.

This section includes:

- ["To configure user name detection in applications" below](#)
- ["To configure Real User Monitor to use the IP of the real user connected to a XenApp server as the client IP in the web application" on the next page](#)

## To configure user name detection in applications

1. In End User Management Administration in APM, configure a new application or edit an existing application.
2. Select **Real User Monitor > General** and in the **Real User Monitor Application General** page, expand the **User Name Detection** area.
3. Click the **New User Name Detection** button. The **User Name Detection** dialog box opens in a new window.

4. In the **User Name Detection** dialog box, configure the following:

- In compatibility mode:

Field	Value
Search in	HTTP Header
Header name	User-Agent
<b>Extract text:</b>	
Between	RUM_USER_NAME=
and	;

- In the new configuration mode:

Field	Value
Search in	HTTP Header
Header name	RUM_USER_NAME
Content	All content

5. Click **OK** to save the configuration changes.

**Note:** The web application may require users to log on when opening the application in the web browser. In such cases, you should decide whether you prefer configuring the user name for the web application as the Citrix user name, or as the web application's user name. In either case, you may consider configuring the other user name (Citrix or web application) as a Session Property.

## To configure Real User Monitor to use the IP of the real user connected to a XenApp server as the client IP in the web application

1. On the RUM Engine, edit the file:

```
<RUM>\conf\configurationmanager\Beatbox_Default_Const_Configuration.xml
```

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

- In compatibility mode, add:

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

- In the new configuration mode, add:

```
forwarded_for_header RUM_CLIENT_ADDRESS IPV4\\*([^;]*)$.* $1
```

3. Save the file.

4. In the RUM Engine web console, synchronize configuration data by selecting **Tools > Monitoring Configuration Information > Sync All Configuration**. For details, see "[Monitoring Configuration Information](#)" on page 123.

## Advanced Configuration for HTTP Traffic

You configure advanced settings by editing the **<All users Application Data path>\Micro Focus\RumHttpAgent\settings\RumHttpAgent.cfg** file on the Citrix XenApp server on which the RUM VDI Agent is installed.

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

### To set the configuration mode for VDI Agent

The following files appear in the settings directory:

- RumHttpAgent.cfg
- RumHttpAgent.cfg.update

By default, VDI Agent works in the new configuration mode using **RumHttpAgent.cfg**. In the new configuration mode, new headers are created and the UserAgent header is not used.

To work in compatibility mode (in which information is added to the User-Agent field), rename the **RumHttpAgent.cfg.update** file to **RumHttpAgent.cfg**.

### To disable the RUM VDI Agent

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

To disable the RUM VDI Agent for a specific browser type

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

### To filter and rename header fields (for example, User Agent)

To avoid the following limitation, we recommended you work in the new configuration mode.

However, if you do decide to work in compatibility mode, be aware that some versions of ASP.NET limit the length of the User-Agent HTTP header to 256 byte (see <http://support.microsoft.com/kb/974762/en-us>). If the User-Agent HTTP header exceeds this threshold, the web browser is not able to browse through the web pages. Although Microsoft released a patch for this issue, not all environments worldwide have been updated.

The current implementation of the RUM VDI Agent cannot control the entire User-Agent HTTP header. The RUM VDI Agent tells the browser to include a substring like `RUM_USER_NAME=<john_smith>;RUM_DOMAIN_NAME=<company_domain>;RUM_CLIENT_ADDRESS=IPV4*<11.22.33.44>; RUM_CLIENT_NAME=<JOHN-WORK-NOTEBOOK>` in the header. This substring may exceed the 256 character limit.

Starting from version 9.23, you can configure which fields RUM VDI Agent will publish and, optionally, you can configure these fields to be renamed with a shorter alias.

To achieve this goal, **<ProgramData>\Micro Focus\RumHttpAgent\settings\RumHttpAgent.cfg** has a new parameter **allowedFieldList** under the **[Common]** section:

```
# With the aim to reduce the User-Agent header, you can specify only some of the fields
```

```
# If you want to use all of the field:
# allowedFieldList=RUM_USER_NAME,RUM_CLIENT_ADDRESS,RUM_CLIENT_NAME,RUM_DOMAIN_NAME
# Optionally, you can specify an alias for those fields, use (shorter_name) syntax:
# allowedFieldList=RUM_USER_NAME(RUNAME), RUM_CLIENT_ADDRESS(RCADDR), RUM_CLIENT_
NAME(RCLIENT)
# By default, we do not publish RUM_DOMAIN_NAME

allowedFieldList=RUM_USER_NAME, RUM_CLIENT_ADDRESS, RUM_CLIENT_NAME
```

As one can see, by default, RUM\_DOMAIN\_NAME is not published anymore, as the field is not used in either User Name Detection or Real User IP detection. RUM\_CLIENT\_NAME also could be eliminated from the list, since User Name Detection is configured solely by RUM\_USER\_NAME (see *To configure Real User Monitor to use the IP of the real user connected to a XenApp server as the client IP in the web application in "Configurations for Working with the RUM VDI Agent for HTTP Traffic" on page 253.*

Using field aliases, you can save some more space in the User-Agent header. For example, if you enter:

```
allowedFieldList=RUM_USER_NAME(RUNAME), RUM_CLIENT_ADDRESS(RCADDR)
```

the following appears in the User-Agent header:

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C;
.NET4.0E; RUNAME=<john_smith>;RCADDR=IPV4*<11.22.33.44>)
```

Renaming the fields affects the User Name detection and Real User IP detection. Therefore, you need to edit the contents of the 'Between' field in the User Name Detection dialog box, and the forwarded\_for\_header variable. In our example :

1. In the User Name Detection dialog box, configure the following:

Field	Value
Search in	HTTP Header
Header name	User-Agent
Extract Text	
Between	RUNAME=
and	;

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

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

## To turn on logging

In the [common] section of the file, change the enableLog parameter value to true.



Log files are located in the <COMMONAPPDATA>\Micro Focus\RumHttpAgent\logs directory, where <COMMONAPPDATA> is the file system directory that contains application data for all users. (This directory differs between operating systems. For example, in Windows 7 it is C:\ProgramData, and for Windows XP it is C:\Documents and Settings\All Users\Application Data.)

## Using the RUM VDI Agent with Terminal Services for HTTP Traffic

The RUM VDI Agent can be used with Terminal Sessions in a similar way as with Citrix. If an end user is browsing a web application via a Remote Desktop connection, the RUM VDI Agent can be used to extract the real client's IP address and user name when monitoring the web traffic with RUM.

# Chapter 21: Supporting ISO8583 Based Protocols

ISO8583 is the standard for building financial communication protocols. However, this standard does not cover all aspects of a particular implementation. Some things (such as optional headers and field definitions) need to be defined according to your implementation.

RUM provides ISO8583 core support as well as two implementations (MasterCard and Visa) which are supported out of the box. RUM also has a mechanism to adapt the custom flavor of the protocol.

**Note:** There are different implementations of Visa/MasterCard protocol. Only part of them are supported by RUM. In order to verify if your specific implementation is supported by RUM, record a PCAP file and open a support ticket.

Monitoring ISO8583-based protocols can be supported either with standard or custom templates. If you have a custom implementation, you need to change the configuration files to adapt to your implementation.

## ISO8583 Message Format

The following is the ISO8583 message format:

M	O	O	M	M	O	0-127
Message-Length	Padding	Header	Message-Type-Identifier (MTI)	Bitmap-1	Bitmap-2	Data-Elements

M- Mandatory

O- Optional

## RUM Sniffer Probe Configuration Files

The RUM Sniffer Probe configuration files are located in **/etc/rum\_probe/protocols**. The following are the configuration files used in APM:

- **iso8583mc.def, iso8583visa.def**

The **iso8583mc.def** and **iso8583visa.def** configuration files provide basic configuration information, including the fields to be skipped/ hidden (sensitive data).

You can configure the fields that must be used to correlate request-response commands.

- **currencies.xml**

In the **currencies.xml** file you can add or update currency codes used by your customer's implementation

- **MC.xml, VISA\_BASEI.xml**

The **MC.xml** and **VISA\_BASEI.xml** files contain detailed message format definition.

The following is an APM-RUM mapping for each configuration file.

Template Name in APM	Protocol in APM	Protocol Name in RUMProbe's capture.conf	Configuration files on RUMProbe
MasterCard	ISO8583MC	iso8583mc	iso8583mc.def currencies.xml MC.xml
Visa	ISO8583BASEI	iso8583visa	iso8583visa.def currencies.xml VISA_BASEI.xml

If the custom protocol implementation is not supported with standard templates, you can customize the template as follows:

1. Locate the documentation for the custom implementation of the protocol.
2. In RUM probe `/etc/rum_probe/protocols`, open the file **MC.xml** or **VISA\_BASEI.xml** and change the protocol specification.
3. Use the modified version of the template to monitor the application.

If there are several versions of the protocol and all of them have to be monitored with the same RUM Probe instance, you need to have dedicated templates and configurations on APM, RUM Engine, and RUM Probe.

ISO8583 includes a variety of custom flavor implementations some of which are supported by RUM. We recommend consulting Support at an early development stage to provide support of custom flavor implementations.

## Configuration

Based on the message format that the customer has, either the **MC.xml** or **VISA\_BASEI.xml** file must be updated so that the messages gets parsed successfully.

The following is the xml file structure for the **MC.xml** file. The **VISA\_BASEI.xml** file has the same structure. The configuration updates described are applicable for both the **MC.xml** and **VISA\_BASEI.xml** files. The examples are for the **MC.xml** file. Explanations about various nodes appear in square brackets.

```
<?xml version="1.0" encoding="UTF-8" ?>
[First line of the file with xml version is a standard xml node, leave it unchanged]

<MASTERCARD_CIS numeric_encoding="TEXT" length_encoding="TEXT" data_encoding="ASCII">
[Root node of the xml]

<message_types>
[The node 'message_types' contains the details of various MTI types as children, updates/
addition is applicable]
.
.
<mti id="0200" name="Financial Transaction Request" />
.
.
<mti id="0210" name="Financial Transaction Request Response" />
.
```

```
.
</message_types>

<data_fields>
[The node 'data_fields' the details of various data-elements as children]

<data_field id="2" name="Primary Account Number (PAN)" type="N" length_length ="2"
length="19" fixed_length="false" is_padded="false" />

<data_field id="3" name="Processing Code" type="N" length="6" fixed_length="true" >
<sub_fields>
<sub_field id="1" name="Cardholder Transaction Type Code" type="N" length="2" fixed_
length="true" />
<sub_field id="2" name="Cardholder from Account Type Code" type="N" length="2" fixed_
length="true" />
<sub_field id="3" name="Cardholder to Account Type Code" type="N" length="2" fixed_
length="true" />
</sub_fields>
</data_field>

<data_field id="4" name="Amount, Transaction" type="N" length="12" fixed_length="true" >
  <value_transformers>
  <value_transformer id="trim_string" trim_left="true" trim_chars="0" />
  <value_transformer id="put_currency_decimal_point" currency_field_id="49" />
  </value_transformers>
</data_field>
.
.
</data_fields>
</MASTERCARD_CIS>
```

The following details are required from customers in order to update the configuration file:

- Message length-of-length, length-of-length-encoding
- Message padding present or not? If yes the length of padding
- Message Header present or not? If yes the format of the header
- MTI details
- Format of data elements
- Encodings used

## Message Length

Default values: DEFAULT\_MESSAGE\_LENGTH\_OF\_LENGTH = 2;

DEFAULT\_MESSAGE\_LENGTH\_ENCODING = RAW;

If any of the above is different, add a node as below as a child of the root node and update the attribute values

```
<message_length type="N" length="2" length_encoding="RAW"/>
```

An optional attribute ' fixed\_message\_length="the\_length" ' can be added to the node, if the message length is fixed. The other attributes are still required as it will be used to skip the initial bytes of the message which will be the message length

## Padding

There might be an optional padding-data in the message immediately after the message-length. This has to be skipped. Visa format has a default padding length of 2 and for MC 0. If it is different, add a node as below as a child of the root node and update the attribute values. Update the length accordingly

```
<padding_data_field id="0" name="SkipData" type="B" length="2"/>
```

## Header

Padding is followed by an optional header. Visa has a default header of the below format. MC by default has no header. If there is a change it, add a node as a child of the root node. This configuration is similar to the data-elements defined under the node <data\_fields>

Adding sub-fields is optional, refer the xml format above for a reference without sub-fields.

## Default Visa Header

```
<custom_header id="1" name="VisaHeader" type="B" length_length="1" length_encoding="RAW"
length_embedded_in_data="true">
  <sub_fields>
    <sub_field id = "2"    name = "Format"           type = "B" positions = "2:2" />
    <sub_field id = "3"    name = "TextFormat"       type = "B" positions = "3:3" />
    <sub_field id = "4"    name = "MessageLength"    type = "B" positions = "4:5" />
    <sub_field id = "5"    name = "DestinationID"   type = "B" positions = "6:8" />
    <sub_field id = "6"    name = "SourceID"        type = "B" positions = "9:11" />
    <sub_field id = "7"    name = "RoundTripInfo"   type = "B" positions = "12:12" />
    <sub_field id = "8"    name = "BASEIFlags"     type = "B" positions = "13:14" />
    <sub_field id = "9"    name = "StatusFlag"      type = "B" positions = "15:17" />
    <sub_field id = "10"   name = "BatchNumber"     type = "B" positions = "18:18" />
    <sub_field id = "11"   name = "Reserved"       type = "B" positions = "19:21" />
    <sub_field id = "12"   name = "UserInfo"       type = "B" positions = "22:22" />
    <sub_field id = "13"   name = "BitMap"         type = "B" positions = "23:24" />
    <sub_field id = "14"   name = "RejectDataGroup" type = "B" positions = "25:26" />
  </sub_fields>
</custom_header>
```

**Note:** If any of the above changes from Message-Length, Padding, or Header gets applied, make sure to apply the below change also. Add an attribute "configuration\_version" to the root node. The value of this attribute is not important currently, the product version can be mentioned.

So, for example, for 9.50 the attribute to be added to root node is:-

```
configuration_version="9.50"
```

## MTI

The header is followed by the MTI. There is a default list of MTIs added in the default configuration files available out-of-the-box. If there are addition MTIs add them. For example: <mti id="0100">

```
name="Authorization Request" />
```

An additional attribute [`is_request="true/false"`] can be added to the MTI nodes.

By default, the Sniffer Probe decides whether a message is a request or response based on the direction of the TCP connection. But for some implementations of ISO8583 based applications, a request may be sent from server to client

If the client is the node which initiates a connection, the `is_request` can be used to override the default logic.

## Bitmap

The MTI in an iso8583 message is followed by the bitmaps which indicates the presence/absence of the 127 data-elements in the following part of the message. The bitmap can be encoded. Default encoding is RAW. If it is different, add a node as below as a child of the root node and update the attribute value `<bitmap data_encoding="ASCII"/>`.

## Data\_fields

The `Data_fields` section of the xml file defines the format of each data element.

If there is a difference in the format of any of the data elements, modify the configuration for the specific element. If there are any missing elements which the customer's implementation is having, add them There could be 2 types of data elements: `Fixed_length` and `Variable_length` elements.

Some implementation adds padding at the end of `variable_length` fields. For such elements, add an attribute `is_padded="true"`

## Encoding

The root node of the xml will have the following encoding for the data elements.

You can modify it as per the encodings used by the customer's implementation.

Root node:-

```
<MASTERCARD_CIS numeric_encoding="TEXT" length_encoding="TEXT" data_encoding="ASCII">
```

- **numeric\_encoding** - Encoding used for numeral data elements in the iso8583 messages
- **length\_encoding** - Encoding used for length of data elements in the iso8583 messages
- **data\_encoding** - Encoding used for non-numeral data elements in the iso8583 messages

The following encodings are supported for iso8583 messages

- ASCII or TEXT
- EBCDIC
- RAW
- BCD

## Troubleshooting RumProbe - ISO8583 Protocol

**Symptoms:**

- No actions reported for ISO8583 traffic.
- The following parsing errors appear in the probe's log file: **Unexpected stream data. bad lexical cast: source type value could not be interpreted as target**

This issue is observed only in ISO8583 transactions.

### Solution

This issue is related to incorrect decoding of bitmaps for ISO 8583 messages.

In ISO 8583, a bitmap is a field or subfield within a message which indicates which other data elements or data element subfields may be present elsewhere in a message. The bitmap may be transmitted as 8 bytes of binary data, or as 16 hexadecimal characters 0-9, A-F in the ASCII or EBCDIC character sets. Choosing the correct bitmap is key for parsing messages.

In the default probe configuration, the bitmap is 8 bytes of binary data (RAW) and parsing is performed accordingly. To avoid parsing errors, you need to explicitly configure the bitmap.

1. In the `/etc/rum_probe/protocols/MC.xml` file after the line `<MASTERCARD_CIS numeric_encoding="TEXT" length_encoding="TEXT" data_encoding="ASCII">`, add one of the following lines according to the type of bitmap used.
  - `<bitmap data_encoding="ASCII"/>`
  - `<bitmap data_encoding="EBCDIC"/>`
2. Restart the probe.

### Example of the MC.xml configuration file

**Note:** The line in red is the line you need to add for an ASCII bitmap.

```
<?xml version="1.0" encoding="UTF-8" ?>
<MASTERCARD_CIS numeric_encoding="TEXT" length_encoding="TEXT" data_
encoding="ASCII">
bitmap data_encoding="ASCII"/>
<!--
this section contains description of message type identifiers used
in VISA BASE 1. Description is used by probe to describe
request/response type. These identifiers can be used within
protocols def file in skip_mti section to indicated which
messages must not be processed
-->
<message_types>
.....
```

# Send Documentation Feedback

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

**Feedback on Real User Monitor Administration Guide (Real User Monitor 9.50)**

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 [docteam@microfocus.com](mailto:docteam@microfocus.com).

We appreciate your feedback!